GUÍA DE ADMINISTRACIÓN DE RIESGOS

RTVC
Sistema de Medios Públicos

Tabla de contenido

1. Introducción ____ *3*

2. Objetivo General ____ *4*

2.1 Objetivos específicos ____ *4*

3. Alcance ____ *5*

4. Glosario ____ *5*

5. Clasificación de Riesgo ____ *13*

6. Metodología Identificar Riesgos ____ *14*

6.1 Identificar Riesgos De Gestión ____ 14

6.2 Identificar Riesgos De Corrupción ____ 16

6.3 Identificar Riesgos Fiscales ____ 18

6.4 Identificar Riesgos de Seguridad de la Información y Seguridad Digital ____ 21

4.7 Evaluación Del Riesgo ____ 31

4.7.1 Riesgo de Gestión, Fiscal, Seguridad de la Información y Seguridad Digital ____ 31

____ 32

4.7.2 Riesgo de Corrupción ____ 32

4.8 Valoración De Controles ____ 35

4.8.1 Riesgos de Gestión, Fiscal, Seguridad de la Información y Seguridad Digital. ____ 35

4.8.2 Riesgos de Corrupción. ____ 37

7. Referencias y anexos ____ *39*

1. Introducción

El riesgo es un concepto que se puede considerar fundamental, por su vínculo con todo el que hacer. Casi se podría afirmar que no hay actividad de la vida, los negocios, o de cualquier asunto, que no incluya la palabra riesgo. Es por ello por lo que la humanidad desde sus inicios buscó maneras de protegerse contra las contingencias y desarrolló mecanismos para evitar, minimizar o asumir riesgos a través de acciones preventivas.

Es así como se encuentra que existen diferentes formas de abordar el tema de los riesgos, dependiendo por ejemplo del tamaño de una empresa, los objetivos que persigue, la cultura administrativa, la complejidad de sus operaciones y la disponibilidad de recursos, entre otros.

A partir de la Dirección Moderna se concibió una disciplina denominada "Administración de Riesgos" o "Gerencia de Riesgos" siendo una función de muy alto nivel dentro de una organización por ser un elemento de gran valor metodológico y estratégico, que define un conjunto de estrategias que a partir de los recursos físicos, humanos y financieros busca brindar herramientas que le den un manejo adecuado a los riesgos con el fin de lograr, de la manera más eficiente:

- El cumplimiento de la misión y objetivos institucionales en el corto, mediano y largo plazo.
- La garantía de la supervivencia y estabilidad de la empresa.
- El fortalecimiento continuo de la credibilidad misma ante el ciudadano, clientes, aliados o cualquier grupo de interés.
- La preparación para enfrentar cualquier contingencia que se pueda presentar y de esta manera garantizar la continuidad del negocio.

Para todas las empresas, es fundamental la introducción del concepto de la Administración del Riesgo como objetivo primordial dentro su funcionamiento, en donde se puedan identificar, caracterizar y jerarquizar los riesgos que atenten contra el buen desempeño de la Institución, aplicando acciones que eliminen o en su defecto minimicen de manera controlada los riesgos que hayan sido previamente identificados y así puedan alcanzar sus objetivos y metas propuestas, minimizando pérdidas y maximizando oportunidades.

Para alcanzar este objetivo se requiere un marco legal, institucional y técnico que permita instrumentalizar y hacer efectiva la coordinación de las acciones con resultados en el corto, mediano y largo plazo. Para esto se cuenta con instrumentos como; la matriz de riesgos de corrupción, la matriz de riesgos de proceso, el análisis de riesgos en seguridad y salud en el trabajo, el plan de continuidad

de negocio, la política de administración de riesgos, la alineación entre los procesos y controles establecidos, entre otros.

Para RTVC, partiendo de la base de su razón de ser y su compromiso con la sociedad, es preciso identificar y precisar los procesos, procedimientos, instancias y controles dentro de los cuales puede actuarse e incurrirse en riesgos que atentan contra la buena gestión y la obtención de resultados para tener un manejo adecuado del riesgo.

Esta guía de administración del riesgo establece los lineamientos por parte de RTVC para dar cumplimiento con la misión de renovar, consolidar, racionalizar y mejorar las condiciones de operación y funcionamiento, generando desarrollo y posibilidades de sostenibilidad. La importancia de entender, analizar y comprender los impactos generados por los riesgos permite establecer los planes preventivos que facilitan el control de los riesgos y tener capacidad de respuesta ante su materialización.

2. Objetivo General

Garantizar el cumplimiento de la misión y objetivos de la entidad a través de la identificación, el análisis, el control y el seguimiento de los riesgos por procesos o gestión, de corrupción, fiscal y de seguridad de la información y seguridad digital, tomando como modelo las “Guías para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública”.

2.1 Objetivos específicos

- Generar una visión general acerca de la administración y evaluación de riesgos, así como el compromiso y/o declaración de la alta dirección en coordinación con control interno, con relación a los mismos.
- Articular la administración del riesgo con la gestión de procesos.
- Hacer partícipes a todos los servidores públicos y colaboradores de la entidad en la búsqueda de acciones encaminadas a prevenir los riesgos de procesos, de corrupción, fiscal; de seguridad de la información y seguridad digital.
- Socializar el aplicativo dispuesto por la entidad y demás herramientas diseñadas por la Coordinación de Planeación y la Coordinación de TI para facilitar a la entidad una adecuada identificación, valoración y análisis de los riesgos de procesos, corrupción, fiscal; seguridad de la información y seguridad digital.

