# POLÍTICA

INTEGRAL DE ADMINISTRACIÓN DE RIESGOS

(ANEXO 1)

Gestión Integrada MIPG - SIG
Unidad Nacional de Protección
02-10-2024

## TABLA DE CONTENIDO

4.2. Revisión y actualización

### A. DEFINICIONES

La interpretación y el desarrollo integral de esta Política tendrá en cuenta las siguientes definiciones:

ACTIVO. En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la Entidad.

AMENAZA. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Entidad.

APETITO DE RIESGO. Es el nivel de riesgo que la Entidad puede aceptar, en relación con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la Entidad debe o desea gestionar.

CAPACIDAD DE RIESGO. La capacidad de riesgo es el valor máximo del nivel de riesgo que la Entidad puede soportar y a partir del cual no sería posible el logro de los objetivos institucionales.

CAUSA. Factores internos o externos, medios, circunstancias o agentes que, por sí mismos o combinados con otros, pueden producir la materialización de un riesgo. Se clasifican en: personas, materiales, instalaciones y entorno.

CAUSA INMEDIATA. Circunstancias o situaciones bajo las cuales se presenta el riesgo, pero que no constituyen su causa raíz.

CAUSA RAÍZ. Causa principal o básica, que corresponde a las razones por la cuales se puede presentar el riesgo.

CONFIDENCIALIDAD. Principio de la seguridad de la información, según el cual la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

CONSECUENCIA. Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la Entidad, sus grupos de valor y demás partes interesadas.

CONTROL. Medida que permite reducir o mitigar un riesgo.

CONTROL CORRECTIVO. Control accionado en la salida del proceso y después de que se materializa el riesgo.

CONTROL DETECTIVO. Control accionado durante la ejecución del proceso.

CONTROL PREVENTIVO. Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo.

DISPONIBILIDAD. Principio de la seguridad de la información, según el cual se garantiza el acceso y uso de la información y de los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados, cuando estos lo requieran.

EVENTO POTENCIAL. Posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones en el recurso humano, los procesos, la tecnología o la infraestructura o por la ocurrencia de acontecimientos externos. En el marco del riesgo fiscal, los eventos potenciales se relacionan con una potencial acción u omisión que podría generar daño sobre los recursos públicos, bienes o intereses patrimoniales de naturaleza pública. El evento potencial es equivalente a la causa raíz.

IMPACTO. Consecuencia de la materialización de un riesgo.

INTEGRIDAD. Principio de la seguridad de la información que promueve el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

NIVEL DE RIESGO. El nivel de riesgo es el valor que resulta de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud de su impacto sobre la capacidad de alcanzar los objetivos institucionales.

PLAN DE TRATAMIENTO. Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implementar los controles necesarios para su protección.

PROBABILIDAD. Posibilidad de ocurrencia de un riesgo, asociada a la exposición al riesgo del proceso o actividad. La probabilidad inherente corresponde al número de veces que se pasa por el punto de riesgo en 1 año.

PUNTO DE RIESGO. Los puntos de riesgo son actividades, dentro del flujo de procesos, donde existe evidencia o indicio de que pueden ocurrir eventos de riesgo. Los puntos de riesgo fiscal son todas las actividades que representan gestión fiscal, como las actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de bienes, recursos o intereses de naturaleza pública.

RIESGO. Efecto que se causa sobre los objetivos de la Entidad, debido a eventos potenciales.

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 FISCAL. Efecto dañoso sobre los recursos públicos o los bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. El riesgo fiscal es un tipo de riesgo de gestión.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

RIESGO INHERENTE. Se entiende como riesgo inherente aquel que enfrenta una entidad u organismo ante la ausencia de acciones orientadas a controlar su probabilidad de ocurrencia o impacto.

RIESGO RESIDUAL. Se entiende como riesgo residual el nivel de riesgo que permanece, una vez implementados los controles sobre su probabilidad de ocurrencia o impacto.

TOLERANCIA DEL RIESGO. La tolerancia del riesgo es el valor de la máxima desviación admisible del nivel de riesgo, con respecto al valor del apetito de riesgo de la Entidad.

TRATAMIENTO. Respuesta de la primera línea de defensa, para mitigar un riesgo de la Entidad.

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

### B. MARCO NORMATIVO

| Año | Norma | Epígrafe |
|---|---|---|
| 1991 | Constitución Política | Constitución Política de 1991 |
| 1993 | Ley 87 | Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones |
| 1998 | Ley 489 | Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones |
| 2011 | Ley 1473 | Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública |

| Año | Norma | Epígrafe |
|---|---|---|
| 2015 | Ley 1753 | Por la cual se expide el Plan Nacional de Desarrollo 2014-2018, «Todos por un nuevo país» |
| 2015 | Decreto Nacional 1083 | Por medio del cual se expide el Decreto Único Reglamentario de sector Función Pública |
| 2022 | Resolución 1023 | Por la cual se adopta el Modelo Integrado de Planeación y Gestión de la Unidad Nacional de Protección y se dictan otras disposiciones |

## CAPÍTULO 1

ASPECTOS GENERALES

### 1.1. INTRODUCCIÓN

La Alta Dirección de la Unidad Nacional de Protección, liderada por el director general y con la participación del Comité Institucional de Coordinación de Control Interno, adopta esta Política Integral de Administración de Riesgos, de acuerdo con la dirección e intenciones generales de la Entidad, en materia de la gestión integral del riesgo.

### 1.2. DECLARATORIA

La Alta Dirección de la Unidad Nacional de Protección se compromete a mantener niveles aceptables en los riesgos de todos sus procesos y a promover una cultura institucional basada en la gestión integral del riesgo; mediante la identificación e implementación oportuna de acciones preventivas y de control, orientadas a mitigar, corregir y evitar la materialización de los riesgos institucionales.

### 1.3. METODOLOGÍA

La propuesta metodológica subyacente responde a los lineamientos de la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas* - versión 6 (2022) del Departamento Administrativo de la Función Pública, del *Documento Maestro del Modelo de Seguridad y Privacidad de la Información* (2021), del *Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas – Anexo 4* (2021) y de la *Guía de gestión de riesgos número 7: seguridad y privacidad de la información* (2016)

del Ministerio de Tecnologías de la Información y las Comunicaciones; en armonía con la Norma Técnica Colombiana NTC ISO 31000:2018 – Gestión del riesgo, ISO 9001:2015 - Sistema de Gestión de la Calidad e ISO 27001:2022 - Sistema de Gestión en Seguridad de la Información.

### 1.4. OBJETIVO GENERAL

El objetivo de la Política Integral de Administración de Riesgos es alcanzar un nivel aceptable del riesgo residual en todos los procesos del Sistema Integrado de Gestión de la Unidad Nacional de Protección, a través de la identificación e implementación oportuna de mecanismos y acciones de control, alineados con los objetivos y con la plataforma estratégica de la Entidad.

### 1.5. OBJETIVOS ESPECÍFICOS

Para la consecución del objetivo general, se definen los siguientes objetivos específicos:

I. Contribuir a la consolidación de una cultura organizacional basada en la gestión integral del riesgo y en la apropiación de los valores institucionales.
II. Unificar los lineamientos, controles, responsabilidades y estrategias asociadas a la administración y gestión integral de los riesgos de gestión/por procesos, fiscales, de corrupción y de seguridad digital de la Entidad.
III. Garantizar la pertinencia, idoneidad e integralidad de los lineamientos, mecanismos y controles del riesgo, con énfasis en la mitigación o eliminación de los riesgos que comprometen el cumplimiento misional o el logro de los objetivos estratégicos de la Entidad.
IV. Contribuir a la mejora continua de los procesos del Sistema Integrado de Gestión, mediante el diseño e implementación de acciones periódicas de monitoreo, seguimiento, control y revisión del riesgo.

### 1.6. ALCANCE

El alcance y ámbito de aplicación de esta Política comprende a los servidores públicos, contratistas y colaboradores de todas las dependencias y niveles jerárquicos de la Entidad; así como a los procesos, procedimientos, planes, programas, proyectos y demás componentes del Sistema Integrado de Gestión (SIG), del Sistema de Gestión de Calidad (SGC), del Sistema de Gestión Ambiental (SGA), del Sistema de Gestión de Seguridad y Privacidad

de la Información (SG-SPI) y del Sistema de Gestión de Salud y Seguridad en el Trabajo (SG-SST) de la Unidad Nacional de Protección.

