TABLA DE CONTENIDO

Listado de imágenes

Listado de tablas

1. OBJETIVOS

Definir los lineamientos generales de la administración de riesgos de la Unidad, que guíen el accionar de los funcionarios, en el tratamiento de los riesgos de gestión, corrupción, seguridad de la información y fiscales.

2. DESARROLLO

Con el propósito de continuar con la implementación de la mejora permanente relacionada con la Administración del Riesgo en la UAECD, se ha elaborado esta metodología para dar claridad sobre las etapas en la gestión del riesgo que se deben abordar por cada uno de los responsables de procesos, la cual considera lo establecido en el Modelo Integrado de Planeación y Gestión MIPG, alcance, la normatividad aplicable y la Guía para la administración del riesgo y el diseño de controles en entidades públicas, del Departamento Administrativo de la Función Pública –DAFP, versión 6 de 2022.

A. CONSIDERACIONES GENERALES

ALCANCE DE LA METODOLOGÍA DE RIESGOS

Esta metodología aplica para riesgos de gestión, corrupción, seguridad de la información y fiscales.

Para temas asociados a Seguridad y salud en el trabajo, Continuidad de negocio, Contratación, Proyectos de inversión, la gestión de riesgos deberá desarrollarse de acuerdo con los lineamientos normativos y legales específicos aplicables.

En el Modelo Integrado de Planeación y Gestión -MIPG, en la Política de Planeación institucional de la dimensión Direccionamiento Estratégico y Planeación se indica que la entidad debe definir los posibles riesgos asociados al cumplimiento de las prioridades y establecer los controles para su mitigación.

MARCO NORMATIVO GESTIÓN DEL RIESGO

A continuación, se presenta un marco de referencia asociado a la gestión del riesgo.

Tabla 1. Normatividad relevante

SISTEMA	REGULACIÓN	OBSERVACIÓN
Gestión de	ISO 9001 – 2015	Sistemas de Gestión de la Calidad – Requisitos

Calidad	Ley 1753 de 2015, artículo 133	"Intégrense en un solo Sistema de Gestión, los Sistemas de Gestión de la Calidad de que trata la Ley 872 de 2003 y de Desarrollo Administrativo de que trata la Ley 489 de 1998. El Sistema de Gestión deberá articularse con los Sistemas Nacional e Institucional de Control Interno consagrado en la Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998, de tal manera que permita el fortalecimiento de los mecanismos, métodos y procedimientos de control al interior de los organismos y entidades del Estado. El Gobierno Nacional reglamentará la materia y establecerá el modelo que desarrolle la integración y articulación de los anteriores sistemas, en el cual se deberá determinar de manera clara el campo de aplicación de cada uno de ellos con criterios diferenciales en el territorio nacional."
	Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Control Interno	Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones
	Decreto 1499 de 2017 y en el Manual Operativo del MIPG	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
	Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
Seguridad de la información	NTC/ISO/IEC 27.001 de 2013	Sistema de Gestión de seguridad de la información.
	Norma ISO 31000:2011	Gestión del riesgo – principios y directrices.
	Norma ISO 27005:2011	Gestión del riesgo en la seguridad de la información.
	Documento CONPES 3854 de 2017	Política Nacional de Seguridad Digital
	Ley estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentado por el Decreto 1377 de 2013.
	CONPES 3854 del 11 de abril de 2016, 3.2. Estrategia de gestión de riesgos de seguridad digital	El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará un modelo de gestión de riesgos de seguridad digital, teniendo en cuenta el marco.

	Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de gobierno digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 del 2015, decreto único reglamentario del sector de tecnologías de la información y las telecomunicaciones.
Corrupción	Ley 1474 de 2011	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". En su Art. 73 establece la obligatoriedad.
	Decreto 124 de 2016	Por el cual se sustituye el Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano.
	Ley 2195 de 2022	Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones. Programa de transparencia y ética pública en el sector público

Fuente: Oficina Asesora de Planeación y Aseguramiento de Procesos -OAPAP y Gerencia de Tecnología - GT.

TÉRMINOS Y DEFINICIONES

Tomados de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, versión 6, el documento CONPES 3854 de 2017.

- **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.
- **Activo cibernético:** En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Amenaza cibernética:** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).
- **Análisis del riesgo:** Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).
- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Ataque cibernético:** Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).

- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:
  a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.
  b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.
- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la Entidad.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata), pero se asocia a la misma causa inmediata.
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
  Causa Raíz (Causa Eficiente o Causa Adecuada): Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.
- **CCOC:** Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.
- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
  Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **Fraude:** Acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.
- **Gestión del riesgo:** Un 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.
- **Gestión del Riesgo Fiscal:** son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto

dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

- **Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales". A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.
- **Gestor Fiscal:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)". A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.
- **ICC:** Infraestructura Crítico Cibernético son las infraestructuras estratégicas soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO) cuyo funcionamiento es indispensable por lo que su perturbación o destrucción tendría un grabe impacto sobre los servicios esenciales.
- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** Propiedad de exactitud y completitud.
- **Intereses patrimoniales de naturaleza pública:** Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.
- **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras

maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

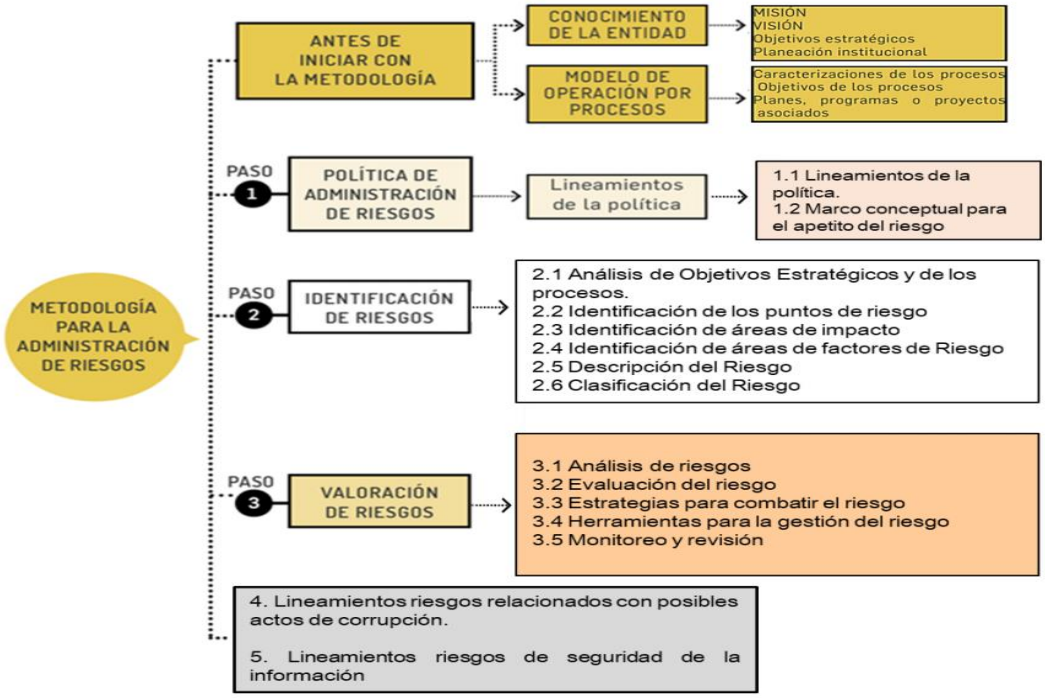
- **Patrimonio público:** conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C340-07)
- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Recurso público:** Los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de fraude:** Efecto que se causa sobre los objetivos de las entidades debido a una acción de engaño intencional, que un servidor público o particular con funciones públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.
- **Riesgo fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **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 de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad
- **Riesgo residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Servicios esenciales:** son los necesarios para el mantenimiento de las funciones sociales básicas la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del estado y las administraciones públicas.
- **Tolerancia al riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Tratamiento al riesgo:** es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

B. METODOLOGÍA DE RIESGOS

ETAPAS DE LA GESTIÓN DE RIESGO

La Unidad Administrativa Especial de Catastro Distrital –UAECD- ejecutará las etapas de la Gestión del Riesgo teniendo en cuenta como buena práctica, la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública –DAFP, versión 6.