3. Alcance

Aplica a todos los procesos, programas, proyectos, planes, procesos, trámites y servicios conforme a cada tipo y clasificación de riesgo, inicia desde el análisis de contextos alineados a los objetivos estratégicos y/o de procesos, la identificación, el análisis, valoración de controles, tipo de manejo hasta el seguimiento o monitoreo de estos de acuerdo con el rol y responsabilidad del esquema de líneas de defensa.

Nota: los riesgos y peligros identificados en el marco del sistema de seguridad y salud en el trabajo serán gestionados con los lineamientos definidos por la Coordinación de Talento Humano y normatividad legal vigente, así como los aspectos e impactos identificados en el marco del sistema Gestión Ambiental serán gestionados con los lineamientos definidos por grupos de interés y normatividad legal vigente.

4. Glosario

- **Aceptar el Riesgo:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).[1]
- **Activo:** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.[2]
- **Afectación económica y reputacional:** son aspectos principales frente a la posible materialización de los riesgos que impacten la imagen de la entidad y/o presupuestalmente, en tal sentido, se ajusta la matriz de calor de acuerdo con la escala de severidad definida en 5 zonas (baja, moderada, alta y extrema)
- **Amenaza**: Causa potencial de un incidente no deseado el cual puede causar daños a un sistema u organización[3].
- **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.[4]

[1] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 68

[2] CONPES 3854:2016, , página 56

[3] Norma ISO 27000:2018 - Términos y definiciones

[4] CONPES 3854 página 87

- **Análisis de riesgo:** en este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo.[5]
- **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 y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar. [6]
- **Ataque cibernético:** Acción organizada y premeditada de una o más agentes para causar daño o problemas a un sistema informático a través del ciberespacio.[7]
- **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 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 riesgos**: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.[8]
- **Causa**: todos aquellos factores internos y externos que solo o en combinación con otros, pueden producir la materialización de un riesgo.[9]
- **Causa Inmediata**: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. [10]
  Nota: 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[11].
- **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

[5] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 36

[6] Norma ISO 27000 Términos y definiciones, DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 13

[7] CONPES 3854:2016, página 88

[8] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 13

[9] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12

[10] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12

[11] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12

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.

- **CICCI:** Comité Institucional de Coordinación de Control Interno
- **CIGD:** Comité Institucional de Gestión y Desempeño
- **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.[12]
- **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.[13]
  Nota: 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.
- **Compartir el riesgo:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.[14]
- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.[15]
- **Contingencia:** posible evento futuro, condición o eventualidad
- **Continuidad del negocio**: capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis
- **Control**: Medida que permite reducir o mitigar un riesgo.[16]
- **Declaración de aplicabilidad**: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo. (Inglés: *Statement of Applicability*; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de la norma ISO 27001:2013[17]
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad autorizada.[18]
- **DAFP**: Departamento Administrativo de la función Publica

---

[12] CONPES 3854. Pág.13

[13] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12

[14] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 68

[15] NTC-ISO/IEC 27000:2017 - Términos y definiciones

[16] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12

[17] Norma ISO 27000

[18] NTC-ISO/IEC 27000:2017 - Términos y definiciones

- **Evaluación del riesgo:** Su objetivo es comparar los resultados del análisis de riesgos inherentes con los controles establecidos, para determinar la zona de riesgo final.[19]
- **Evitar el riesgo:** Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.[20]
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos[21].
- **Gestión del riesgo**: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.[22]
- **Gestión del Riesgo Fiscal:** son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) 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 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)4 ” . 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.
- **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.
- **Identificación del Riesgo:** en esta etapa se debe establecer las fuentes o factores del riesgo, los eventos o riesgos, sus causas o consecuencias. Para el análisis se puede tener involucrara datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes interesadas. [23]

[19] Norma ISO 31000 numeral 2.24

[20] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 68

[21] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12

[22] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 8

[23] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 18

- **Impacto**: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo. [24]
- **Incidente de Seguridad de la información**: evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.[25]
- **Infraestructura crítica cibernética nacional**: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. [26]
- **Integridad**: Propiedad de exactitud y completitud.[27]
- **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 información del riesgo.
- **MIPG:** Modelo Integrado de Planeación y Gestión
- **Monitorear:** en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizaran monitoreo y evaluación permanente a la gestión de riesgos de corrupción.[28]
- **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

[24] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 8 y DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12
[25] Norma ISO 27000:2018 Términos y definiciones
[26] CONPES 3854:2016 Pág.29
[27] NTC-ISO/IEC 27000:2017 - Términos y definiciones
[28] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 26

maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto. [29]

- **Patrimonio público:** se entiende como el 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).
- **Política de administración del riesgo:** declaración de las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO 31000, numeral 2.4). La gestión del riesgo establece lineamientos acerca del tratamiento, manejo y seguimiento del riesgo.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo.
  Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.[30]

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.

Punto de Riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.