Conforme a lo anterior, la Política Integral de Administración de Riesgos de la Unidad Nacional de Protección será aplicable, vinculante y de cumplimiento prioritario para todos los servidores públicos, contratistas y colaboradores de la Entidad; de acuerdo con el esquema de líneas de defensa y con las responsabilidades específicas de los líderes de proceso y de la Alta Dirección.

## CAPÍTULO 2

### OPERATIVIDAD Y APETITO DEL RIESGO

A continuación, se establecen las responsabilidades de las líneas de defensa, la operatividad de la Política y se definen el apetito del riesgo, las zonas de riesgo y la tabla de clasificación de riesgos:

### 2.1. RESPONSABILIDADES

De acuerdo con el alcance de esta Política y con el esquema de líneas de defensa definido en la Resolución 1023 de 2022 de la Unidad Nacional de Protección, o la norma que haga sus veces, se adoptan los siguientes niveles de responsabilidad y de autoridad para la gestión integral del riesgo, en consonancia con la dimensión de control interno del Manual operativo del Modelo Integrado de Planeación y Gestión:

| Línea de defensa | Instancias responsables | Responsabilidad frente a la gestión del riesgo |
|---|---|---|
| Línea Estratégica | • Alta Dirección.<br>• Comité Institucional de Gestión y Desempeño.<br>• Comité Institucional de Coordinación de Control Interno. | • Definir, aprobar y supervisar el marco institucional de gestión de riesgos y la Política Integral de Administración de Riesgos de la Entidad.<br>• Monitorear los riesgos críticos, con base en la información suministrada por la Segunda Línea de Defensa y de acuerdo con la periodicidad establecida por la Entidad.<br>• Supervisar, intervenir y corregir las situaciones de incumplimiento, retraso o irregularidades de la gestión integral del riesgo. |

| Línea de defensa | Instancias responsables | Responsabilidad frente a la gestión del riesgo |
|---|---|---|
| Primera Línea de Defensa | • Responsables de procesos.<br>• Coordinadores de grupos internos de trabajo.<br>• Responsables de planes y programas institucionales.<br>• Gerentes de proyecto.<br>• Servidores públicos de la Entidad. | • Hacer seguimiento permanente e implementar los controles y mecanismos de gestión de riesgos, a través de la identificación, análisis, valoración y monitoreo de riesgos.<br>• Orientar el desarrollo e implementación de las políticas y procedimientos, garantizando su compatibilidad con las metas y objetivos institucionales, y diseñar e implementar las acciones de mejora correspondientes. |
| Segunda Línea de Defensa | • Supervisores e interventores de contratos o convenios de la Entidad.<br>• Jefe de la Oficina Asesora de Planeación e Información.<br>• Secretario general.<br>• Comités institucionales distintos a los que trata el artículo 3 de la Resolución 1023 de 2022 de la Unidad Nacional de Protección, o la norma que haga sus veces.<br>• Los representantes de la Alta Dirección para las políticas del Modelo Integrado de Planeación y Gestión, conforme al artículo 4 de la Resolución 1023 de 2022 de la Unidad Nacional de Protección, o la norma que haga sus veces.<br>• Representantes de la Alta Dirección para el Sistema Integrado de Gestión (SIG) de la Entidad y los sistemas que lo componen, de acuerdo con el artículo 5 de la Resolución 1023 de 2022 | • Monitorear los mapas integrales de riesgos de gestión/por procesos, fiscales, de corrupción y de seguridad y privacidad de la información; conforme a la periodicidad establecida por la Entidad.<br>• Formular recomendaciones que permitan el ajuste y mejora continua de los controles y mecanismos de gestión de riesgos a cargo de la Primera Línea de Defensa.<br>• Supervisar y apoyar el diseño y el funcionamiento de los controles y mecanismos de gestión de riesgos a cargo de la Primera Línea de Defensa. |

| Línea de defensa | Instancias responsables | Responsabilidad frente a la gestión del riesgo |
|---|---|---|
| | de la Unidad Nacional de Protección, o la norma que haga sus veces. | |
| Tercera Línea de Defensa | • Jefe de la Oficina de Control Interno. | • Evaluar la efectividad de los controles de los mapas integrales de riesgos y supervisar el cumplimiento de la Política Integral de Administración de Riesgos, de acuerdo con la periodicidad establecida por la Entidad.<br>• Asesorar y acompañar a las dependencias internas de la Entidad, en el marco del Plan Anual de Auditoría, para evitar la materialización de riesgos.<br>• Monitorear, identificar y alertar a la Línea Estratégica sobre posibles cambios o factores que afecten la exposición o la gestión integral de riesgos de la Entidad. |

## 2.2. OPERATIVIDAD

Se adopta el siguiente esquema de operatividad para la administración y gestión integral del riesgo:

| | |
|---|---|
| Comité Institucional de Coordinación de Control Interno | Aprobación y seguimiento de la Política Integral de Administración de Riesgos<br><br>Análisis de eventos y riesgos críticos |
| Comité Institucional de Gestión y Desempeño | Análisis de la gestión integral del riesgo y aplicación de acciones de mejora |
| Oficina de Control Interno – Tercera Línea de Defensa | Asesoría, acompañamiento y orientación técnica para la administración del riesgo<br><br>Monitoreo de la exposición al riesgo y evaluación de la efectividad de los controles y de la gestión de la Segunda Línea de Defensa |

| | |
|---|---|
| Oficina Asesora de Planeación e Información – Segunda Línea de Defensa | Acompañamiento y recomendaciones para la administración del riesgo<br><br>Monitoreo de los controles y procesos de gestión del riesgo a cargo de la Primera Línea de Defensa |
| Líderes de proceso – Primera Línea de Defensa | Identificación de riesgos e implementación de controles |

Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) del Departamento Administrativo de la Función Pública.

La operatividad de la Política Integral de Administración de Riesgos de la Unidad Nacional de Protección observará las directrices y criterios definidos por el Gobierno Nacional, a través de los siguientes documentos:

| Núm. | Documento |
|---|---|
| 1 | *Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6* (2022) del Departamento Administrativo de la Función Pública; o el documento que haga sus veces. |
| 2 | *Guía para la administración del riesgo y el diseño de controles en entidades públicas: riesgos de gestión, corrupción y seguridad digital versión 4* (2018) del Departamento Administrativo de la Función Pública; en lo que respecta a la gestión del riesgo de corrupción. |
| 3 | *Documento Maestro del Modelo de Seguridad y Privacidad de la Información* (2021) del Ministerio de Tecnologías de la Información y las Comunicaciones, o el documento que haga sus veces, en lo que respecta a la gestión del riesgo de seguridad y privacidad de la información. |
| 4 | *Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas – Anexo 4* (2021) del Ministerio de Tecnologías de la Información y las Comunicaciones, o el documento que haga sus veces, en lo que respecta a la gestión del riesgo de seguridad de la información. |
| 5 | *Guía de Gestión de Riesgos: Seguridad y Privacidad de la Información – Guía 7* (2016) del Ministerio de Tecnologías de la Información y las Comunicaciones, o el documento que haga sus veces, en lo que respecta a la gestión del riesgo de seguridad y privacidad de la información. |

Para los anteriores efectos, la Unidad Nacional de Protección armonizará y dispondrá de los siguientes elementos en su Sistema Integrado de Gestión:

- Manual Integral de Gestión de Riesgos (GIN-MA-02) - proceso de Gestión Integrada MIPG-SIG.

- Modelo de Seguridad y Privacidad de la Información - proceso de Gestión Tecnológica.
- Guía Identificación y Valoración de Riesgos de Seguridad y Privacidad de la Información (GTE-GU-04) - proceso de Gestión Tecnológica.
- Plan de Seguridad y Privacidad de la Información (GTE-PL-02) - proceso de Gestión Tecnológica.
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (GTE-PL-03) - proceso de Gestión Tecnológica.