Imagen 1. Proceso para la Gestión del Riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v.6.

Antes de iniciar con la metodología es importante tener claridad sobre el modelo de operación por procesos (cadena de valor, mapa de procesos, caracterizaciones y objetivos de los procesos) y la planeación estratégica (misión, visión, objetivos estratégicos, planeación institucional).

1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Como primer paso en la aplicación de la metodología, se define una Política para la administración del riesgo, la cual es aprobada por la Alta Dirección en el Comité Institucional de Coordinación de Control Interno de la Unidad.

1.1. Descripción de la política

La Unidad Administrativa Especial de Catastro Distrital se compromete a dar tratamiento, manejo y seguimiento de los riesgos de gestión, corrupción, de seguridad de la información y fiscales, que puedan afectar de manera negativa el alcance de los objetivos estratégicos y los objetivos de procesos de la cadena de valor; cuya gestión se realizará bajo la metodología y procedimiento de la gestión del riesgo del Proceso de Direccionamiento estratégico, acorde con lo establecido por el Departamento Administrativo de la Función Pública en su Guía para la administración del riesgo y el diseño de controles en entidades públicas.

La entidad también se compromete a gestionar otro tipo de riesgos como los de Seguridad y salud en el trabajo, Continuidad de negocio, Contratación, Proyectos de inversión, desarrollando su gestión de acuerdo con los lineamientos normativos y legales específicos aplicables.

En el marco del cumplimiento de esta Política, se integran o adoptan los roles y responsabilidades sobre Gestión de los riesgos institucionales que establece el Modelo Integrado de Planeación y Gestión – MIPG.

1.2. Objetivos de la política

La Política de Administración del Riesgo de la UAECD y sus objetivos descritos a continuación, brindan el marco general de actuación para gestionar los riesgos a un nivel aceptable y proporcionar a la administración un aseguramiento razonable con respecto al logro de sus objetivos estratégicos y de procesos.

Objetivos:

- Contribuir a la eficiencia operacional mediante la mitigación de probabilidad e impacto de eventos adversos.
- Gestionar de forma anticipada las vulnerabilidades o eventos que puedan afectar el logro de los objetivos organizacionales.
- Aportar información para tomar adecuadas decisiones estratégicas y operativas.
- Fortalecer la mejora continua en la gestión de los procesos y en general del Sistema de Control Interno.
- Brindar un marco en el que se identifiquen las amenazas y vulnerabilidades a las que puede estar expuesta la entidad desde la perspectiva de un entorno digital y se fortalezca el ambiente de control.
- Reprobar y combatir la corrupción por parte de cada uno de los servidores públicos que pertenecen a la Unidad, que afecte el logro de los objetivos de la entidad, socave el Estado de Derecho, distorsione el efecto de las políticas gubernamentales, quebrante la legitimidad del gobierno, desestimule la participación ciudadana y propicie escenarios de politización y de captura de la entidad por parte de intereses particulares.

1.3. Alcance

Esta política y metodología específica establece la intención general de la Unidad respecto al manejo de riesgos de gestión, corrupción, seguridad de la información y fiscales, con el fin que se realicen las actividades necesarias iniciando con la identificación de los factores externos e internos hasta realizar el tratamiento de los riesgos y seguimiento a las actividades de control definidas en cada uno de los procesos de la entidad. Es aplicable a todos los procesos de la entidad en materia de gestión de riesgos.

1.4. Roles y responsabilidades

La definición de los roles y responsables de la gestión del riesgo en la entidad parten de lo definido por el Modelo Integrado de Planeación y Gestión – MIPG en su Manual Operativo[1] del cual se destacan:

Línea Estratégica – Alta dirección, Comité Institucional de Gestión y Desempeño, Comité Institucional de Coordinación de Control Interno:

Esta línea define y aprueba la Política de Administración del Riesgo en el marco del Comité Institucional de Coordinación de Control Interno, realizando el monitoreo correspondiente a partir de la información suministrada por la segunda línea.

"La responsabilidad de esta línea de defensa se centra en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad."

Primera línea de defensa – Líderes de programas, procesos y proyectos y sus equipos de trabajo (en general servidores públicos en todos los niveles):
"Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos."

Segunda línea de defensa – Jefe de la Oficina Asesora de Planeación, coordinadores de equipos de trabajo que respondan de manera directa por el aseguramiento de la operación, Oficial de Seguridad de la Información:

"Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos."

En términos generales para los riesgos de gestión, corrupción, fiscales, seguridad de la información y para otro tipo de riesgos como los enunciados en la declaración de la Política de riesgos, la segunda línea es:

[1] Manual Operativo del Modelo Integrado de Planeación y Gestión versión 5.

Tabla 2. Resumen de responsables de segunda línea

Tema o tipo de riesgo	**Segunda línea**
Gestión	Oficina Asesora de Planeación y Aseguramiento de Procesos
Corrupción	Oficina Asesora de Planeación y Aseguramiento de Procesos
Fiscales	Oficina Asesora de Planeación y Aseguramiento de Procesos
Seguridad de la Información	Gerencia de Tecnología – Oficial de Seguridad
Otros riesgos	
Seguridad y salud en el trabajo	Subgerencia de Talento Humano
Continuidad de negocio	Gerencia de Tecnología – Oficial de Continuidad
Contratación	Subgerencia de Contratación - Supervisores
Proyectos de inversión	Oficina Asesora de Planeación y Aseguramiento de Procesos

Fuente: Oficina Asesora de Planeación y Aseguramiento de Procesos -OAPAP

Tercera línea de defensa – Jefe Oficina de Control Interno:
"evalúan de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos -y los que inadecuadamente son cubiertos por la 2ª línea de defensa"

Asimismo, el Anexo No 4 Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas señala las responsabilidades del funcionario designado para Seguridad Digital, en concordancia con lo establecido por el Ministerio de Tecnologías de la información y las comunicaciones, la Unidad delegará la responsabilidad de gestionar los riesgos de seguridad de la información al encargado de seguridad de la información con los siguientes compromisos:

"Responsable de seguridad de la información:

- *Actualizar el procedimiento para la Identificación y Valoración de Activos de la Entidad, de acuerdo a los criterios de seguridad de la información (Confidencialidad, integridad y disponibilidad).*
- *Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento).*
- *Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.*
- *Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.*
- *Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información."*[2]

1.5. Lineamientos para la gestión del riesgo

La implementación de la Gestión del Riesgo en la entidad cumple con las etapas de la Gestión del Riesgo a saber: Política de administración de riesgos, Identificación de riesgos y Valoración de riesgos.

[2] Anexo 4. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.

En relación con los riesgos de seguridad de la información, estos se definirán a partir de los activos de información identificados con criticidad alta y aquellos identificados como Infraestructura Crítico Cibernética (ICC). El responsable del proceso podrá incorporar en su mapa, riesgos sobre activos de información con criticidad diferente a alta.

Riesgos asociados a proyectos en territorio

En desarrollo de la facultad dada a la entidad para prestar el servicio público de gestión y operación catastral multipropósito en cualquier lugar del territorio nacional, cuando sea contratada para ello, se pueden generar riesgos que la entidad debe abordar.

Por un lado, al ser proyectos constituidos como parte de un compromiso contractual, estos deberán incorporar los lineamientos que sobre riesgos en contratación defina el ente rector, Colombia Compra Eficiente.

De igual forma, si estos hacen parte de proyectos de inversión, este último debe en su formulación contemplar la identificación de riesgos según la metodología o lineamientos que para ello determinan las autoridades de planeación distrital y/o nacional.