- **Reducir el riesgo:** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.[31]
- **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[32]

[29] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 13
[30] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12
[31] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 68
[32] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12

- **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[33].
- **Riesgo de cumplimiento:** posibilidad de ocurrencia de eventos que afecten la situación jurídica de la organización debido a su incumplimiento a la normatividad legal vigente y las obligaciones contractuales.[34] Al interior de RTVC esta categoría de procesos también es denominado como riesgos de gestión o riesgos de proceso.
- **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.[35] Al interior de RTVC esta categoría de procesos también es denominado como riesgos de proceso.
- **Riesgo de imagen o reputacional**: posibilidad de ocurrencia de un evento que afecten la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.[36] Al interior de RTVC esta categoría de procesos también es denominado como riesgos de gestión o riesgos de proceso
- **Riesgos estratégicos:** posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización y por tanto impactan a toda la entidad.[37] Al interior de RTVC esta categoría de procesos también es denominado como riesgos de gestión o riesgos de proceso.
- **Riesgos financieros:** posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.[38] Al interior de RTVC esta categoría de procesos también es denominado como riesgos de gestión o riesgos de proceso, se asocian principalmente a los riesgos identificados por los líderes de los procesos clasificados como de apoyo específicamente el proceso de gestión financiera, recaudo y gasto público .
- **Riesgo gerencial:** posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o de la alta dirección.[39] Al interior de RTVC esta categoría de procesos también es denominado como riesgos de gestión o riesgos de proceso, identificados por los líderes de los procesos clasificados como estratégicos cuando aplica, principalmente el proceso de Direccionamiento estratégico y planeación.
- **Riesgo de seguridad digital:** posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía

---

[33] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2018. Página 12 y DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12

[34] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 28

[35]. DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 8

[36] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 28

[37] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 28

[38] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 28

[39] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 28

nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.[40]

- **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 fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública
- **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.[41] El análisis se realiza bajo un escenario hipotético, cuando el riesgo a analizar no se ha materializado en la historia de la entidad.
- **Riesgos operativos:** posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.[42] Al interior de RTVC esta categoría de procesos también es denominado como riesgos de gestión o riesgos de proceso, identificados por los líderes de los procesos clasificados como misionales.
- **Riesgo Residual:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento[43] El resultado de aplicar la efectividad de los controles al riesgo inherente[44].
- **Riesgos tecnológicos:** posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.[45] Al interior de RTVC esta categoría de procesos también es denominado como riesgos de gestión o riesgos de proceso, identificados por los líderes de los procesos clasificados como misionales.
- **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y confiabilidad. [46]
- **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. [47]

---

[40] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 28

[41] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12

[42] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 28

[43] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 8

[44] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 12

[45] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 28

[46] Norma ISO 27000:2018 Términos y definiciones

[47] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas versión 5. 2020. Página 13

- **Tratamiento al riesgo:** es la respuesta establecida en la aplicación de controles para la mitigación de los riesgos.[48]
- **Valoración de los riesgos:** establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgos inicial (riesgo inherente)[49].

5. Clasificación de Riesgo

La clase de riesgos se clasifican en las siguientes categorías:

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

Tabla 1. Clasificación del Riesgo

[48] Norma ISO 31000 numeral 2.25

[49] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018. Página 36

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

Clasificación del riesgo	Descripción
Corrupción	Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. "Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).
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.
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).

Tabla 2. Tipología de Riesgos
Fuente: Adaptado Guía del DAFP versión 5 y 6

Nota: Una vez la alta dirección, el representante legal, la coordinación de planeación y el comité institucional de control interno han definido (aprobado) la política operacional de administración de riesgos se socializará al Comité Institucional de Gestión y Desempeño para conocimiento de los presentes.

6. Metodología Identificar Riesgos

6.1 Identificar Riesgos De Gestión

De acuerdo como se indica en la política operacional de gestión del riesgo se creó el formato E-F-12 "Análisis de Contextos e Identificación de Riesgos" como una de las fuentes generadoras, en donde se analiza el contexto externo, interno y del proceso con base a la herramienta PESTAL, así como la alineación al objetivo del proceso, el Plan Estratégico Institucional y demás factores considerados dentro del documento así como el conocimiento de situaciones del entorno de la entidad, antecedentes, registros históricos, experiencias significativas registradas, informes internos y externos, puntos y/o actividades de posibles riesgos, los cuales pueden proporcionar información importante.

Así mismo se debe verificar que no esté ya definido en otra categoría de riesgos o por otro proceso, para evitar duplicidad, esta actividad se debe realizar con el líder de cada proceso, con el enlace y/o su equipo de trabajo.

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

Identificación de áreas de factores de riesgo: son las fuentes generadoras de riesgos. En la Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas de la Función Pública en la versión vigente está el listado de factores de riesgo que puede tener la entidad, así mismo pueden crear otros factores aplicables de acuerdo con la necesidad del análisis realizado.

Descripción del riesgo: debe contener los detalles necesarios y que sea fácil de entender. Debe iniciar con la frase "POSIBILIDAD DE" y se analizan los siguientes aspectos:

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

Desglosando la estructura propuesta tenemos:

- ✓ Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- ✓ Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- ✓ Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Por ejemplo:

Objetivo del proceso: Brindar asesoría jurídica para la toma de decisiones con respaldo en el ordenamiento jurídico; propender por la adecuada y oportuna defensa de los intereses de la Entidad en los procesos judiciales, administrativos y extrajudiciales en los que sea parte o vinculada; así como realizar el cobro jurídico de la cartera comercial y de cobro coactivo, previa remisión por el área responsable.