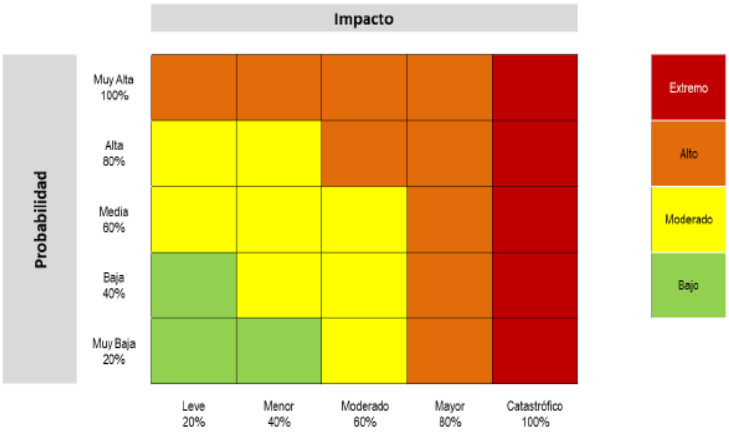
### 2.3. APETITO DEL RIESGO

A continuación, se establece el apetito del riesgo, que comprende los niveles de riesgo aceptables para la Entidad, en relación con sus objetivos estratégicos, marco normativo y directrices de la Alta Dirección:

| **Apetito del riesgo** | |
|---|---|
| Riesgo de gestión/por procesos | Se acepta en el nivel de riesgo residual bajo o moderado. |
| Riesgo de corrupción | No se acepta en ningún nivel de riesgo residual. |
| Riesgo fiscal | No se acepta en ningún nivel de riesgo residual. |
| Riesgo de seguridad y privacidad de la información | Se acepta en el nivel de riesgo residual bajo o moderado. |

### 2.4. ZONAS DE RIESGO

Se adoptan las siguientes cuatro (04) zonas de riesgo, correspondientes a los niveles de riesgo:




Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública.

| | |
|---|---|
| E | Nivel de riesgo extremo |
| A | Nivel de riesgo alto |
| M | Nivel de riesgo moderado |
| B | Nivel de riesgo bajo |

## CAPÍTULO 3

## ESTRUCTURA DE IMPLEMENTACIÓN

La metodología para la administración del riesgo requiere de un análisis inicial, relacionado con el estado actual de la estructura de riesgos y su gestión en la Entidad, además del conocimiento de esta, desde un punto de vista estratégico de la aplicación de los tres (03) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la Entidad, para que su efectividad pueda evidenciarse.

La Política Integral de Administración de Riesgos de la Unidad Nacional de Protección tendrá la siguiente estructura de implementación:

- Paso 0. Política Integral de Administración de Riesgos.
- Paso 1. Identificación del riesgo.
- Paso 2. Valoración del riesgo.
- Paso 3. Tratamiento del riesgo.

### 3.1. PASO 0. ADOPCIÓN DE LA POLÍTICA

El paso cero (0) de la estructura de implementación comprende la aprobación, expedición y socialización inicial del acto administrativo, por medio del cual se adopta la Política Integral de Administración de Riegos de la Unidad Nacional de Protección.

La socialización inicial estará dirigida a los servidores públicos, contratistas, colaboradores y demás grupos de valor de la Entidad y promoverá su apropiación, entendimiento y aplicación permanente.

### 3.2. PASO 1. IDENTIFICACIÓN DEL RIESGO

El paso número 1 de la estructura de implementación tiene el objetivo de identificar las fuentes o factores de riesgo, los eventos o riesgos y sus causas y consecuencias.

La identificación de los riesgos comprenderá seis fases consecutivas: (i) análisis de objetivos estratégicos y de los procesos de la Entidad, (ii) identificación de los puntos de riesgo, (iii) identificación de las áreas de impacto, (iv) identificación de las áreas de factores de riesgo, (v) descripción del riesgo y (vi) clasificación del riesgo.

Para la identificación de los riesgos fiscales, adicionalmente se adopta la tabla de preguntas orientadoras para puntos de riesgo fiscal y causas inmediatas de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6* (2022) del Departamento Administrativo de la Función Pública:

| Sirve para identificar | Preguntas y respuestas para la identificación |
|---|---|
| Puntos de riesgo fiscal | ¿En qué procesos de la Entidad se realiza gestión fiscal? |
| Puntos de riesgo fiscal y circunstancias inmediatas | Clasifique por procesos (según el mapa de procesos de la Entidad) los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal; los fallos con responsabilidad fiscal en firme, relacionados con hechos de la Entidad o del sector; las advertencias de la Contraloría General de la República o las alertas reportadas en el Sistema de Alertas de Control Interno – SACI. |
| Circunstancias inmediatas | En un ejercicio autocrítico, realista y objetivo, ¿cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la Oficina de Control Interno, en los últimos 3 años? |
| Puntos de riesgo fiscal y circunstancias inmediatas | ¿Qué puntos de riesgo fiscal y circunstancias inmediatas del «Catálogo Indicativo y Enunciativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas»[1] son aplicables a la Entidad? |

Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública.

Para la identificación y gestión integral del riesgo de seguridad y privacidad de la información, se adoptan los lineamientos del *Documento Maestro del Modelo de Seguridad y Privacidad de la Información* (2021), del

[1] Anexo 1 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6 (2022) del Departamento Administrativo de la Función Pública.

*Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas – Anexo 4* (2021) y de la *Guía de gestión de riesgos número 7: seguridad y privacidad de la información* (2016) del Ministerio de Tecnologías de la Información y las Comunicaciones.

Para la gestión integral del riesgo de corrupción, se adoptan los lineamientos de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas: riesgos de gestión, corrupción y seguridad digital versión 4* (2018) del Departamento Administrativo de la Función Pública, en armonía con las directrices de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6* (2022) del Departamento Administrativo de la Función Pública.

### 3.2.1. ANÁLISIS DE OBJETIVOS ESTRATÉGICOS Y DE LOS PROCESOS

La primera fase de la identificación del riesgo comprende el análisis de los objetivos estratégicos y de los objetivos de los procesos de la Entidad, así:

| **Análisis de objetivos** |
|---|

| **Objetivos estratégicos** | **Objetivos de proceso** |
|---|---|
| La Entidad analizará la formulación de sus objetivos estratégicos y su consonancia con los objetivos de proceso, en el marco de la identificación de posibles riesgos que afecten su cumplimiento y que puedan conllevar a su éxito o fracaso.<br><br>Los objetivos estratégicos deben estar alineados con la misión y visión institucional y se garantizarán los siguientes atributos mínimos: específico, medible, alcanzable, relevante y proyectado en el tiempo (temporal). | La Entidad analizará la formulación de los objetivos de sus procesos, en el marco de la identificación de posibles riesgos que afecten su cumplimiento y que puedan conllevar a su éxito o fracaso.<br><br>Los objetivos de proceso deben estar alineados con la misión y visión institucional y se garantizarán los siguientes atributos mínimos: específico, medible, alcanzable, relevante y proyectado en el tiempo (temporal). |

| La formulación de los objetivos estratégicos y de los objetivos de los procesos institucionales debe responder ¿qué?, ¿cómo?, ¿para qué?, ¿cuándo? y ¿cuánto? |
|---|

La correcta formulación de los objetivos estratégicos y de los objetivos de los procesos de la Entidad es necesaria para el desarrollo de la metodología de gestión de riesgos.

Adaptado de: Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública y Marco Integrado: componente evaluación de riesgos del Comittee of Sponsoring Organizations of the Treadway Commission COSO (2013).

### 3.2.2. **PUNTOS DE RIESGO**

La segunda fase de la identificación del riesgo exige el análisis e inventario de los puntos de riesgo, entendidos como las actividades de los flujos de proceso para las que existe evidencia o indicio de posibles riesgos operativos. Para los anteriores efectos, se tendrá en cuenta la cadena de valor público:


Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública

### 3.2.3. **ÁREAS DE IMPACTO**

La tercera fase de la identificación del riesgo comporta la definición del área de impacto, entendida como la consecuencia económica o reputacional a la que se expone la Entidad, en caso de materializarse el riesgo. Los impactos aplicables son: afectación económica o presupuestal y afectación reputacional.

### 3.2.4. **FACTORES DE RIESGO**

La cuarta fase de la identificación del riesgo exige la caracterización de los factores de riesgo o fuentes generadoras de riesgo. Estos factores podrán ser, entre otros:

- Procesos: eventos relacionados con errores en las actividades que deben realizar los servidores de la Entidad (falta de procedimientos, errores de grabación, autorización, errores en cálculos para pagos internos y externos, falta de capacitación).
- Talento humano: incluye seguridad y salud en el trabajo y se analiza posible dolo e intención frente a la corrupción (hurto de activos, posibles comportamientos no éticos, fraude interno, soborno).
- Tecnología: eventos relacionados con la infraestructura tecnológica de la Entidad (daño de equipos, caída de aplicaciones, caída de redes, errores en programas).
- Infraestructura: eventos relacionados con la infraestructura física de la Entidad (derrumbes, incendios, inundaciones, daños a activos físicos).
- Eventos externos: situaciones externas que afectan a la Entidad (suplantación de identidad, asalto a la oficina, atentados, vandalismo, afectaciones al orden público).