Por otra parte, al ser parte de la cadena de valor de la Unidad, puede contemplar riesgos propios de la gestión de procesos determinados en esta metodología, para lo cual:

- En la identificación del contexto y dependiendo de los proyectos en curso durante una vigencia, se podrán precisar o identificar aquellos elementos de factores internos o externos que puedan generar riesgos a la ejecución del proyecto.
- De ser requerido podrán generarse riesgos específicos diferenciados de la gestión de Bogotá.
- En la identificación y valoración de los controles que se encuentran documentados en los procedimientos e instructivos, el proceso asociado deberá contemplar aquellos controles aplicables a la gestión de territorio que permitan mitigar los riesgos identificados.
- En la formulación de planes de tratamiento se deberán proponer actividades que mitiguen riesgos y se ejecuten desde el territorio.

Para riesgos de proceso teniendo en cuenta que los proyectos en territorio son temporales y dependen de los contratos que se suscriban, los riesgos que se identifiquen en los mapas de riesgos estarán sujetos a esta temporalidad y a los objetos contractuales, por ejemplo, si en una vigencia no se tuviera operación en territorio no se tendrían riesgos asociados en el mapa, o si no se tuvieran contratos para la actualización catastral en territorio no aplicarían riesgos de la actualización.

Por otra parte, teniendo en cuenta que la mitigación de riesgos se promueve a partir de un adecuado ejercicio de planeación, es importante que desde la elaboración de las propuestas económicas y con la posterior planeación de cada uno de los proyectos, se tengan en cuenta factores del contexto como los sociales, culturales, económicos, políticos, legales, ambientales y organizacionales que puedan afectar su

ejecución y de igual forma, se promueva el seguimiento permanente a la ejecución de los proyectos, sus cronogramas internos de trabajo y la entrega de los productos pactados contractualmente.

Niveles de calificación de probabilidad e impacto

Los criterios para la valoración de los riesgos en relación con los niveles para calificar los aspectos de probabilidad e impacto serán los definidos en las tablas de valoración consignadas en el numeral 3.1.

Tratamiento de los riesgos

El tratamiento de los riesgos de gestión y de seguridad de la información tendrá tres escenarios posibles: reducir, aceptar y evitar. El tratamiento a los riesgos de corrupción y fiscales sólo tendrá dos escenarios posibles que corresponden a reducir o evitar el riesgo.

El seguimiento de los Planes de Manejo de Riesgo – PMR que permiten dar tratamiento a los riesgos residuales se realizará con periodicidad trimestral.

En relación con los riesgos de corrupción, su formulación y seguimiento seguirán los lineamientos que sobre la materia establezcan el Gobierno Nacional y Distrital.

En el caso de los riesgos de seguridad de la información, estos se gestionan siguiendo los lineamientos para la gestión de riesgos en entidades públicas, basados en el Modelo de Seguridad y Privacidad de la Información, la Guía de orientación para la gestión de riesgos de seguridad digital en el Gobierno Nacional, territoriales y sector público y el Modelo de Gestión de Riesgos de Seguridad Digital, del Ministerio de Tecnologías de la Información y las Comunicaciones.

La materialización del riesgo de corrupción en la UAECD obliga a todos y cada uno de los servidores públicos y contratistas de la Unidad a:

- Comunicar a las autoridades competentes la ocurrencia del hecho.
- Comunicar al superior inmediato del servidor público y supervisor del contrato en caso de contratista, la ocurrencia del hecho.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- Monitorear permanentemente los riesgos.

1.6. Niveles de aceptación del riesgo

La Unidad generará planes de tratamiento o manejo para los riesgos residuales ubicados en zonas de niveles: extremo, alto y moderado. Sobre los riesgos ubicados en zona baja pese a no generar plan de manejo del riesgo – PMR, trimestralmente se deberá identificar si se presentó o no materialización identificando si requiere realizar ajustes o mejoras.

Los riesgos de corrupción no admiten aceptación del riesgo, siempre debe conducir a realizar el tratamiento correspondiente.

1.7. Comunicación y consulta de la política

Esta política es aprobada por la Alta dirección en el Comité Institucional de Coordinación de Control Interno y seguirá el trámite de gestión de documentos que establece el Manual del Sistema de Gestión Integral del proceso Direccionamiento Estratégico, por esta razón, se encontrará disponible para consulta a través del Sistema de Gestión Integral –SGI-; también se publica para consulta en la página web de la Unidad.

2. IDENTIFICACIÓN DEL RIESGO

En la identificación del riesgo se tiene en cuenta el contexto estratégico en que opera la entidad, los objetivos y alcance de los procesos y los factores internos y externos del proceso a partir de un análisis de contexto específico con factores que representen una amenaza o una oportunidad y factores en los que la entidad tiene debilidades o fortalezas.

Como punto de partida se tomarán los objetivos estratégicos y los objetivos de los procesos, para identificar los posibles riesgos que afectan su cumplimiento y que estén adecuadamente formulados.

Asimismo, en la formulación de riesgos se tienen en cuenta la identificación de puntos de riesgo, es decir aquellas actividades o momentos del proceso en donde existe evidencia o indicios de situaciones que pueden generar riesgo y deben mantenerse bajo control.

Como insumo para el análisis también se podrá tomar de referente información proveniente de fuentes como auditorías internas y externas (planes de mejoramiento), necesidades y expectativas de los grupos de valor, entre otros.

2.1. Descripción del riesgo

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso.

Inician con la frase “Posibilidad de” ya que son eventos potenciales.

Dentro de las recomendaciones para la redacción del riesgo dadas por el DAFP, se tienen:

- No describir como riesgos omisiones ni desviaciones del control. Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.
- No describir causas como riesgos. Ejemplo: Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

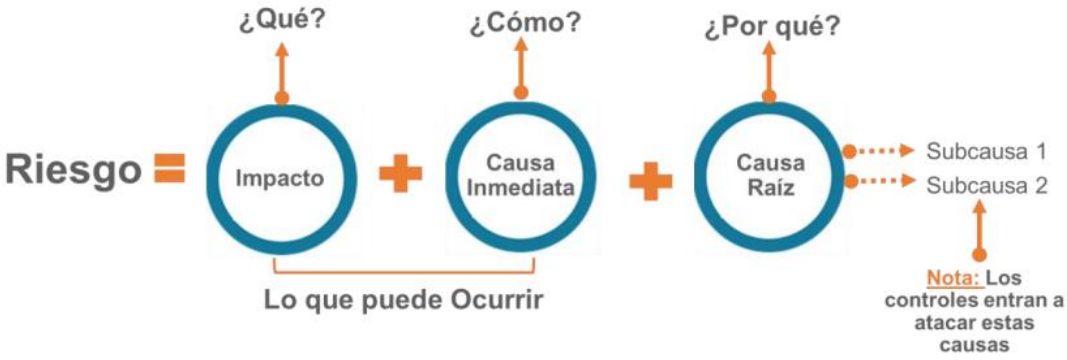
- No describir riesgos como la negación de un control. Ejemplo: Retrasos en la prestación del servicio por no contar con digiturno para la atención.
- No existen riesgos transversales, lo que pueden existir son causas transversales. Ejemplo: Pérdida de expedientes. Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

2.2. Riesgos de gestión

En la formulación de los riesgos de gestión es necesario partir de identificar los productos del proceso relacionados en la Caracterización, a partir de ellos identificar en cuál(es) pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo. En el producto se identifica el problema central y a partir de allí causas y efectos o consecuencias.

Para los riesgos de gestión la estructura propuesta por DAFP es:

Imagen 2. Estructura propuesta por DAFP para la redacción del riesgo de gestión



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v.6.

En la descripción de los riesgos de gestión se deben identificar las consecuencias económicas o reputacionales a las que se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional o ambas.

