CONTENIDO

1 OBJETIVO 3
2 DESTINATARIOS 3
3 GLOSARIO 3
4 REFERENCIAS 11
5 GENERALIDADES 12
5.1 Contexto Estratégico del Riesgo 13
5.2 Actualización de los mapas de Riesgo 14
5.3 ROLES Y RESPONSABILIDADES 15
5.3.1 Tipología de los conflictos de intereses 19
5.3.2 Características: 19
5.3.3 Materialización del conflicto de intereses y corrupción 19
5.3.4 Diferencias entre conflicto de intereses y corrupción 20
5.4 GENERALIDADES DEL CONTROL FISCAL INTERNO Y PREVENCIÓN DEL RIESGO FISCAL 20
5.4.1 Articulación entre el Control Fiscal y el Sistema de Control Interno 21
6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO 23
7 DESCRIPCION DE ETAPAS Y ACTIVIDADES 27
7.1 ETAPA 1: IDENTIFICAR EL RIESGO 27
7.1.1 Analizar el objetivo del proceso 27
7.1.2 Establecer contexto estratégico del proceso 27
7.1.3 Identificar los activos de información del proceso 28
7.1.4 Identificar las actividades críticas del proceso 28
7.1.5 Establecer y priorizar los riesgos 29
7.1.6 Estructurar el riesgo identificado 30
7.1.7 Describir Riesgo Identificado 36

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Laura Forero Torres Cargo: Profesional Universitario OAP Nombre: Oscar Fabián Ramírez Torres Cargo: Coordinador Grupo de Trabajo de Informática Forense y Seguridad Digital	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Jefe Oficina Asesora de Planeación Nombre: Jaroslav Marlén López Chávez Cargo: Jefe Oficina de Tecnología e Informática (E)	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2023-12-28

7.1.8 Clasificar la tipología del Riesgo 38
7.1.9 Analizar Causas o Vulnerabilidades 40
7.1.10 Analizar Consecuencias Potenciales 53
7.2 ETAPA 2: ANÁLIZAR Y CALIFICAR EL RIESGO ANTES DE CONTROLES (RIESGO INHERENTE) 54
7.2.1 Analizar y determinar la probabilidad 55
7.2.2 Analizar y determinar el impacto 56
7.2.3 Generar calificación y zona del riesgo inherente 58
7.3 ETAPA 3: IDENTIFICAR, CLASIFICAR Y VALORAR LOS CONTROLES 59
7.3.1 Identificar controles 59
7.3.2 Valorar los controles 62
7.4 ETAPA 4: ANALIZAR Y CALIFICAR EL RIESGO DESPUÉS DE CONTROLES (RIESGO RESIDUAL) 64
7.4.1 Calificar el riesgo residual 64
7.4.2 Seleccionar Opciones de Manejo 67
7.5 ETAPA 5: FORMULAR PLAN DE TRATAMIENTO DEL RIESGO 69
7.5.1 Formular actividades 69
7.5.2 Establecer responsables y fechas de ejecución de las actividades 70
7.5.3 Establecer mecanismo de detección de materialización 70
7.5.4 Modificar el plan de tratamiento del riesgo, en caso de ser necesario 70
7.6 ETAPA 7: APROBAR Y PUBLICAR EL MAPA DE RIESGOS EN EL APLICATIVO SIGI 71
7.6.1 Enviar mapa de riesgos a revisión metodológica 71
7.6.2 Revisar Metodológicamente el mapa de riesgos 72
7.7 ETAPA 7: REALIZAR MONITOREO, EVALUACION Y SEGUIMIENTO 72
7.7.1 Realizar Monitoreo 72
7.7.2 Elaborar plan de mejoramiento en caso de materialización de un riesgo 73
7.7.3 Realizar evaluación y seguimiento 74
7.8 ETAPA 8: REALIZAR DIVULGACIÓN, COMUNICACIÓN, CONSULTA Y CONTROL DE LOS MAPAS DE RIESGOS 74
7.8.1 Consultar mapa de riesgos 74
7.8.2 Controlar y registrar la administración del riesgo 76
8 DOCUMENTOS RELACIONADOS 76
8.1 documentos externos 77
9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN 77

1 OBJETIVO

Establecer la metodología para la identificación, análisis, valoración, definición de acciones de prevención, detección, corrección, mitigación y seguimiento a los riesgos de los procesos de la Superintendencia de Industria y Comercio-SIC, a través del desarrollo de la política de administración del riesgo adoptada por la Entidad.

2 DESTINATARIOS

La metodología para la administración de riesgos de la Superintendencia de Industria y Comercio aplica a los procesos planes y proyectos, de conformidad con cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso, gestores fiscales y la correspondencia con las líneas de defensa.