Nombre del riesgo: Posibilidad de afectación económica por sentencia o imposición de multas o sanciones como consecuencia de la intervención ante autoridades administrativas, judiciales y extrajudiciales en la defensa de los intereses de RTVC S.A.S., debido al incumplimiento de lineamientos normativos, o extemporáneos.

Redacción inicial	Posibilidad de	
¿qué?	Afectación económica	Impacto
¿Cómo?	por sentencia o imposición de multas o sanciones como consecuencia de la intervención ante autoridades administrativas, judiciales y extrajudiciales en la defensa de los intereses de RTVC	Causa inmediata
¿Porqué?	Debido al incumplimiento de lineamientos normativos, o extemporáneos	Causa raíz

Tabla 3. Ejemplo Riesgo de Gestión

6.2 Identificar Riesgos De Corrupción

De acuerdo como se indica en la política operacional de gestión del riesgo se creó el formato E-F-12 “Análisis de Contextos e Identificación de Riesgos” como una de las fuentes generadoras, en donde se analiza el contexto externo, interno y del proceso con base a la herramienta PESTAL, así como la alineación al objetivo del proceso, el Plan Estratégico Institucional y demás factores considerados dentro del documento así como el conocimiento de situaciones del entorno de la entidad, antecedentes, registros históricos, experiencias significativas registradas, informes internos y externos, puntos y/o actividades susceptibles de actos de corrupción, los cuales pueden proporcionar información importante.

Así mismo se debe verificar que no esté ya definido en otra categoría de riesgos o por otro proceso, para evitar duplicidad, esta actividad se debe realizar con el líder de cada proceso, con el enlace y/o su equipo de trabajo.

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

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

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

1. ACCIÓN U OMISIÓN

+

2. USO DEL PODER

+

3. DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO

+

4. EL BENEFICIO PRIVADO.

Los riesgos de corrupción se establecen sobre procesos.

Por ejemplo:

Objetivo del proceso: Administrar, controlar y realizar seguimiento eficiente a los recursos financieros de la Entidad, garantizando el cumplimiento oportuno de las obligaciones, el cobro de los servicios prestados por RTVC y la confiabilidad de la información reflejada en los estados financieros.

Nombre del riesgo: Posibilidad de realizar transacciones de recursos a nombre propio o de un tercero interno o externo a RTVC.

Redacción inicial	Posibilidad de
Acción U Omisión	Acción: realizar transacciones
Uso Del Poder	de recursos
Desviación De La Gestión De Lo Público	Tiene el rol y la responsabilidad para desviar el recurso púbico
El Beneficio Privado	A nombre propio o de un tercero interno o externo a RTVC.

Tabla 4. Ejemplo Riesgo de Corrupción

6.3 Identificar Riesgos Fiscales

Se pone a disposición, como insumo de referencia, un catálogo indicativo y enunciativo de puntos de riesgo fiscal y circunstancias inmediatas (ver anexo), el cual ha sido construido como resultado del análisis de precedentes (aproximadamente 130 fallos con responsabilidad fiscal de contralorías territoriales y de la Contraloría General de la República) y debe ser utilizado como marco de referencia para la identificación y valoración de riesgos fiscales, siempre atendiendo las particularidades, naturaleza, complejidad, recursos, usuarios o grupos de valor, portafolio de productos y servicios, sector en el cual se desenvuelva (contexto), así como otras condiciones específicas de la entidad. En consecuencia, se deberá analizar si existen, de acuerdo con el contexto y particularidades puntos de riesgos y circunstancias inmediatas diferentes a los identificados en dicho catalogo y tenerlas en cuenta en la identificación de los riesgos fiscales.

Así mismo se debe verificar que no esté ya definido en otra categoría de riesgos o por otro proceso, para evitar duplicidad, esta actividad se debe realizar con el líder de cada proceso, con el enlace y/o su equipo de trabajo.

El Riesgo Fiscal es el efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. A continuación, se describen los elementos que componen la definición de riesgo fiscal:

Efecto: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública.

El evento potencial es equivalente a la causa raíz. Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso

Nota: Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.

Para mayor detalle en la identificación del riesgo fiscal ver la Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas de la Función Pública en la versión vigente.

Ejemplo:

Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes, por 6 meses, generándose intereses moratorios por $30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago.

¿Cuál es el daño? El daño fiscal corresponde al monto pagado por concepto de intereses moratorios
¿Cuál es el hecho generador? La omisión de pagó oportuno del canon de arrendamiento.

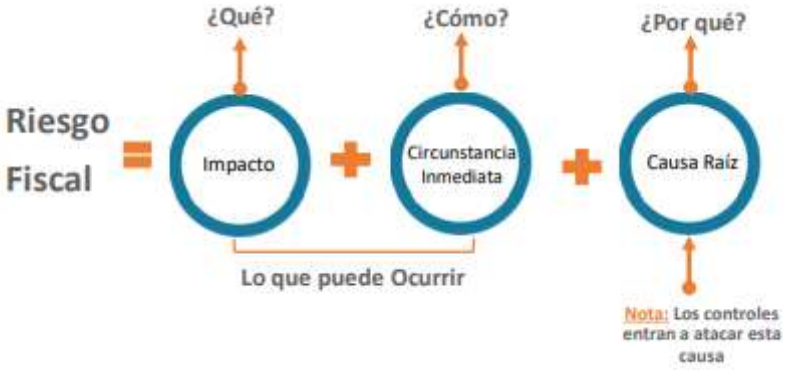
Conclusión: El hecho generador del daño no es el pago de los intereses moratorios, ya que el pagó es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.