Indicador clave de riesgo (riesgos de gestión)

Una vez formulados los riesgos de gestión, teniendo en cuenta el problema central o evento de riesgo, se establece un indicador que permita controlar el evento de riesgo y facilite la identificación de una materialización.

A través del monitoreo de este indicador podrá identificarse si se presenta o no la materialización del riesgo.

2.3. Riesgos fiscales

Para identificar el riesgo fiscal:

- Identificar puntos de riesgo que son situaciones/actividades en las que potencialmente se genera riesgo fiscal, actividades sobre los bienes, recursos o patrimonio en donde potencialmente hay riesgo.

Para ello, es importante analizar en qué procesos se realiza gestión fiscal (actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado).

Para identificar los procesos se toma como base el análisis de advertencias, alertas, hallazgos o fallos con responsabilidad fiscal en firme relacionados con la entidad de los últimos 5 años.

Por lo anterior, en la fase de identificación del riesgo es importante realizar la consulta de los planes de mejoramiento de la Contraloría de Bogotá u otros documentos en los que se hayan encontrado hallazgos y/o fallos con responsabilidad fiscal de los últimos años.

- Identificar las circunstancias inmediatas, es decir, las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o fallos y/o advertencias de la oficina de control interno de los últimos 5 años.

Para lo anterior es importante también la consulta como apoyo del Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas de la Guía DAFP para identificar cuáles de ellas pueden ser aplicables a la entidad.

La identificación de los riesgos fiscales apoya la adecuada gestión de los recursos, bienes e intereses públicos, previniendo efectos dañosos y mitigando la configuración de responsabilidades fiscales.

El riesgo fiscal se define por el DAFP como un: “Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.”

Entendiendo el efecto como un daño que se generaría sobre los recursos, bienes, intereses patrimoniales en caso de ocurrir un evento potencial (acción u omisión que podría generar daño).
Los riesgos fiscales se relacionan con tres expresiones según DAFP: bienes públicos, recursos públicos e intereses patrimoniales de naturaleza pública:

“Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales.

a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.
b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

Recurso público: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.
Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal."

- Identificar la afectación

Para los riesgos fiscales el área de impacto siempre es económica.

No todos los riesgos con afectación económica son fiscales por lo que se requiere realizar el análisis, por ejemplo, riesgos como los de daño antijurídico (pago de condenas y conciliaciones) y aquellos generados por causas exógenas no relacionadas con acción u omisión de los gestores públicos, que son hechos de fuerza mayor, caso fortuito o hecho de un tercero.

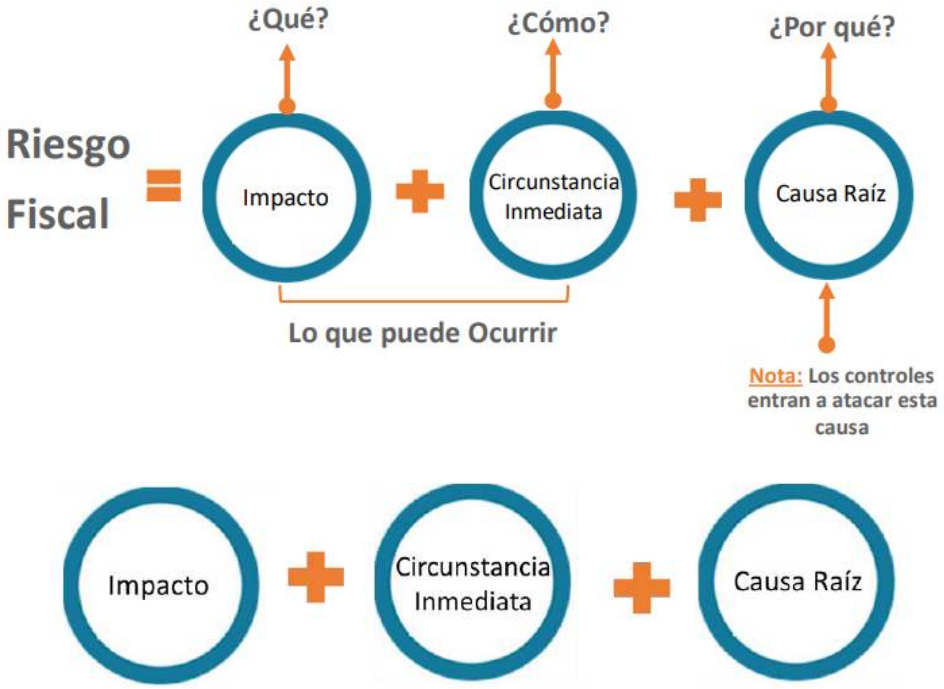
- Identificar la causa raíz o potencial hecho generador

Según la Auditoría General de la República la causa raíz es cualquier evento potencial (acción u omisión) que de presentarse provocaría menoscabo, disminución, perjurio, detrimento, pérdida o deterioro.

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. Los controles deben apuntar a atacar esta causa.

Para los riesgos fiscales la estructura propuesta por DAFP es:

Imagen 3. Estructura propuesta por DAFP y ejemplos para la redacción del riesgo fiscal



¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre **bienes públicos**	por pérdida, extravío o hurto de bienes muebles de la entidad.	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato.
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo, a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v.6.

En el formato de matriz de riesgos se cuenta con un árbol de problemas como apoyo en la identificación de los riesgos de gestión, fiscales y de corrupción.

Para el caso de riesgos fiscales si bien no les aplica indicador clave, deberán tener un indicador para la gestión del proceso que se relacione con el riesgo y que complemente el seguimiento y control.

2.4. Riesgos de seguridad de la información

Identificación de activos de seguridad de la información

Como punto de partida para los riesgos de seguridad de la información se tendrán los activos de información.

La identificación de los activos de seguridad de la información corresponde a la primera línea de defensa y se realizará según lo descrito en el documento asociado a la Gestión de Activos en el Marco de la Seguridad de la Información.

Los activos en un contexto de seguridad digital son elementos como: Aplicaciones, servicios web, redes, información física o digital, tecnologías de la información, tecnologías de operación, que utiliza la

entidad para funcionar en un entorno digital. Al realizar una identificación de activos se puede saber qué proteger para garantizar su funcionamiento y con ello aumentar la confianza ciudadana.
Para la formulación de riesgos de seguridad de la información se debe partir de la identificación de los activos de información que fueron identificados con criticidad alta y aquellos activos identificados como Infraestructura Crítico Cibernética (ICC). El responsable del proceso podrá incorporar en su mapa, riesgos sobre activos de información con criticidad diferente a alta.

En el evento de presentarse un incidente de seguridad sobre un activo o grupo de activos de información se debe tener presente lo siguiente:

a. Si el activo o grupo de activos no se encuentran identificados en el inventario general de activos o instrumento de gestión de la información pública es necesaria la actualización de estos, su valoración y su correspondiente análisis de riesgos.
b. Si no existe ningún riesgo asociado con el incidente presentado es necesario incluir el riesgo actualizando la matriz de riesgos del proceso.

Para cada activo o grupo de activos de información se podrán identificar los siguientes tres riesgos inherentes de seguridad digital: Pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos.

Para los riesgos de seguridad de la información se tomará como guía para la identificación de amenazas y vulnerabilidades lo descrito en el anexo C y Anexo D de la ISO27005:2009 las cuales se presentan al final de este documento como anexos y en donde se definen los ejemplos más comunes de amenazas y vulnerabilidades que pueden afectar un activo de información.

Se aclara que se pueden identificar amenazas y vulnerabilidades que no se encuentren asociadas en las tablas anteriormente mencionadas.

Se recomienda realizar la identificación de hasta 3 amenazas por grupo de activos de información; y para cada amenaza hasta 3 vulnerabilidades asociadas.