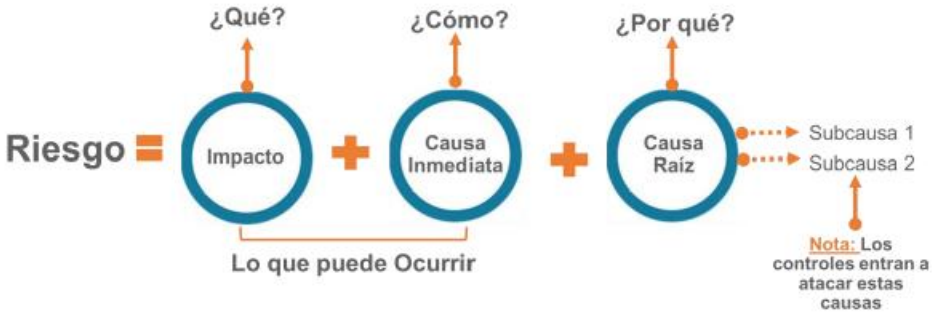
### 3.2.5. **DESCRIPCIÓN DEL RIESGO**

La quinta fase de la identificación del riesgo es la redacción o descripción del riesgo, para lo cual se tendrán en cuenta las siguientes premisas generales:

- No se describirán como riesgos las omisiones o desviaciones del control.
- No se describirán como riesgos las negaciones de un control.
- No existen riesgos transversales, sino causas transversales.
- Las causas no harán parte de la descripción del riesgo.

#### **3.2.5.1. DESCRIPCIÓN DEL RIESGO DE GESTIÓN/POR PROCESOS**

La descripción de los riesgos de gestión/por procesos iniciará con las palabras «posibilidad de» y contendrá los detalles necesarios para facilitar su entendimiento tanto por el líder del proceso como por personas ajenas a este:



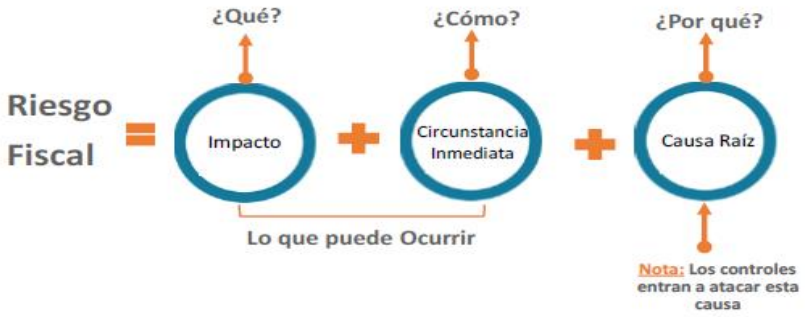

Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública.

La descripción de los riesgos de gestión/por procesos evitará la subjetividad en la redacción y permitirá comprender su forma de materialización, su impacto, sus causas inmediatas y su causa raíz; entendidas así:

- Impacto. Responde al ¿qué? y se refiere a un efecto dañoso sobre la Entidad o sobre el alcance de sus objetivos estratégicos, como consecuencia de la materialización de un riesgo.
- Causa inmediata. Responde al ¿cómo? y se refiere a las circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, pero que no constituyen su causa raíz.
- Causa raíz. Responde al ¿por qué? y se refiere a la causa principal, causa básica, generador directo, causa eficiente o causa adecuada del riesgo. La causa raíz es la condición necesaria para la materialización del riesgo.

### 3.2.5.2. DESCRIPCIÓN DEL RIESGO FISCAL

La descripción del riesgo fiscal –entendido como un tipo de riesgo de gestión/por procesos– iniciará con las palabras «posibilidad de» y contendrá los detalles necesarios para facilitar su entendimiento tanto por el líder del proceso como por personas ajenas a este:




Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública.

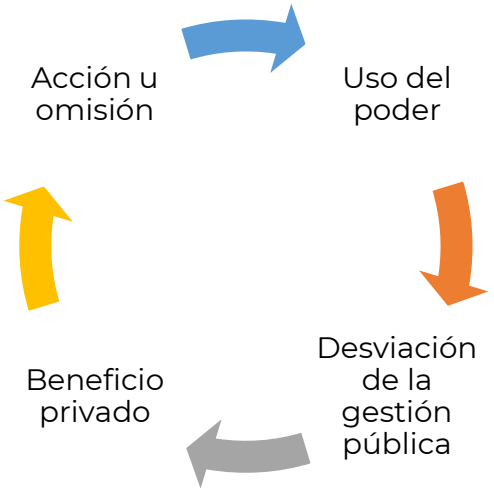
La descripción de los riesgos fiscales evitará la subjetividad en la redacción y permitirá comprender su forma de materialización, su impacto, sus causas inmediatas y su causa raíz; entendidas así:

- Impacto. Responde al *¿qué?* y se refiere a un efecto dañoso sobre la Entidad o sobre el alcance de sus objetivos estratégicos, como consecuencia de la materialización de un riesgo.
- Circunstancia o causa inmediata. Responde al *¿cómo?* y se refiere a las circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, pero que no constituyen su causa raíz.
- Causa raíz. Responde al *¿por qué?* y se refiere a la causa principal, causa básica, generador directo, causa eficiente o causa adecuada del riesgo. La causa raíz es la condición (acción u omisión) necesaria para la materialización del riesgo.

#### 3.2.5.3. DESCRIPCIÓN DEL RIESGO DE CORRUPCIÓN

Para la gestión integral del riesgo de corrupción, se aplicarán los lineamientos de la cuarta versión de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas: riesgos de gestión, corrupción y seguridad digital* (2018) del Departamento Administrativo de la Función Pública, en armonía con las directrices de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6* (2022) del Departamento Administrativo de la Función Pública.

La descripción de los riesgos de corrupción: (i) iniciará con las palabras «posibilidad de», (ii) incluirá los detalles necesarios para facilitar su entendimiento tanto por el líder del proceso como por personas ajenas a este y (iii) contendrá los siguientes cuatro elementos conceptuales:




Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) del Departamento Administrativo de la Función Pública.

De acuerdo con lo anterior, los riesgos de corrupción describen una posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. Las prácticas corruptas se originan en actores públicos o en actores privados con poder e incidencia en la toma de decisiones y administración de bienes públicos.

Para la descripción de los riesgos de corrupción, se adopta la matriz de definición de riesgos de corrupción de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6* (2022) del Departamento Administrativo de la Función Pública:

| 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 |

Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública.

### 3.2.5.4. DESCRIPCIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la gestión integral del riesgo de seguridad y privacidad de la información, se aplicarán los lineamientos del *Documento Maestro del Modelo de Seguridad y Privacidad de la Información* (2021), del *Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas – Anexo 4* (2021) y de la *Guía de gestión de riesgos número 7: seguridad y privacidad de la información* (2016) del Ministerio de Tecnologías de la Información y las Comunicaciones.

Para la descripción de los riesgos de seguridad y privacidad de la información, se tendrán las siguientes seis (06) tipologías específicas, referentes a la afectación de (i) los principios de la seguridad y privacidad de la información o (ii) de las actividades propias del Sistema de Gestión de Seguridad y privacidad de la Información:

| Tipologías específicas de riesgos de seguridad y privacidad de la información | |
|---|---|
| 1 | Posibilidad de comprometer la integridad de la información institucional debido las fallas técnicas y operativas en el proceso. |
| 2 | Posibilidad de comprometer la confidencialidad de la información institucional debido a las fallas técnicas y operativas en el proceso. |
| 3 | Posibilidad de comprometer la disponibilidad de la información institucional debido las fallas técnicas y operativas en el Proceso. |
| 4 | Posibilidades de no atender la automatización de proceso de la Entidad, por capacidad de productos adquiridos. |
| 5 | Posibilidad de tener sistemas de información desatendidos o sin soporte. |
| 6 | Posibilidad de afectación de confidencialidad, integridad o disponibilidad de la información institucional por errores humanos. |

Los riesgos de seguridad y privacidad de la información deben asociarse a un grupo de activos o activos específicos del proceso y, conjuntamente, deben analizarse las amenazas y vulnerabilidades que puedan causar su materialización.