A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos ejemplos de riesgos fiscales identificados como resultado del estudio de fallos de contralorías territoriales y Contraloría General de la República.

Para redactar un riesgo fiscal se debe tener en cuenta:

✓ Iniciar con la oración: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
✓ Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
✓ Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.
✓ Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

De acuerdo con lo indicado, la estructura es la siguiente:



Ejemplo:

Proceso: Gestión de Recursos
Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Riesgo: Posibilidad de Efectos dañosos sobre bienes públicos Por pérdida, extravío o hurto de bienes muebles de la entidad a causa de la omisión en la aplicación de procedimiento para el ingreso y salida de bienes del almacén.

REDACCIÓN INICIAL	Posibilidad de	
IMPACTO	Efectos dañosos sobre bienes públicos	¿Qué?
CIRCUNSTANCIA INMEDIATA	Por pérdida, extravío o hurto de bienes muebles de la entidad.	¿Cómo?
CAUSA RAIZ	A causa de la omisión en la aplicación de procedimiento para el ingreso y salida de bienes del almacén	¿por qué?

Tabla 5. Ejemplo de Riesgo Fiscal

6.4 Identificar Riesgos de Seguridad de la Información y Seguridad Digital

Se refiere a la identificación de los riesgos que puedan generar consecuencias negativas a la entidad provocadas por la pérdida de la confidencialidad, integridad y/o disponibilidad de la información.

La gestión de riesgos de seguridad de la información y seguridad digital incluye entonces la identificación de los riesgos, la probabilidad de su ocurrencia y la valoración de las consecuencias de su materialización (impacto), así como, la definición de controles y, en caso de que aplique, el plan de tratamiento para mitigar los mismos.

La siguiente figura muestra el esquema en el que RTVC, a través de la Coordinación de T.I., realiza la gestión de los riesgos de seguridad de la información y seguridad digital de acuerdo con lo estipulado en el Modelo de Seguridad y Privacidad de la información – MSPI propuesto por el MinTIC.

Ilustración 1. Plan de Gestión de Riesgos de Seguridad de la Información y Seguridad Digital
Fuente: Coordinación de T.I. - RTVC

La interacción entre ambos modelos se ve reflejada de la siguiente manera (tomado del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - 2021):

1. La identificación de activos y riesgos se alinean con la fase de Planificación del MSPI.

2. Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de Implementación del MSPI.

3. Las actividades de monitoreo, revisión de los riesgos residuales, efectividad de los controles y planes de tratamiento, así como el tema de auditoría, se alinean con la fase de Evaluación del desempeño del MSPI.

4. Las actividades de mejoramiento continuo en ambos modelos son similares.

Los riesgos de Seguridad de la Información y Seguridad Digital se establecen sobre procesos y su estructura de redacción se encuentra en la política operaciones de gestión del riesgo. Así mismo, es importante destacar que las actividades para la gestión de riesgos de seguridad de la información y seguridad digital cumplen con lo establecido en la Política operacional de Administración de riesgos de RTVC.

6.4.1 Identificación De Los Activos De Información

Se identifican, clasifican y valoran los activos de información teniendo en cuenta que en el contexto de seguridad de la información y seguridad digital estos se refieren a información, software, hardware, servicios, redes, información física y digital, que se utilizan para el funcionamiento de la entidad.

La identificación, clasificación y valoración de los activos será realizada por los líderes de proceso orientados por los colaboradores del Equipo de Seguridad de la información.

La clasificación y valoración de los activos de información se realiza según lo establecido en la ley 1712 de 2014, el Modelo de Seguridad y Privacidad de la información del MinTIC en su Guía de Gestión de Activos y el Modelo de Gestión de riesgos de Seguridad Digital del MinTIC.

Para la realización de esta actividad se establece el formato “Matriz de inventario y clasificación de activos de información” en el cual se detallan cada uno de los activos de información de la entidad, por proceso, teniendo en cuenta los aspectos mencionados anteriormente. Los campos de la matriz son los siguientes:

Campo	Descripción
ID	Número consecutivo único que identifica al activo en el inventario
Proceso / Oficina Productora	Nombre del proceso y área al que pertenece el activo
Nombre Del Activo	Nombre de identificación del activo dentro del proceso al que pertenece
Clasificación Documental - Trd	Serie y subserie dentro de la TRD a la que pertenece el activo, si aplica. Este campo será diligenciado por el área de Gestión documental.
Descripción Del Activo	Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso
Tipo De Activo	Información: datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
	Hardware: equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información.
	Software / Sistema de información: aplicaciones, software del sistema, herramientas de desarrollo y otras utilidades relacionadas
	Servicio: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet
	Recurso Humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información
	Otro: activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso
Idioma	El idioma en el cual se encuentra el activo
Ubicación Y Formato Del Activo	Medio de conservación y soporte: Físico (papel, Discos duros, CD, DVD), Electrónico (aplicaciones, documentos digitales.), Físico y electrónico
	Formato: Texto, hojas de cálculo, presentaciones, bases de datos, audio, video (.doc, .txt, .rtf, .pdf, .xls, .xlt, .csv, .ppt, .pps, .jpg, etc)