La descripción de riesgos de seguridad de la información parte de la identificación de los tres siguientes riesgos:

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

En la descripción de los riesgos de seguridad de la información se deben identificar las consecuencias económicas o reputacionales a las que se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

2.5. Riesgos de corrupción

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

En la definición de los riesgos debe presentarse:

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

de esta forma, se pueden evitar las confusiones entre riesgos de gestión y corrupción.

La formulación inicial de los riesgos de corrupción debe ser socializada a servidores públicos y ciudadanía en general para recibir su retroalimentación. Los resultados y recomendaciones deben publicarse.

El mapa de riesgos de corrupción deberá ser publicado en la página web de la entidad antes del 31 de enero de cada año.

En la formulación de riesgos de corrupción se tendrá en cuenta la identificación de áreas con riesgo de conflictos de interés y la definición de riesgos y controles asociados.

También se tendrá en cuenta la asociación de riesgos de corrupción a los trámites prestados por la entidad.

3. VALORACIÓN DEL RIESGO

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial o inherente.

3.1. Análisis del riesgo

Busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, lo cual permite establecer la zona de Riesgo Inherente.

3.1.1 Determinar la probabilidad

Para los riesgos de gestión, seguridad de información y fiscales, la probabilidad es la posibilidad de ocurrencia del riesgo y está asociada a la exposición al riesgo, del proceso o actividad que se está analizando.

La probabilidad está dada al evaluar con qué frecuencia se realiza la actividad que conlleva el riesgo por año, es decir, con base en el producto/activo seleccionado identificar con qué frecuencia se genera.

A continuación, se presentan los Criterios para definir el nivel de probabilidad de los riesgos de gestión, seguridad de la información y fiscales:

Imagen 4. Criterios para definir la probabilidad – Riesgos de gestión, seguridad de la información y fiscales

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad/producto/activo que conlleva el riesgo se ejecuta/genera como máximos 2 veces por año.	20%
Baja	La actividad/producto/activo que conlleva el riesgo se ejecuta/genera de 3 a 24 veces por año.	40%
Media	La actividad/producto/activo que conlleva el riesgo se ejecuta/genera de 24 a 500 veces por año.	60%
Alta	La actividad/producto/activo que conlleva el riesgo se ejecuta/genera mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy Alta	La actividad/producto/activo que conlleva el riesgo se ejecuta/genera más de 5000 veces por año.	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v.6. DAFP con ajustes propios

Para los riesgos de corrupción se analiza qué tan posible es que ocurra el riesgo, se expresa en criterios 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.

Para los riesgos de corrupción la tabla para definir los criterios de probabilidad es la siguiente:

Tabla 3. Escala o calificación de la probabilidad - Riesgos de corrupción

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v.4. DAFP

3.1.2. Análisis del impacto

Para los riesgos de gestión y seguridad de la información, las variables principales de análisis son los impactos económicos y reputacionales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se toma el nivel más alto.

Para los riesgos fiscales el impacto siempre es económico.

A continuación, se presentan los Criterios para definir el nivel de impacto:

Imagen 5. Criterios para definir el impacto – Riesgos de gestión, seguridad de la información y fiscal

	Afectación Económica (o presupuestal)	Pérdida Reputacional	Impacto
Leve	Afectación menor a 100 SMLMV	El riesgo afecta la imagen de alguna área de la organización	20%
Menor	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	40%
Moderado	Entre 500 y 1000 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	60%
Mayor	Entre 1000 y 5000 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal	80%
Catastrófico	Mayor a 5000 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v.6. DAFP con ajustes propios

Tanto en el análisis de probabilidad como el de impacto se considera el conocimiento y experiencia del responsable y funcionarios del proceso como conocedores de este.

El nivel de impacto para los riesgos de seguridad de la información deberá ser determinado con la presencia de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo (reputacional) o cuantitativo (económico).

Nota. Tener presente que, para los riesgos de seguridad de la información, la probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Riesgos de corrupción: Para medición del impacto de estos riesgos se debe diligenciar un cuestionario específico por cada riesgo identificado.

Tabla 4. Criterios para calificar el impacto – Riesgos de corrupción

No	PREGUNTA Si el riesgo se materializa podría:
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?
1	¿Afectar al grupo de funcionarios del proceso?
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?
3	¿Afectar el cumplimiento de misión de la Entidad?
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?
6	¿Generar pérdida de recursos económicos?
7	¿Afectar la generación de los productos o la prestación de servicios?
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?
9	¿Generar pérdida de información de la Entidad?
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?
11	¿Dar lugar a procesos sancionatorios?
12	¿Dar lugar a procesos disciplinarios?
13	¿Dar lugar a procesos fiscales?
14	¿Dar lugar a procesos penales?
15	¿Generar pérdida de credibilidad del sector?
17	¿Afectar la imagen regional?
18	¿Afectar la imagen nacional?
19	¿Genera daño ambiental?

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital v.4. DAFP

En esta tabla se deben responder las preguntas para cada uno de los riesgos identificados.

Si se responde afirmativamente la pregunta 16, el riesgo se considera catastrófico y no será necesario responder las otras preguntas.
Si al sumar las respuestas, se encuentran entre una y cinco preguntas del total como respondidas afirmativamente se genera un impacto MODERADO, (genera medianas consecuencias sobre la entidad).
Si son entre seis a once preguntas las respondidas afirmativamente el impacto es MAYOR, (genera altas consecuencias sobre la entidad).

Si se responden entre doce y diecinueve preguntas afirmativamente el impacto es CATASTRÓFICO, (genera consecuencias desastrosas para la entidad).

Para los riesgos de corrupción del resultado del cuestionario se determinará la categoría del impacto teniendo en cuenta solamente los niveles moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos.

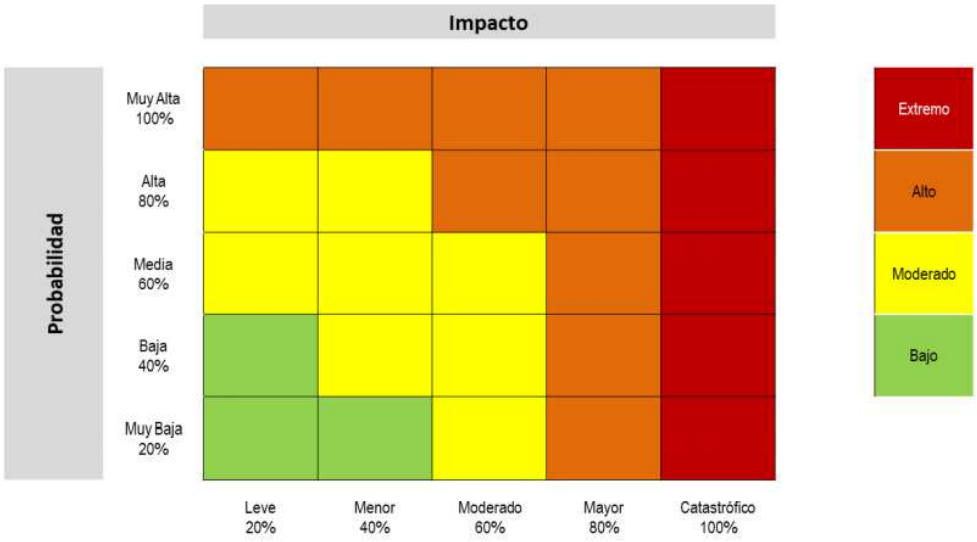
3.2. Evaluación de riesgos

Se busca determinar la zona de riesgo inherente a partir del análisis de la probabilidad y el impacto.

3.2.1. Análisis de Riesgo Inherente

Se determinan los niveles de severidad a través de la combinación entre probabilidad e impacto.