### 3.2.6. CLASIFICACIÓN DEL RIESGO

Durante la última fase de la identificación de riesgos, se agruparán o clasificarán los riesgos identificados, según las categorías de la siguiente tabla:

| | |
|---|---|
| Ejecución y administración de procesos | Pérdidas derivadas de errores en la ejecución y administración de procesos. |
| Fraude externo | Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la Entidad). |
| Fraude interno | Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros. |

| | |
|---|---|
| Fallas tecnológicas | Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos. |
| Relaciones laborales | Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación. |
| Usuarios, productos y prácticas | Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos. |
| Daños a activos fijos/eventos externos | Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público. |

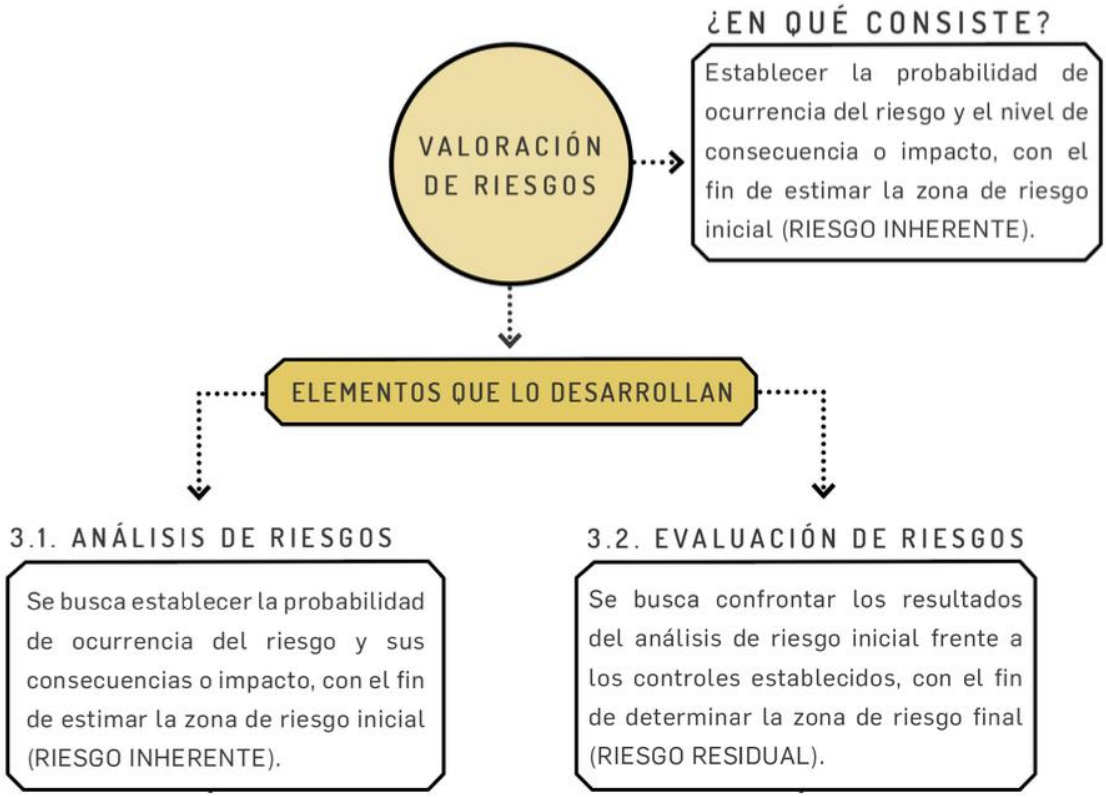
Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública.

La relación entre los factores de riesgo y la clasificación de los riesgos será la siguiente:


Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública.

### 3.3. VALORACIÓN DEL RIESGO

Atendiendo los lineamientos del Departamento Administrativo de la Función Pública y del Ministerio de Tecnologías de la Información y las Comunicaciones en materia de administración de riesgos y diseños de controles efectivos, la Unidad Nacional de Protección adelantará la valoración del riesgo en dos fases: (1) análisis del riesgo y (2) evaluación del riesgo:




Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022)
Departamento Administrativo de la Función Pública.

### 3.3.1. ANÁLISIS DEL RIESGO

La primera fase de la valoración del riesgo tiene el objetivo de establecer su probabilidad de ocurrencia y las consecuencias o impacto asociado a su materialización.

La probabilidad de ocurrencia está asociada a la exposición al riesgo del proceso o actividad analizada. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el período de un (01) año.

#### 3.3.1.1. ANÁLISIS DEL RIESGO FISCAL Y DE GESTIÓN/POR PROCESOS

Se adoptan las siguientes tablas de impacto y de probabilidad para el análisis de los riesgos fiscales y de gestión/por procesos:

#### 3.3.1.1.1. TABLA DE IMPACTO – RIESGO FISCAL Y DE GESTIÓN/POR PROCESOS

Se adopta la siguiente tabla para calificar el impacto de los riesgos fiscales y de gestión/por procesos:

| | Afectación económica | Reputacional |
|---|---|---|
| Leve 20% | Inferior a 10 SMLMV. | El riesgo afecta la imagen de alguna dependencia de la Entidad. |
| Menor-40% | Entre 10 y 50 SMLMV. | El riesgo afecta la imagen de la Entidad a nivel interno, Dirección General, Consejo Directivo o proveedores. |
| Moderado 60% | Entre 50 y 100 SMLMV. | El riesgo afecta la imagen de la Entidad con algunos usuarios de relevancia frente al logro de los objetivos estratégicos. |
| Mayor 80% | Entre 100 y 500 SMLMV. | El riesgo afecta la imagen de la Entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal. |
| Catastrófico 100% | Superior a 500 SMLMV. | El riesgo afecta la imagen de la Entidad a nivel nacional, con efecto publicitario sostenible a nivel país. |

Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública.

#### 3.3.1.1.2. TABLA DE PROBABILIDAD DE OCURRENCIA – RIESGO FISCA Y DE GESTIÓN/POR PROCESOS

Se adopta la siguiente tabla para calificar la probabilidad de ocurrencia de los riesgos fiscales y de gestión/por procesos:

| | Frecuencia de la actividad | Probabilidad |
|---|---|---|
| Muy Baja | La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año. | 20% |
| Baja | La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año. | 40% |
| Media | La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año. | 60% |
| Alta | La actividad que conlleva el riesgo se ejecuta mínimo 500 y máximo 5.000 veces por año. | 80% |
| Muy Alta | La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año. | 100% |

Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública.

#### 3.3.1.2. ANÁLISIS DEL RIESGO DE CORRUPCIÓN

Se adoptan los siguientes criterios para el análisis y calificación del impacto y de la probabilidad de ocurrencia de los riesgos de corrupción:

##### 3.3.1.2.1. CRITERIOS DE IMPACTO – RIESGO DE CORRUPCIÓN

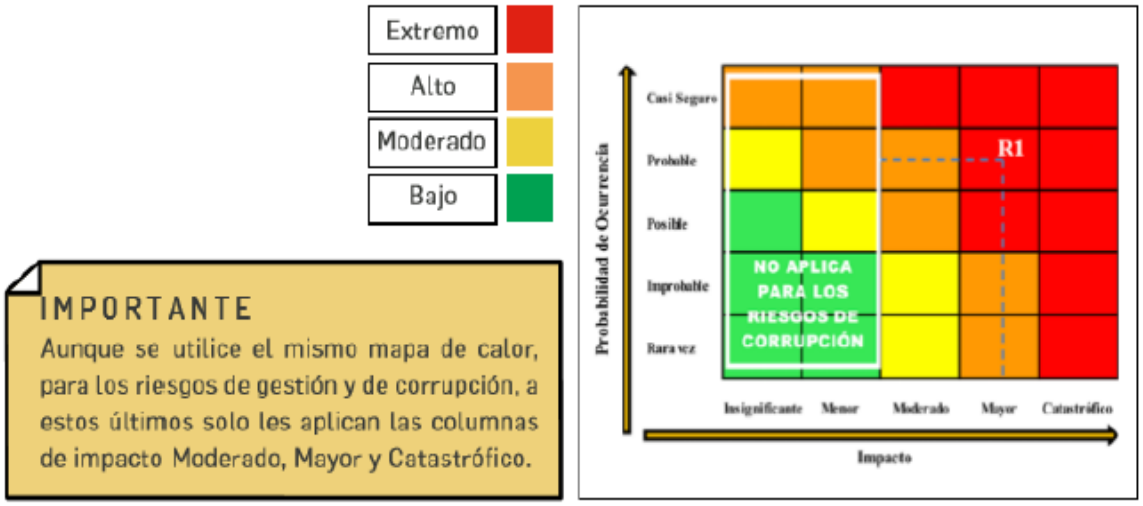
El análisis de impacto de los riesgos de corrupción se realiza a partir de las consecuencias identificadas en la fase de descripción del riesgo y conforme a la siguiente tabla de valoración:

| # | Pregunta:<br>Si el riesgo de corrupción se materializa, podría... | Respuesta | |
|---|---|---|---|
| | | Sí | No |
| 1 | ¿Afectar al grupo de funcionarios del proceso? | | |
| 2 | ¿Afectar el cumplimiento de metas y objetivos de la dependencia? | | |
| 3 | ¿Afectar el cumplimiento de misión de la Entidad? | | |
| 4 | ¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad? | | |

| | | | |
|---|---|---|---|
| 5 | ¿Generar pérdida de confianza en la Entidad, afectando su reputación? | | |
| 6 | ¿Generar pérdida de recursos económicos? | | |
| 7 | ¿Afectar la generación de los productos o la prestación de servicios? | | |
| 8 | ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien | | |
| 9 | ¿Generar pérdida de información en la Entidad? | | |
| 10 | ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente? | | |
| 11 | ¿Dar lugar a procesos sancionatorios? | | |
| 12 | ¿Dar lugar a procesos disciplinarios? | | |
| 13 | ¿Dar lugar a procesos fiscales? | | |
| 14 | ¿Dar lugar a procesos penales? | | |
| 15 | ¿Generar pérdida de credibilidad del sector? | | |
| 16 | ¿Ocasionar lesiones físicas o pérdida de vidas humanas? | | |
| 17 | ¿Afectar la imagen regional? | | |
| 18 | ¿Afectar la imagen nacional? | | |
| 19 | ¿Generar daño ambiental? | | |
| | TOTAL | | |
| Responder afirmativamente de UNA a CINCO preguntas, genera un impacto MODERADO. | | | |
| Responder afirmativamente de SEIS a ONCE preguntas, genera un impacto MAYOR. | | | |
| Responder afirmativamente de DOCE a DIECINUEVE preguntas, genera un impacto CATASTRÓFICO. | | | |
| NOTA. Cuando la respuesta a la pregunta número 16 sea afirmativa, el riesgo será CATASTRÓFICO. | | | |

Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022)
Departamento Administrativo de la Función Pública.

El análisis de impacto de los riesgos de corrupción solo tendrá en cuenta los niveles *moderado, mayor* y *catastrófico*, ya que estos riesgos siempre serán significativos. Para los riesgos de corrupción no serán aplicables los niveles de impacto *insignificante* y *menor*.




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

Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022)
Departamento Administrativo de la Función Pública

### 3.3.1.2.2. CRITERIOS DE PROBABILIDAD – RIESGO DE CORRUPCIÓN

Para la gestión de riesgos de corrupción, continúan vigentes los lineamientos de la versión 4 de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas: riesgos de gestión, corrupción y seguridad digital* (2018) del Departamento Administrativo de la Función Pública.

La probabilidad de ocurrencia de los riesgos de corrupción se expresa en términos de frecuencia o factibilidad, donde: (i) la *frecuencia* implica analizar el número de eventos en un período determinado –tratándose de hechos que se han materializado o para los que se cuenta con un historial de situaciones o eventos asociados al riesgo– y (ii) la *factibilidad* implica analizar la presencia de factores internos y externos que propician el riesgo, tratándose de hechos que no se han presentado, pero es posible que sucedan.

| Nivel | Descriptor | Descripción | Frecuencia |
|---|---|---|---|
| 5 | Casi seguro | Se espera que el evento ocurra en la mayoría de las circunstancias. | Más de una (01) vez al año. |
| 4 | Probable | Es viable que el evento ocurra en la mayoría de las circunstancias. | Al menos una (01) vez en el último año. |
| 3 | Posible | El evento podrá ocurrir en algún momento. | Al menos una (01) vez en los últimos dos (02) años. |
| 2 | Improbable | El evento puede ocurrir en algún momento. | Al menos una (01) vez en los últimos cinco (05) años. |
| 1 | Rara vez | El evento puede ocurrir solo en las circunstancias excepcionales (poco comunes o anormales) | No se han presentado en los últimos cinco (05) años. |

*Guía para la administración del riesgo y el diseño de controles en entidades públicas: riesgos de gestión, corrupción y seguridad digital* – versión 4 (2018) del Departamento Administrativo de la Función Pública

#### 3.3.1.3. ANÁLISIS DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se describen los criterios para calificar el impacto y la probabilidad de los riesgos de seguridad y privacidad de la información:

#### 3.3.1.4. TABLA DE IMPACTO – RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se adopta la siguiente tabla para calificar el impacto de los riesgos de seguridad y privacidad de la información:

| | Afectación a los activos de información | Calificación |
|---|---|---|
| Insignificante | El riesgo afecta Información que no tiene relevancia frente a la operación del Proceso. | 3 |
| Menor | El riesgo afecta el acceso a los Activos de Información de algún Proceso de la Entidad por automatización o errores humanos. | 6 |
| Moderado | El riesgo afecta los Activos de Información de la Entidad con efecto sobre la Integridad de la Información de la Entidad. | 9 |

| | Afectación a los activos de información | Calificación |
|---|---|---|
| Mayor | El riesgo afecta los Activos de Información de la Entidad con efecto sobre la Confidencialidad y la Integridad de la Información de la Entidad. | 12 |
| Catastrófico | El riesgo afecta los Activos de Información de la Entidad con efecto sobre la Confidencialidad, la Integridad y la Disponibilidad de la Información de la Entidad. | 15 |

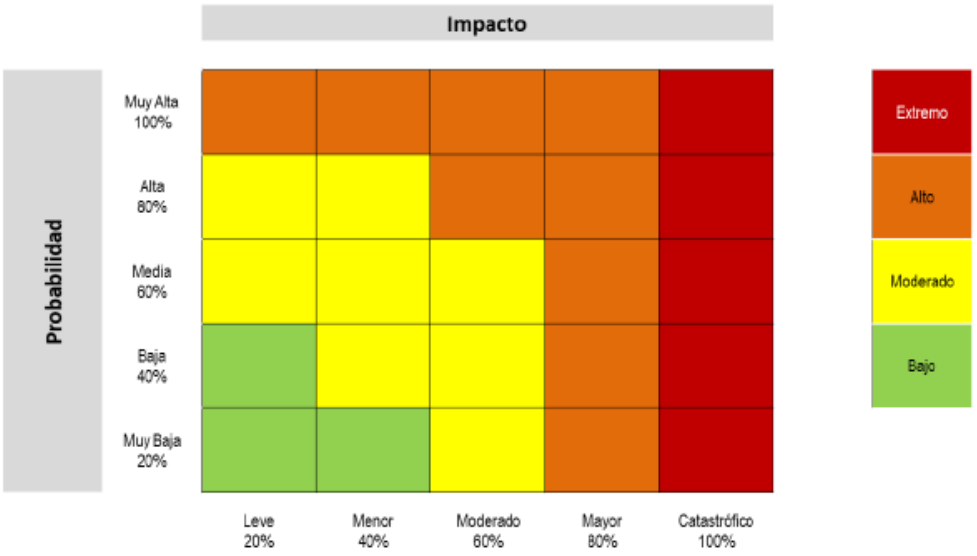
#### 3.3.1.5. TABLA DE PROBABILIDAD – RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se adopta la siguiente tabla para calificar la probabilidad de ocurrencia de los riesgos de seguridad y privacidad de la información:

| | Probabilidad de Afectación | Probabilidad |
|---|---|---|
| Raro | La afectación a la información no se presenta en las actividades del proceso y si se presenta no genera afectaciones en el logro de los Objetivos. | 1 |
| Improbable | La afectación a los Activos de información se presenta en las actividades del proceso sin generar afectaciones en el logro de los Objetivos. | 2 |
| Posible | La afectación a los Activos de información se presenta en las actividades del proceso generando afectaciones en el logro de los Objetivos. | 3 |
| Probable | La afectación a los Activos de información se presenta en las actividades del proceso generando afectaciones en el logro de los Objetivos y reprocesos en las actividades del Proceso. | 4 |
| Casi Seguro | La afectación a los Activos de información se presenta en las actividades del proceso generando afectaciones en el logro de los Objetivos y cese o paro de las actividades del Proceso. | 5 |

### 3.3.2. EVALUACIÓN DEL RIESGO

A partir del análisis de la probabilidad de ocurrencia y del impacto del riesgo, se determinará la zona de riesgo inicial, riesgo inherente o nivel de severidad, así:




Guía para la administración del riesgo y diseño de controles en entidades públicas v.6. (2022) Departamento Administrativo de la Función Pública.