Campo	Descripción
	Estado: Publicada - Internet (se encuentra en la página Web oficial de la Entidad) Publicada – Intranet (se encuentra en la página de la intranet de la Entidad) Disponible (se encuentra en los archivos de gestión o Archivo Central y que la ciudadanía puede consultar o solicitar)
	Ubicación física: describe la ubicación física del activo de información
	Ubicación electrónica: describe la ubicación electrónica del activo de información
Propiedad Y Uso	Responsable de la producción de la información (propietario del activo): Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente.
	Responsable de la información (custodio del activo): Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original)
	Usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información
Gestión Del Activo	Fecha de ingreso en el inventario: Fecha en la que se registró el activo en el Inventario (DD/MM/AAAA)
	Fecha de salida del inventario: Fecha en la que se retiró el activo en el Inventario (DD/MM/AAAA)
Clasificación Del Activo	Confidencialidad de la información: Pública: información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad. Publica clasificada: Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta.

Campo	Descripción
	Publica reservada: Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. Integridad de la información: la susceptibilidad a la pérdida de integridad se clasifica, según el impacto que puede generar, de la siguiente manera: ALTA: impacto negativo de índole legal o económica, retrasar funciones o generar pérdidas de imagen severas a la entidad. MEDIA: un impacto negativo de índole legal o económica, retrasar funciones o generar pérdida de imagen moderado a funcionarios de la entidad. BAJA: impacto no significativo para la entidad o entes externos. NO CLASIFICADA: ALTA Disponibilidad de la información: la susceptibilidad a la pérdida de disponibilidad se clasifica, según el impacto que puede generar, de la siguiente manera: ALTA: impacto negativo de índole legal o económica, retrasar funciones o generar pérdidas de imagen severas a entes externos. MEDIA: impacto negativo de índole legal o económica, retrasar sus funciones o generar pérdida de imagen moderada de la entidad. BAJA: puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen. NO CLASIFICADA: ALTA Nivel de criticidad: ALTO: activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta MEDIO: activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio. BAJO: activos de información en los cuales la clasificación de la información en todos sus niveles es baja.
Ley 1581 De 2012	Documentar si el activo contiene datos personales, posibles respuestas SI/NO

Tabla 6. Matriz de inventario y clasificación de activos de información
Fuente: Coordinación T.I. – RTVC

6.4.2 Identificación De Los Riesgos Inherentes De Seguridad De La Información Y Seguridad Digital

Se identifican tres (03) riesgos de seguridad de la información y seguridad digital:

1. **Pérdida de confidencialidad** (la confidencialidad se refiere a la propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados)
2. **Pérdida de integridad** (la integridad de la información garantiza que no se produzca su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada)
3. **Pérdida de disponibilidad** (la disponibilidad hace referencia a que la información debe estar disponible en el momento, lugar y formato que se requiera por personas autorizadas)

Para cada riesgo se debe asociar el activo o grupo de activos específicos del proceso y conjuntamente se debe analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

A continuación, se menciona un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados y que están descritas en el Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas y complementadas en la Guía de gestión de riesgos emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Deliberadas (D), fortuitas (F) o ambientales (A)

AMENAZAS COMUNES[50]		
TIPO	**AMENAZA**	**ORIGEN**
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A

[50] Fuente: Modelo para la gestión de riesgos de seguridad digital en entidades públicas

AMENAZAS COMUNES[50]		
TIPO	**AMENAZA**	**ORIGEN**
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia Comprometida	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	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Tabla 7. Amenazas Comunes

Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

TABLA DE AMENAZAS DIRIGIDA POR EL HOMBRE[51]		
FUENTE DE AMENAZA	**MOTIVACIÓN**	**ACCIONES AMENAZANTES**
Pirata informático, intruso ilegal	• Reto • Ego • Rebelión • Estatus • Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	• Destrucción de la información • Divulgación ilegal de la información • Ganancia monetaria • Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	• Chantaje • Destrucción • Explotación • Venganza • Ganancia política • Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	• Ventaja competitiva • Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica • Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema

[51] Fuente: Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

TABLA DE AMENAZAS DIRIGIDA POR EL HOMBRE[51]		
FUENTE DE AMENAZA	**MOTIVACIÓN**	**ACCIONES AMENAZANTES**
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	• Curiosidad • Ego • Inteligencia • Ganancia monetaria • Venganza • Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

Tabla 8. Amenazas dirigidas por el hombre

Identificación de vulnerabilidades: la entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

TABLA DE VULNERABILIDADES COMUNES[52]	
Tipo	**Vulnerabilidades**
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas

[52] Fuente: Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

TABLA DE VULNERABILIDADES COMUNES[52]	
Tipo	**Vulnerabilidades**
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Tabla 9. Vulnerabilidades comunes

La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

4.7 Evaluación Del Riesgo

4.7.1 Riesgo de Gestión, Fiscal, Seguridad de la Información y Seguridad Digital

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos, con el fin, de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. El análisis del riesgo dependerá de la información obtenida en la identificación de riesgos y de la disponibilidad de datos históricos y aportes de líderes y colaboradores de proceso.

Se han establecido dos aspectos para tener en cuenta en el análisis de los riesgos identificados, Probabilidad e Impacto.

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

Riesgo inherente: Para determinar la **probabilidad** de ocurrencia de los riesgos de gestión y fiscal estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. El criterio de calificación se realizará conforme la ilustración 2.