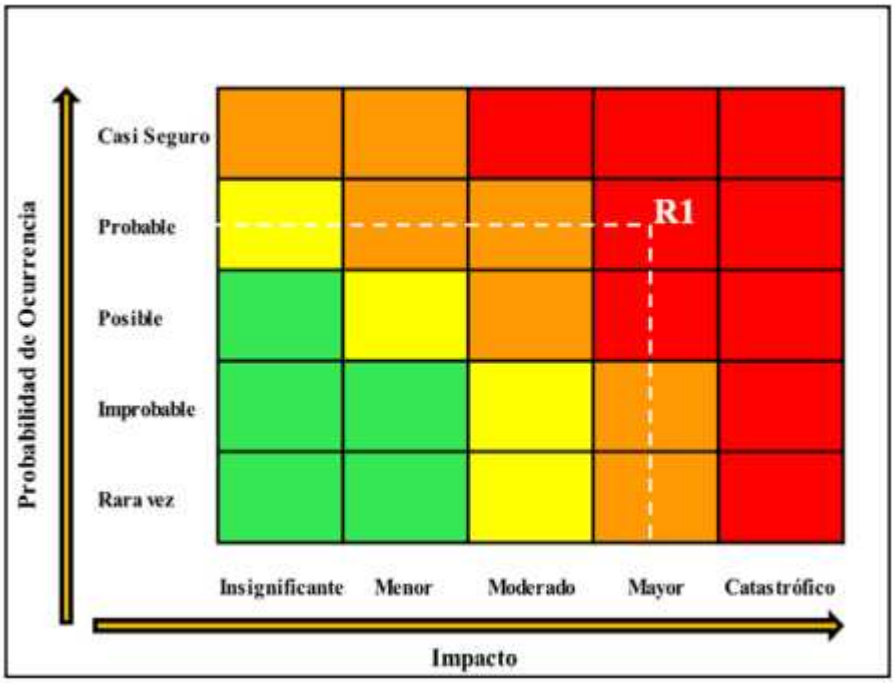
Imagen 6. Matriz de calor (niveles de severidad del riesgo) riesgos de gestión, seguridad de la información y fiscales



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v.6. DAFP

Para los riesgos de corrupción se toma el mapa de calor definido en la Guía versión 4 del DAFP.

Imagen 7. Matriz de calor - Riesgos de corrupción



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital v.4. DAFP

3.2.2. Valoración de controles

Un control es la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta lo establecido por el DAFP:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control riesgos de gestión, seguridad de la información y fiscales:

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

Estructura para la descripción del control riesgos de corrupción

Para estos riesgos los controles deben identificar el responsable, periodicidad, propósito, como se realiza la actividad de control, que pasa con las observaciones o desviaciones y evidencia de la ejecución del control.

3.2.2.1. Tipología de controles:

Es posible identificar una tipología de controles según el momento en que se activan dentro del ciclo del proceso.

- Control preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. Va hacia las causas del riesgo.
- Control detectivo: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Detecta que algo ocurre y devuelve el proceso a los controles preventivos.
- Control correctivo: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

De acuerdo con la forma como se ejecutan:

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

Para los riesgos de seguridad de la información, se podrán emplear los controles tomados del Anexo A del estándar ISO/IEC 27001:2013 y los dominios a los que pertenecen, siempre y cuando se ajusten al análisis de riesgos.

3.2.2.2. Análisis y Evaluación de los controles – atributos:

Riesgos de gestión, de seguridad de la información y fiscales:

A continuación, se analizan los atributos para el diseño del control para riesgos de gestión, seguridad de la información y fiscales, teniendo en cuenta características relacionadas con la eficiencia y la formalización, también se presentan su descripción y pesos asociados.

Imagen 8. Atributos de los controles – Riesgos de gestión, seguridad de la información y fiscales:

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la	25%

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v.6. DAFP

Para cada control, dependiendo su tipo y su implementación se realiza una valoración, que resulta de sumar el peso del tipo por el peso de la implementación, con lo que, por ejemplo, si un control es preventivo y manual, se suma 25% más 15% con lo que su valoración da 40%.

Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Imagen 9. Calificación de los atributos de los controles – Riesgos de gestión, seguridad de la información y fiscales

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2º control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2 %**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v.6.

Los controles preventivos y detectivos afectan la probabilidad, mientras que los correctivos el impacto. En caso de no contar con controles correctivos, el impacto residual es el mismo al inherente.

En el ejemplo de la gráfica, teniendo un control preventivo y asumiendo que la probabilidad inherente fue de 60% (media) y la valoración del primer control fue de 40%, se multiplica la probabilidad 60% por la valoración del control 40%, luego se le resta la probabilidad inherente de 60% a ese resultado de 24%, con lo que la valoración de probabilidad termina en 36%. Pero ese riesgo tiene adicionalmente un control detectivo con un peso de 30%, por lo que de esa valoración residual de 36% se le empieza a calcular la mejora con este segundo control, con lo que se obtiene un 36% por el 30% del control lo que da 10,8% y luego al 36% se le resta el 10.8% resultante, con lo que la valoración de la probabilidad queda en 25.2%, la cual es la probabilidad residual o final después de controles.

En el mismo ejemplo del gráfico, no se tienen controles correctivos, los cuales son aquellos que afectan el impacto, razón por la cual, el impacto inherente de 80% (mayor) no se modifica y el impacto residual resulta igual a 80%. En el caso que haya controles correctivos se sigue el mismo ejercicio del ejemplo

para los controles preventivos y detectivos, es decir, se multiplicaría el valor del impacto por la valoración del control y luego a la valoración del impacto inicial se le restaría ese resultado, con lo que se genera el impacto residual, si se tuvieran más controles correctivos, se seguiría la misma lógica disminuyendo progresivamente la valoración de impacto.

Riesgos de corrupción:

Para estos riesgos se tienen los lineamientos de la Guía versión 4 del DAFP así:

Tabla 5. Análisis y evaluación de los controles para mitigación - Riesgos de corrupción

CRITERIO DE EVALUACIÓN	ASPECTO POR EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	EVALUACION
Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No asignado	0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
		Inadecuado	0
Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, ¿etc.?	Prevenir	15
		Detectar	10
		No es un control	0
Como se realiza la actividad de control.	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15
		No confiable	0
Que pasa con las observaciones o desviaciones.	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan	0
Evidencia de la ejecución del Control	¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?	Completa	10
		Incompleta	5
		No existe	0

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, con ajustes OAPAP. DAFP

El resultado de cada criterio de evaluación para diseñar un control, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todos estos, para que un control se evalué como bien diseñado.

Tabla 6. Resultados de la evaluación de diseño - Riesgos de corrupción

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
DEBIL	Calificación entre 0 y 85

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4. DAFP

Si el resultado del diseño del control es diferente de fuerte se debe generar una mejora al control para que cumpla los criterios.

Tabla 7. Resultados de la evaluación de la ejecución del control – Riesgos de corrupción

Resultados de la Evaluación de la EJECUCIÓN del control	
Rango de Calificación de LA EJECUCIÓN	Resultado - Peso en la evaluación 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.
DEBIL	El control no se ejecuta por parte del responsable.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades pública, versión 4. DAFP

La solidez individual de un control se mide aplicando el cuadro de Análisis y Evaluación de los Controles para la Mitigación de los Riesgos.