Identificada la zona de riesgo inicial o el riesgo inherente, se valorarán los controles o medidas orientadas a la reducción o mitigación del riesgo, así:

- La identificación de controles se efectuará frente a cada riesgo, a través de entrevistas con los líderes de proceso o servidores expertos en su quehacer.
- Los líderes de proceso son los responsables de la implementación y monitoreo de los controles.

La redacción o descripción de los controles obedecerá la siguiente estructura:

- Responsable de ejecutar el control: identifica el cargo del servidore que ejecuta el control. En caso de que, en controles automáticos, se identificará el sistema que realiza la actividad.
- Acción: se determina mediante verbos que indican la acción que debe realizarse, como parte del control.
- Complemento: corresponde a los detalles que identifican claramente el objeto del control.

Las tipologías de controles aplicables, según su naturaleza, serán las siguientes:

- Control preventivo: control accionado en la entidad del proceso y antes de que se realice la actividad originadora del riesgo. Busca establecer las condiciones que aseguran el resultado final esperado.
- Control detectivo: control accionado durante la ejecución del proceso.
- Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo.

Las tipologías de controles aplicables, según la forma de su ejecución, serán las siguientes:

- Control manual: control ejecutado por personas.
- Control automático: control ejecutado por un sistema.

Para el análisis y evaluación de los controles, se tendrán en cuenta los siguientes atributos informativos y de eficiencia:

| Características | | | Descripción | Peso |
|---|---|---|---|---|
| Atributos de eficiencia | Tipo | Preventivo | Va hacia las causas del riesgo y asegura el resultado final esperado. | 25% |
| | | Detectivo | Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Puede generar reprocesos. | 15% |
| | | Correctivo | Permite reducir el impacto de la materialización del riesgo y tiene costos de implementación. | 10% |
| | Implementación | Automático | Son actividades de procesamiento o validación de información que se ejecutan por un sistema o aplicativo de manera automática, sin la intervención de personas. | 25% |

| Características | | | Descripción | Peso |
|---|---|---|---|---|
| | | Manual | Son actividades ejecutadas por personas y tienen implícito el error humano. | 15% |
| Atributos informativos | Frecuencia | Continua | El control se aplica siempre que se realiza la actividad que conlleva el riesgo. | No aplica |
| | | Aleatoria | El control se aplica aleatoriamente a la actividad que conlleva el riesgo. | No aplica |
| | Evidencia | Con registro | El control deja un registro que permite evidenciar su ejecución. | No aplica |
| | | Sin registro | El control no deja registro de su ejecución. | No aplica |

Adaptado de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6* (2022) del Departamento Administrativo de la Función Pública.

### 3.4. TRATAMIENTO

A continuación, se establece el tratamiento de los riesgos de gestión/por procesos, fiscales, de corrupción, de seguridad y privacidad de la información:

#### 3.4.1. RIESGO NO MATERIALIZADO

| Tratamiento | Descripción |
|---|---|
| Aceptar el riesgo | 1. No se adoptan medidas que afecten la probabilidad ni el impacto del riesgo. |
| Reducir o mitigar el riesgo | 1. Se diseñan e implementan controles específicos para disminuir la probabilidad o el impacto del riesgo. |

| Tratamiento | Descripción |
|---|---|
| | 2. Seguimiento cuatrimestral de los controles, a través de los responsables o líderes de proceso, y formulación de plan de tratamiento o plan de acción. |
| Evitar el riesgo | 1. Se abandonan o no se inician las actividades que provocan el riesgo. |
| Compartir o transferir el riesgo | 1. Se comparte o se transfiere el riesgo, para reducir su probabilidad o impacto. |

#### 3.4.1.1. RIESGO DE GESTIÓN/POR PROCESOS (DIFERENTE DEL RIESGO FISCAL)

A continuación, se establece el tratamiento de los riesgos de gestión/por procesos diferentes del riesgo fiscal:

| Nivel de riesgo residual | | Tratamiento |
|---|---|---|
| B | Nivel Bajo. | Aceptar el riesgo. |
| M | Nivel Moderado. | Aceptar o reducir el riesgo. |
| A | Nivel Alto. | Reducir, evitar, compartir o transferir el riesgo. |
| E | Nivel Extremo. | Reducir, evitar, compartir o transferir el riesgo. |

Los riesgos de gestión/por procesos (diferentes del riesgo fiscal) que deban tratarse mediante la alternativa de «reducir el riesgo» serán objeto de plan de acción, de acuerdo con la metodología y formatos de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6* (2022) del Departamento Administrativo de la Función Pública o el documento que haga sus veces:

| Plan de acción - riesgos de gestión/por procesos | | | | | |
|---|---|---|---|---|---|
| Plan de acción | Responsable | Fecha de implementación | Fecha de seguimiento | Seguimiento | Estado |
| - | - | - | - | - | - |

Adaptado de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6* (2022) del Departamento Administrativo de la Función Pública.

#### 3.4.1.2. RIESGO DE CORRUPCIÓN

A continuación, se establece el tratamiento de los riesgos de corrupción:

| Nivel de riesgo | | Tratamiento |
|---|---|---|
| B | Nivel de Riesgo Bajo. | Evitar, compartir o reducir el riesgo. |
| M | Nivel de Riesgo Moderado. | Evitar, compartir o reducir el riesgo. |
| A | Nivel de Riesgo Alto. | Evitar, compartir o reducir el riesgo. |
| E | Nivel de Riesgo Extremo. | Evitar, compartir o reducir (de forma prioritaria) el riesgo. |

Los riesgos de corrupción que deban tratarse mediante la opción de «reducir el riesgo» serán objeto de plan de tratamiento, de acuerdo con la metodología y formatos definidos en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas: riesgos de gestión, corrupción y seguridad digital* – versión 4 (2018) del Departamento Administrativo de la Función Pública o en el documento que haga sus veces:

| Plan de tratamiento de riesgos de corrupción | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Número | Riesgo | Clasificación | Causas | Probabilidad | Impacto | Riesgo residual | Opción de manejo | Actividad de control | Soporte | Responsable | Tiempo | Indicador |
| | | | | | | | | | | | | |

Adaptado de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas: riesgos de gestión, corrupción y seguridad digital* – versión 4 (2018) del Departamento Administrativo de la Función Pública

La Unidad Nacional de Protección, en el marco de la Red Interinstitucional de Transparencia y Anticorrupción de la Secretaría de Transparencia de la Presidencia de la República y la Vicepresidencia de la República, dispone de un canal especializado de denuncia para riesgos de corrupción: soytransparente@unp.gov.co

#### 3.4.1.3. RIESGO FISCAL

A continuación, se establece el tratamiento de los riesgos fiscales:

| Nivel de riesgo | | Tratamiento |
|---|---|---|
| B | Nivel Bajo | Reducir, evitar, compartir o transferir el riesgo. |
| M | Nivel Moderado | Reducir, evitar, compartir o transferir el riesgo. |
| A | Nivel Alto | Reducir, evitar, compartir o transferir el riesgo. |
| E | Nivel Extremo | Reducir (de forma prioritaria), evitar, compartir o transferir el riesgo. |

Los riesgos fiscales que se traten mediante la opción de «reducir el riesgo» serán objeto de plan de acción, de acuerdo con la metodología y formatos definidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6 (2022) del Departamento Administrativo de la Función Pública o en el documento que haga sus veces:

| Plan de acción - riesgos fiscales | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Número | Riesgo | Clasificación | Causas | Probabilidad | Impacto | Riesgo residual | Opción de manejo | Actividad de control | Soporte | Responsable | Tiempo | Indicador |
| | | | | | | | | | | | | |

Adaptado de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6* (2022) del Departamento Administrativo de la Función Pública.