Ilustración 2. Criterios para definir el nivel de probabilidad

Para determinar el **impacto** de ocurrencia de los riesgos de gestión y fiscal se definen con base en dos variables la económico y reputacional. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, es decir, económico.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Ilustración 3. Criterios para definir el nivel de impacto

Análisis preliminar (riesgo inherente): se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor:

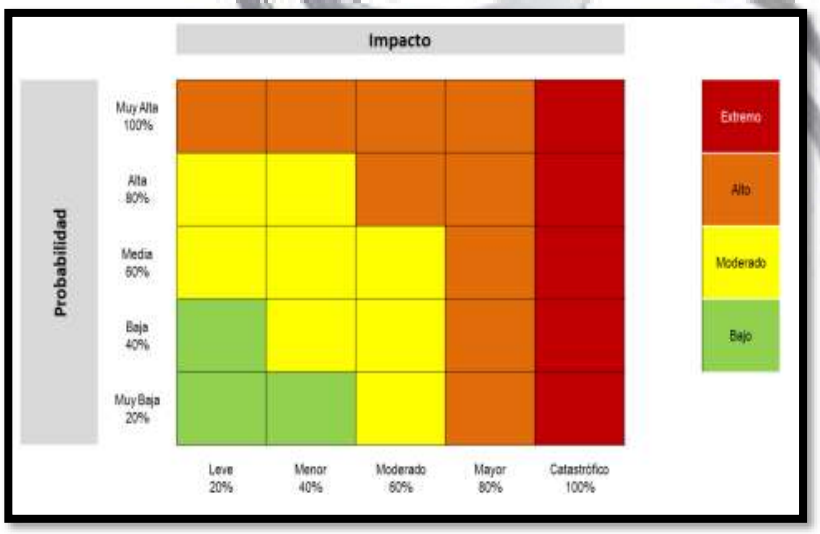


Ilustración 4. Matriz de calor para riesgos de gestión y fiscal

4.7.2 Riesgo de Corrupción

La valoración del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos, con el fin, de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. El análisis del riesgo dependerá de la

información obtenida en la identificación de riesgos y de la disponibilidad de datos históricos y aportes de líderes y colaboradores de proceso.

Se han establecido dos aspectos para tener en cuenta en el análisis de los riesgos identificados, Probabilidad e Impacto.

Riesgo inherente: Para determinar la **probabilidad** Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda. El criterio de calificación se realizará conforme a la ilustración 5.

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.

Ilustración 5. Criterios para definir el nivel de probabilidad

Para determinar el **impacto** de ocurrencia de los riesgos de corrupción frente a posibles materializaciones se analizarán únicamente los siguientes niveles:

Responder afirmativamente de UNA a CINCO preguntas genera un impacto moderado.
Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.
Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.

Dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos. Para determinar el impacto de los riesgos de corrupción, se debe aplicar las siguientes preguntas de la tabla 12:

N°	IMPACTO RIESGOS DE CORRUPCIÓN		
	PREGUNTA	RESPUESTA	
1.	¿Afectar al grupo de funcionarios del proceso?		
2.	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3.	¿Afectar el cumplimiento de la 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 la 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?		
16.	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17.	¿Afectar la imagen regional?		
18.	¿Afectar la imagen nacional?		
19.	¿Generar daño ambiental?		

Tabla 10. Preguntas para definir impacto

Nota: si se responde de forma afirmativa la pregunta No. 16 se debe considerar materialización del riesgo.

Análisis preliminar (riesgo inherente): en esta etapa se define el nivel de severidad para el riesgo de corrupción identificado, para lo cual se aplica la matriz de la guía de riesgos del DAFP, teniendo en cuenta el ajuste frente a los niveles de impacto insignificante y menor mencionados en la determinación del impacto, lo que implica que las zonas de severidad para este tipo de riesgos se delimitan como se muestra en la ilustración 6.

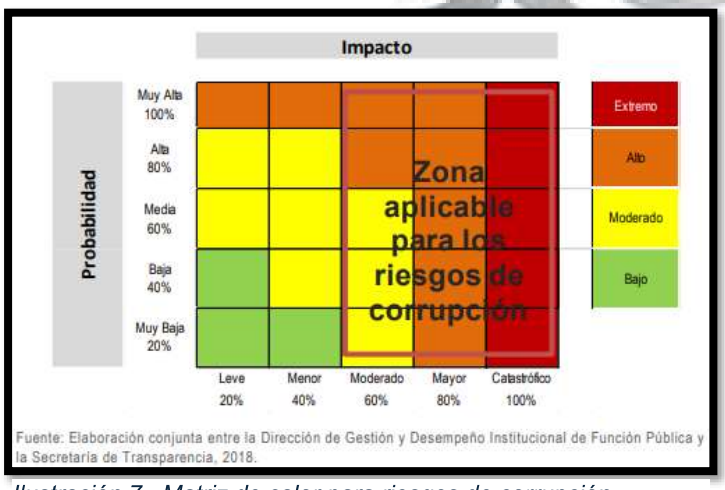


Ilustración 7. Matriz de calor para riesgos de corrupción

Determinación del nivel de riesgo inherente: A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo

inicial (riesgo inherente), se trata de determinar los niveles de severidad, para lo cual se aplica la ilustración 7.