Tabla 8. Análisis y Evaluación de los controles para la mitigación de los riesgos – Riesgos de corrupción

Análisis y Evaluación de los Controles para la Mitigación de los Riesgos				
Peso del diseño individual o promedio de los Controles. (DISEÑO)	El Control se ejecuta de manera consistente por los responsables. (EJECUCION)	Solidez individual de cada control Fuerte:100 Moderado:50 Debil:0		Aplica para mejora del control
Fuerte Calificación entre 96 y 100	Fuerte (Siempre se ejecuta)	Fuerte + Fuerte = Fuerte	100	NO
	Moderado (Algunas veces)	Fuerte + Moderado = Moderado	50	SI

Análisis y Evaluación de los Controles para la Mitigación de los Riesgos				
Peso del diseño individual o promedio de los Controles. (DISEÑO)	El Control se ejecuta de manera consistente por los responsables. (EJECUCION)	Solidez individual de cada control Fuerte:100 Moderado:50 Debil:0		Aplica para mejora del control
	Débil (No se ejecuta)	Fuerte + Débil = Débil	0	SI
Moderado Calificación entre 86 y 95	Fuerte (Siempre se ejecuta)	Moderado + Fuerte = Moderado	50	SI
	Moderado (Algunas veces)	Moderado + Moderado = Moderado	50	SI
	Débil (No se ejecuta)	Moderado + Débil = Débil	0	SI
Débil entre 0 y 85	Fuerte (Siempre se ejecuta)	Débil + Fuerte = Débil	0	SI
	Moderado (Algunas veces)	Débil + Moderado = Débil	0	SI
	Débil (No se ejecuta)	Débil + Débil = Débil	0	SI

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4. DAFP Con ajustes propios

La evaluación consiste en realizar la sumatoria de los resultados del diseño y la ejecución del control, la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil.

Aquellos controles que no sean fuertes tienen posibilidad de mejora.

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

Tabla 9. Calificación de la solidez de controles – Riesgos de corrupción

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4. DAFP

Considerando lo anterior, para cada uno de los riesgos identificados se debe establecer la solidez individual de cada uno de los controles y la solidez del conjunto de controles.

3.2.3. Nivel de riesgo residual

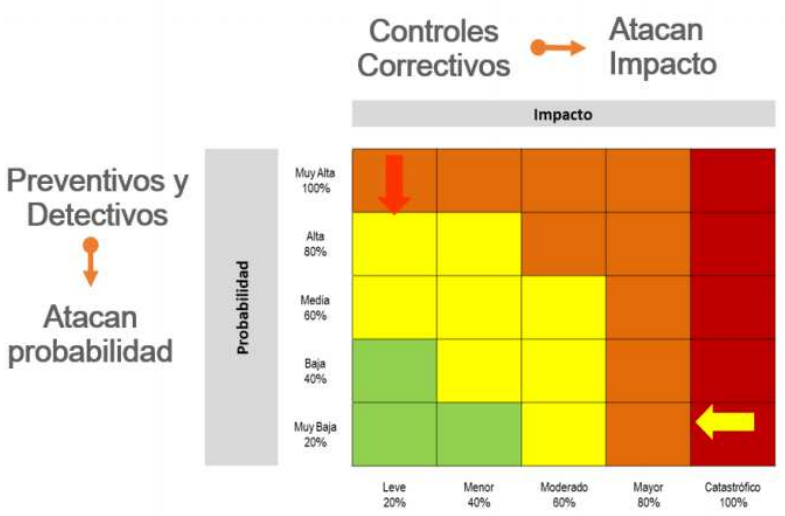
Es el resultado de aplicar la efectividad de controles al riesgo inherente.

Los controles mitigan el riesgo de manera acumulativa, es decir, una vez se aplica el valor de uno de los controles, el siguiente valor se aplica con el valor resultante luego de la aplicación del primer control.

Desplazamiento

A continuación, se presenta como se genera desplazamiento en la matriz de calor según el tipo de control.

Imagen 10. Movimiento en la matriz de calor acorde con el tipo de control – Riesgos de gestión, seguridad de la información y fiscales



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v.6. DAFP

Para los riesgos de corrupción, una vez evaluados los controles, se procede nuevamente a calificar y evaluar el riesgo en relación con su probabilidad e impacto por lo cual, dependiendo del tipo de control y de la calificación de solidez, opera desplazamiento en el mapa de calor, según la siguiente tabla:

Tabla 10. Resultados de los posibles desplazamientos de la probabilidad y del impacto- Riesgos de corrupción

SOLIDEZ DEL CONJUNTO DE CONTROLES	Controles que ayudan a disminuir la probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de la Probabilidad
FUERTE	Preventivos Detectivos	2
MODERADO	Preventivos Detectivos	1

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4. DAFP con ajustes propios

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

3.2.4. Tratamiento del riesgo

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser reducir, aceptar o evitar. Se analiza frente al riesgo residual.

Reducir: Cuando el nivel de riesgo residual es moderado, alto o extremo se determina tratarlo mediante transferencia o mitigación de este. Transferir corresponde a la estrategia de tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas, la responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad reputacional. Mitigar corresponde a implementar acciones que mitiguen el nivel de riesgo, no necesariamente un control adicional.
Implica tomar medidas encaminadas a disminuir la probabilidad: medidas de prevención, el impacto (medidas de protección) o ambas. Por lo general conlleva a la implementación de controles.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: actividades, recursos, responsables, fecha de implementación.

Aceptar: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Es una decisión informada de tomar un riesgo en particular. Los riesgos asumidos deben estar sujetos a monitoreo y revisión. Esta opción opera cuando la zona de riesgo residual es baja.

Evitar: No asumir la actividad que genera el riesgo.

El tratamiento a los riesgos de corrupción sólo tendrá dos (2) escenarios posibles que corresponden a reducir o evitar el riesgo.

3.3. Monitoreo y seguimiento

El monitoreo y revisión de la gestión de riesgos, está alineada con la dimensión 7 de MIPG de Control Interno, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual parte del Esquema de líneas de defensa.

Reportes periódicos

La formulación de los mapas de riesgos de gestión, fiscales y corrupción es revisada por la Oficina Asesora de Planeación y Aseguramiento de Procesos OAPAP, mientras que, para el caso de riesgos de Seguridad de la información, se realiza la revisión por parte del Oficial de Seguridad de la Información de la Gerencia de Tecnología.

Los responsables de procesos de la Unidad deben monitorear permanentemente sus mapas de riesgos para determinar cambios en las diferentes etapas de la Gestión del riesgo.

El seguimiento y la revisión deben:
- Garantizar que los controles son eficaces tanto en el diseño como en la operación.
- Obtener información adicional para valorar el riesgo.
- Analizar y aprender lecciones.
- Verificar, atender e informar la materialización del riesgo.

El seguimiento y la revisión del riesgo y su materialización se efectuará trimestralmente, remitiendo la información a la Oficina Asesora de Planeación y Aseguramiento de Procesos (riesgos de gestión y corrupción) y al Oficial de Seguridad de la Información – Gerencia de Tecnología (riesgos de seguridad de información).

Los responsables deberán generar el seguimiento trimestralmente los primeros diez días hábiles siguientes al corte del trimestre, acorde con lo establecido con el Procedimiento Gestión de riesgos.

Excepcionalmente y por necesidades del servicio, este plazo podrá ampliarse con la aprobación del Jefe de la Oficina Asesora de Planeación y Aseguramiento de Procesos y/o Gerente de Tecnología –Oficial de Seguridad de la Información según corresponda, sin exceder los plazos establecidos para publicación y envío de la información a la Oficina de Control Interno.

Los procesos tendrán un repositorio de información para conservar los soportes trimestrales que dan cuenta o son evidencia de la ejecución de las actividades del plan de manejo de riesgos.

La Oficina Asesora de Planeación y Aseguramiento de Procesos determinará la herramienta a través de la cual se realizará la formulación y seguimiento de los riesgos, la cual podrá ser entre otros, excel o aplicativo web, de lo cual se detallará su manejo en el procedimiento y/o instructivo asociado.

Si bien no se desarrolla Plan de Manejo de Riesgo a aquellos riesgos situados en zona de riesgo residual baja, estos se monitorean con el seguimiento periódico.

Seguimiento a los riesgos de corrupción

En concordancia con la cultura del autocontrol al interior de la entidad, los responsables de los procesos junto con su equipo realizarán anualmente la elaboración de los mapas de riesgos de corrupción y son ellos quienes realizarán el monitoreo y evaluación permanente al mismo, en los plazos establecidos.