### 3.4.1.4. RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se establece el tratamiento de los riesgos de seguridad y privacidad de la información:

| Nivel de riesgo | | Tratamiento |
|---|---|---|
| B | Nivel Bajo. | Aceptar el riesgo. |
| M | Nivel Moderado. | Aceptar, reducir el riesgo. |
| A | Nivel Alto. | Reducir, mitigar el riesgo. |
| E | Nivel Extremo. | Reducir (de forma prioritaria), evitar, *mitigar*, compartir o transferir el riesgo. |

En cumplimiento del artículo 2.2.22.3.14 del Decreto Único Reglamentario 1083 de 2015, la Unidad Nacional de Protección publicará, a más tardar el 31 de enero de cada vigencia fiscal, un plan de tratamiento de riesgos de seguridad y privacidad de la información; de acuerdo con la metodología, formatos y directrices definidos en el *Documento Maestro del Modelo de Seguridad y Privacidad de la Información* (2021), la *Guía de Identificación y Valoración de Riesgos de Seguridad de la Información* (GTE-GU-04), el *Manual Integral de Gestión de Riesgos* (GIN-MA-02) y en el *Plan de Seguridad y Privacidad de la Información* (GTE-PL-02).

### 3.4.2. MATERIALIZACIÓN

Ante la materialización de riesgos identificados en los mapas integrales de riesgos de la Entidad, los servidores públicos, contratistas o colaboradores responsables implementarán las acciones previstas en el Manual de Gestión Integral de Riesgos de la Entidad (GIN-MA-03) o el documento que haga sus veces y tendrán en cuenta los siguientes lineamientos, según la clasificación del riesgo:

#### 3.4.2.1. MATERIALIZACIÓN DE RIESGOS DE CORRUPCIÓN

Ante la materialización de riesgos de corrupción, procederán las siguientes acciones:

1. La Primera Línea de Defensa reportará la materialización del riesgo de corrupción a la Alta Dirección, a la Oficina Asesora de Planeación e Información y a la Oficina de Control Interno; y anexará el informe de los hechos y los soportes del presunto evento.
2. La Primera Línea de Defensa pondrá en conocimiento de la Oficina de Control Interno Disciplinario la ocurrencia del presunto hecho de corrupción.
3. La Línea Estratégica informará a las autoridades competentes (fiscalía general de la Nación, Contraloría General de la República o Procuraduría General de la Nación, entre otros) de la ocurrencia del presunto hecho de corrupción.
4. Revisión y actualización de los mapas integrales de riesgos, con énfasis en las causas y controles del riesgo materializado. En caso de que el riesgo de corrupción no se haya identificado previamente, se garantizará su inclusión en el mapa integral de riesgos correspondiente, en un plazo máximo de siete (07) días hábiles, contados a partir de la materialización del riesgo.
5. Formulación e implementación de los planes de acción correspondientes a cada riesgo materializado.
6. Seguimiento y evaluación de los planes de tratamiento de riesgos de corrupción.

7. Los riesgos materializados no pueden retirarse del mapa de riesgos y su gestión será prioritaria.

#### 3.4.2.2. MATERIALIZACIÓN DE RIESGOS DE GESTIÓN/POR PROCESOS Y FISCALES

Ante la materialización de riesgos de gestión/por procesos o fiscales, procederán las siguientes acciones:

1. Reportar la materialización del riesgo a la Oficina Asesora de Planeación e Información y a la Oficina de Control Interno.
2. Realizar el análisis de causas y determinar acciones correctivas y de mejora, inmediatamente después de la materialización del riesgo. Este análisis se deberá realizar en un plazo que no supere los siete (07) días hábiles, contados a partir de la materialización del riesgo.
3. Revisar y actualizar el mapa integral de riesgos, en particular las causas y controles diseñados para el control del riesgo materializado. Si el riesgo no está identificado, se adelantará el proceso necesario para que este ingrese al mapa integral de riesgos. Estos ajustes se deberán realizarse y reportarse en un plazo que no supere los siete (07) días hábiles, contados a partir de la materialización del riesgo.
4. Formular e implementar los planes de acción correspondientes a cada riesgo materializado.
5. Intensificar y hacer seguimiento permanente a los planes de acción y controles.
6. Los riesgos materializados no pueden retirarse del mapa de riesgos y su gestión será prioritaria.

#### 3.4.2.3. MATERIALIZACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Ante la materialización de riesgos de seguridad y privacidad de la información, procederán las siguientes acciones:

1. Reportar la materialización del riesgo a las Oficinas Asesoras de Planeación e Información y de Control Interno, dando a conocer los Activos afectados o la pérdida de Información encontrada.
2. Determinar la afectación que se presentó, ya sea a la Confidencialidad, a la Integridad o a la Disponibilidad de la información; para realizar los análisis de causas, identificar la causa raíz y determinar las acciones correctivas que se deban desarrollar inmediatamente después de la materialización del riesgo. Este análisis se deberá realizar en un plazo que no supere los siete (07) días hábiles, contados a partir de la materialización del riesgo.
3. Verificar la afectación sobre los controles implementados, para reestructurarlos o implementar nuevos controles, en caso de considerarse necesario.

4. Revisar y actualizar el mapa integral de riesgos, en particular las causas y controles diseñados para el control del riesgo materializado Si el riesgo no está identificado, se adelantará el proceso necesario para que este ingrese al mapa integral de riesgos. Estos ajustes se deberán realizarse y reportarse en un plazo que no supere los siete (07) días hábiles, contados a partir de la materialización del riesgo.
5. Formular e implementar los respectivos planes de acción por cada riesgo materializado.
6. Hacer seguimiento permanente de los planes de acción y de la restitución de los activos afectados.
7. Los riesgos materializados no pueden retirarse del mapa de riesgos y su gestión será prioritaria.

## CAPÍTULO 4

SEGUIMIENTO, MONITOREO Y ACTUALIZACIÓN

A continuación, se determinan las actividades y responsabilidades para el seguimiento, monitoreo y actualización de la Política Integral de Administración de Riesgos.

### 4.1. SEGUIMIENTO Y MONITOREO

El seguimiento y monitoreo de la gestión integral del riesgo se enmarcará en los siguientes roles:

| | |
|---|---|
| Primera línea de defensa | Monitoreo y seguimiento permanente de los controles y de planes de tratamiento o planes de acción. |
| Segunda línea de defensa | Monitoreo y seguimiento de las etapas de la gestión del riesgo, para garantizar el correcto diseño y funcionamiento de los controles y mecanismos institucionales de gestión de riesgos, |
| Tercera línea de defensa | Evaluación de la efectividad de los controles y documentación de los resultados o de la creación, modificación o eliminación de riesgos. |

El seguimiento y evaluación de los mapas de riesgos operativos y de riesgos de seguridad y privacidad de la información se realizará así:

- Primera Línea de Defensa: monitoreo permanente de los controles y del cumplimiento a los planes de acción.
- Segunda Línea de Defensa: monitoreo al cumplimiento de las etapas de la gestión del riesgo, junto con el aseguramiento del diseño y

funcionamiento apropiado de los controles que implementa la primera línea de defensa.

- Tercera Línea de Defensa: evaluación de la efectividad de los controles (riesgos operativos y riesgos de seguridad y privacidad de la información) en períodos cuatrimestrales, con corte el 30 de abril, el 31 de agosto y el 31 de diciembre de cada vigencia fiscal. Conforme a lo anterior, la Tercera Línea de Defensa elaborará un informe cuatrimestral que documente los resultados de la evaluación de la efectividad de los controles y que consigne, cuando sea el caso, la materialización, creación, modificación o eliminación de un riesgo; de acuerdo con los mapas de riesgos y los riesgos de procesos.

### 4.2. REVISIÓN Y ACTUALIZACIÓN

La Política Integral de Administración Riesgos será objeto de revisión, como mínimo, una vez cada año y, de ser necesario, se realizarán los ajustes correspondientes, de acuerdo con el nuevo contexto de la Entidad o conforme a la existencia de nuevos escenarios, situaciones o circunstancias que puedan impactar su operación.