4.8 Valoración De Controles

4.8.1 Riesgos de Gestión, Fiscal, Seguridad de la Información y Seguridad Digital.

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

- ✓ La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí 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 (primera línea de defensa).
- ✓ El tipo de control puede ser preventivo, detectivo y/o correctivo

Así mismo se recomienda al momento de realizar el diseño del control tener en cuenta como información adicional lo siguiente:

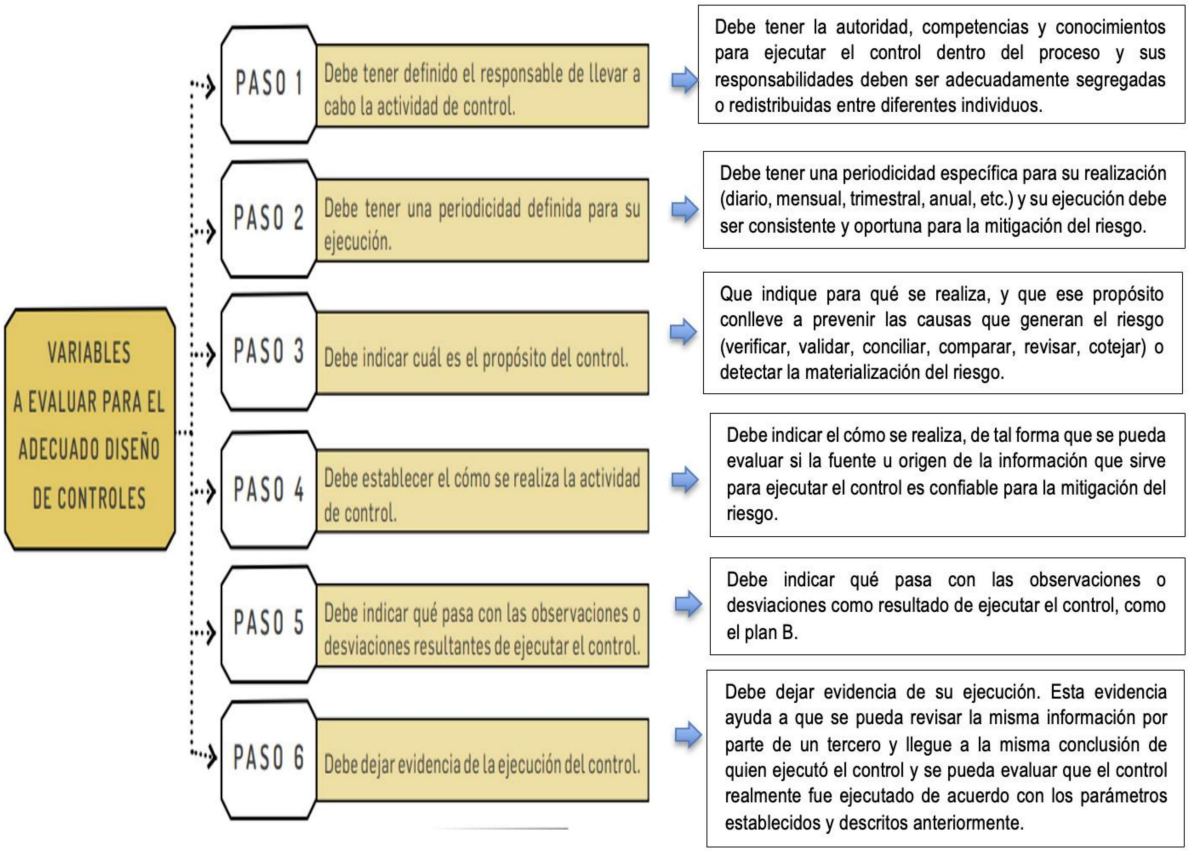


Ilustración 8. Pasos para diseñar un control

Calificación del control: con el desarrollo de esta actividad se determina el RIESGO RESIDUAL, Peso o participación de cada variable en el diseño del control para la mitigación del riesgo:

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%

Características			Descripción	Peso
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	0%
		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	0%
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que con lleva el riesgo.	0%
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	0%
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control	0%
		Sin registro	El control no deja registro de la ejecución del control.	0%

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

Nota: ver el instructivo para la implementación de la metodología en la herramienta dispuesta por la entidad, así mismo tener en cuenta la política operacional para el monitoreo por parte de la primera línea de defensa, el seguimiento por parte de la segunda línea de defensa y la evaluación independiente por parte de la tercera línea de defensa.

4.8.2 Riesgos de Corrupción.

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

- ✓ La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí 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 (primera línea de defensa).
- ✓ El tipo de control puede ser preventivo y/o detectivo

Así mismo se recomienda al momento de realizar el diseño del control tener en cuenta como información adicional en la ilustración No. 8.

Calificación del control: con el desarrollo de esta actividad se determina el RIESGO RESIDUAL, Peso o participación de cada variable en el diseño del control para la mitigación del riesgo:

CRITERIO DE EVALUACIÓN	OPCIONES DE RESPUESTA	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1.1 Asignación del responsable	Asignado	15
	No asignado	0
1.2. Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No Confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

7. Referencias y anexos

-Política de Gestión del riesgo Código E-A-4

-Instructivo explicativo de la herramienta para la gestión del riesgo Código E-I-6

-Guías de administración del riesgo emitidas por DAFP vigentes

Nota: Para visualizar el control de cambios del presente documento, por favor diríjase al sistema KAWAK en módulo de información documentada, consultando por el documento (nombre, proceso, código) en donde encontrará los cambios realizados al mismos.