Se deberá realizar la socialización del mapa de riesgos de corrupción de la entidad a servidores públicos, contratistas y ciudadanía en general, de forma previa a su publicación, con el fin de recibir observaciones para su mejora.

La OAPAP revisará que se cumpla con la presente metodología y liderará la consolidación de la información y su publicación. Para lo cual publicará el mapa de riesgos de corrupción anualmente antes del 31 de enero de cada año.

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

El primer seguimiento se realizará con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
El segundo seguimiento se realizará con corte al 31 de agosto, por lo que la publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre
El tercer seguimiento se realizará con corte al 31 de diciembre, por lo que la publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

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

Ajustes a la matriz de riesgos

Cuando el equipo responsable del proceso, producto del seguimiento y la revisión requiere ajustar, incluir o eliminar algún riesgo (gestión, fiscales, corrupción, éste se realizará en Comité de calidad o por solicitud realizada por medio de correo electrónico al asesor de calidad del proceso, dejando soporte de la justificación por la cual se realiza la inclusión, modificación o eliminación del riesgo.

Cuando luego de la revisión de un riesgo este pase a riesgo residual bajo y haya tenido plan de tratamiento este no requerirá continuar el plan establecido toda vez que la valoración de controles establece la solidez de estos con lo que la opción de tratamiento es asumir.

El ajuste de los riesgos de seguridad de la información se realizará de manera conjunta entre el proceso y el Oficial de Seguridad de la información por correo electrónico o mediante actas o registros de reunión.

De presentarse materialización en los riesgos estos deberán ser revisados de forma integral teniendo en cuenta entre otros, los cambios en el contexto, la descripción del riesgo, causas, probabilidad e impacto, controles, plan de tratamiento). Los resultados de esta revisión deberán ser documentados por correo electrónico o acta. De no ser requerida una actualización o nueva versión del mapa esta deberá ser justificada en el análisis. Las acciones correctivas a realizar en caso de materialización del riesgo se deberán incorporar dentro del plan de tratamiento del riesgo o se documentarán a partir de una no conformidad.

Si luego de una materialización y con el análisis del riesgo este queda en zona de riesgo residual baja y por ende no requiere plan de tratamiento, en todo caso se deberá documentar una no conformidad para tratar la materialización.

Cuando el proceso en desarrollo de su rol de primera línea de defensa identifique una materialización, no requerirá esperar a que se realice el reporte trimestral para revisar y ajustar la matriz, sino que deberá hacerlo luego de identificada la materialización.

En cuanto a seguridad de la información, en el evento de presentarse un incidente de seguridad sobre un activo o grupo de activos de información se debe tener presente lo siguiente:

a. Si el activo o grupo de activos no se encuentren identificados en el inventario general de activos o instrumento de gestión de la información pública es necesaria la actualización de estos, su valoración y su correspondiente análisis de riesgos.
b. Si no existe ningún riesgo asociado con el incidente presentado es necesario incluir el riesgo actualizando la matriz de riesgos del proceso.

Asimismo, en cuanto a seguridad de la información, una vez finalizado el plan de tratamiento deberá ser revaluado el riesgo.

Por otra parte, el Oficial de Seguridad de Información verificará con periodicidad anual, si en los planes de tratamiento de los riesgos, se han incluido nuevos controles adicionales a los establecidos en la declaración de aplicabilidad -DdA de la Unidad, en cuyo caso deberá proceder a ajustarla.

4. INFORMACIÓN, COMUNICACIÓN Y REPORTE

Corresponde a los jefes de oficina, gerentes, subgerentes y responsables de proceso (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.

La Oficina Asesora de Planeación y Aseguramiento de Procesos y el Oficial de Seguridad de la Información – Gerencia de Tecnología (en cuanto a riesgos de seguridad de la información) son los responsables de la difusión y asesoría de la presente metodología, para lo cual deberán adelantar procesos de socialización de esta, así como de realizar el seguimiento a los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.

Se debe conservar evidencia de la comunicación de la información y reporte de la administración del riesgo en todas sus etapas, los soportes de estos reposarán en la Oficina Asesora de Planeación y Aseguramiento de Procesos y en la Gerencia de Tecnología (riesgos de seguridad de la información).

La comunicación y consulta con las partes involucradas tanto internas como externas debería tener lugar en todas las etapas del proceso para la gestión del riesgo.

La Oficina de Control Interno, debe realizar la evaluación independiente sobre la Gestión del Riesgo en la Entidad, catalogándola como una unidad auditable más dentro de su universo de Auditoría, y por tanto debe dar a conocer el Plan Anual de Auditorías basado en riesgos, y los resultados de la evaluación de la Gestión del Riesgo.

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.

Para la revisión por la dirección o para presentar al Comité Institucional de Gestión y Desempeño y/o Comité Institucional de Coordinación de Control Interno, se elabora un informe de riesgos, este es realizado según su competencia y de forma independiente por la Oficina Asesora de Planeación y Aseguramiento de Procesos, la Oficina de Control Interno y el Oficial de Seguridad de la Información (Gerencia de Tecnología).

ANEXO 1. Amenazas – Anexo C ISO27005:2009

Tipo	Amenazas	Origen
Daño físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D

Tipo	Amenazas	Origen
Fallas técnicas	Falla del equipo A	A
	Mal funcionamiento del equipo A	A
	Saturación del sistema de información A, D	A, D
	Mal funcionamiento del software A	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E
Datos personales	Modificación o alteración no autorizada de datos personales	D
	Pérdida o borrado de datos personales	A, D
	Acceso no autorizado a los datos personales	D
	Ausencia de procedimientos para el ejercicio de derechos	D
	Corrupción de datos	A, D
	Tratamiento de datos personales no autorizado	
	Recuperación de medios o documentos desechados o reciclados	D
	Robo de medios o documentos	D
	Pérdida, destrucción, acceso o uso no autorizado	
	Alteración de documentos	
	Ausencia de legitimidad para el tratamiento de los datos personales	D
	Tratamiento ilícito de datos personales	A, D

Fuente: Anexo C ISO27005:2009

ANEXO 2. Vulnerabilidades – Anexo D ISO27005:2005

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo	Destrucción de equipos o de medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de contraseñas	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado
Datos personales	Ausencia de procedimientos para que los titulares puedan ejercer sus derechos	Ausencia de procedimientos para el ejercicio de derechos
	Acceso intencionado por parte de personal no autorizado	Acceso no autorizado a los datos personales
	Perdidas de dispositivos móviles	Acceso no autorizado a los datos personales
	Uso ilegítimo de datos personales	Acceso no autorizado a los datos personales
	Errores en los procesos de recopilación y captura de información	Modificación o alteración no autorizada de datos personales
	Ausencia o indebida asignación de privilegios para el tratamiento de datos personales	Modificación o alteración no autorizada de datos personales
	Ataque para la suplantación de identidad	Modificación o alteración no autorizada de datos personales
	Contraseñas y datos sensibles no cifrados	Tratamiento de datos personales no

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
		autorizado
	Ausencia de control de acceso	Pérdida, destrucción, acceso o uso no autorizado
	Borrado de datos personales por error humano	Pérdida o borrado intencionado de datos personales
	Ataque intencionado que provoca borrado o pérdida de datos personales	Pérdida o borrado intencionado de datos personales

Fuente: Anexo D ISO27005:2005

3. DOCUMENTOS REFERENCIA

BIBLIOGRAFÍA

- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Noviembre de 2022. DAFP.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4. Octubre de 2018. DAFP.
- Manual Operativo Sistema de Gestión MIPG, Modelo Integrado de Planeación y Gestión. Versión 5.
- Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Guía de orientación para la gestión de riesgos de seguridad digital en el Gobierno nacional, territoriales y sector público. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Modelo de Gestión de Riesgos de Seguridad Digital. Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).
- Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018.