3 GLOSARIO

ACTIVIDAD (Plan de tratamiento del riesgo): acciones tendientes a fortalecer los controles identificados para mitigar los riesgos o a prevenir las causas señaladas en la identificación del riesgo.

ACTIVIDAD CRITICA: actividad fundamental dentro del proceso. Esta actividad se identifica en la parte del “HACER” de la caracterización del proceso. Por ser critica en el desarrollo del proceso, se debe ejercer un control para prevenir la materialización de riesgos con alta incidencia en el proceso.

ACTIVO: Son recursos tangibles e intangibles de la Entidad contable pública, obtenidos como consecuencia de hechos pasados y, de los cuales se espera que fluya un potencial de servicios o beneficios económicos futuros, a la Entidad contable pública en desarrollo de sus funciones de cometido estatal. Estos recursos, tangibles e intangibles, se originan en las disposiciones legales, en los negocios jurídicos y en los actos o hechos financieros, económicos, sociales y ambientales de la Entidad contable pública. Desde el punto de vista económico, los activos surgen como consecuencia de transacciones que implican el incremento de los pasivos, el patrimonio o la realización de ingresos. También constituyen activos los bienes públicos que están bajo la responsabilidad de las Entidades contables públicas pertenecientes al gobierno general.

ACTIVO DE INFORMACIÓN: En el contexto de seguridad de la información son elementos tales como aplicaciones de la organización, servicios web, redes,

Hardware, información física o digital, recurso humano, entre otros, que utiliza la Entidad para funcionar en el entorno digital.[1]

ACTIVO FIJO: Recurso tangible que posee una Entidad para su uso en la producción de bienes y prestación de servicios, para arrendarlos a terceros o para propósitos administrativos, sin que se tenga prevista su venta o suministro a la comunidad durante el ciclo normal de las operaciones y que se espera usar durante más de un período contable.

ACTIVO INTANGIBLE: Los activos intangibles son aquellos bienes que no pueden ser percibidos físicamente. Estos, aunque no se pueden ver ni tocar por su naturaleza inmaterial, igualmente aportan valor.

ACTIVO INTANGIBLE ADQUIRIDO: Activo intangible que obtiene la Entidad contable pública de un tercero, que puede ser otra Entidad contable pública o una Entidad privada.

ACTIVO INTANGIBLE DESARROLLADO: Activo intangible que genera internamente la Entidad contable pública.

ADMINISTRACIÓN 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. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de Planeación.

ANÁLISIS DEL RIESGO: busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias, este último aspecto puede orientar la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. El análisis del riesgo depende de la información obtenida en la fase de identificación de riesgos.

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

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.[2]

[1] Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, 2020. Departamento Administrativo de la Función Pública.
[2] Ibid. Pág 13.

BIEN: Son elementos materiales o inmateriales susceptibles de ser valuados en términos monetarios y objeto de conteos para su control. Pueden ser activos de cualquier clase, como por ejemplo el efectivo, activos fijos, artículos en proceso de producción.

BIENES INTANGIBLES: Bien inmaterial, o sin apariencia física, que pueda identificarse, controlarse, de cuya utilización o explotación pueden obtenerse beneficios económicos futuros o un potencial de servicios, y su medición monetaria debe ser confiable. Un activo intangible produce beneficios económicos futuros para la Entidad contable pública cuando está en la capacidad de generar ingresos, o cuando el potencial de servicios que posea genere una reducción de costos. Un activo intangible es controlable siempre que la Entidad contable pública tenga el poder de obtener los beneficios económicos futuros que procedan de los recursos que se derivan del mismo, y además pueda restringir el acceso de terceras persona a tales beneficios; puede identificarse cuando es susceptible de ser separado o escindido de la Entidad contable pública y vendido, cedido, dado en operación, arrendado o intercambiado; o cuando surge de derechos legales, con independencia de que esos derechos sean transferibles o separables de la Entidad o de otros derechos u obligaciones; y su medición monetaria es confiable cuando exista evidencia de transacciones para el mismo activo u otros similares, o la estimación del valor dependan de variables que se pueden medir.

CALIFICACIÓN DEL RIESGO: se logra a través de la estimación de la probabilidad de su ocurrencia y del impacto que puede causar la materialización del riesgo.

CATEGORÍA: criterio para clasificar una situación no deseada (riesgo).

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.[3]

CAUSAS (factores internos o externos): todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo[4].

CAUSA INMEDIATA: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.[5]

[3] Ibid. Pág 13.
[4] Ibid. Pág 12.
[5] Ibid. Pág 13.

CAUSA RAÍZ: causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.[6]

CONFIDENCIALIDAD: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados[7].

CONFLICTO DE INTERÉS: confrontación entre el deber público y los intereses privados de un servidor público y/o contratista, es decir, que éste tiene intereses personales y privados que podrían influenciar indebidamente alguna decisión o afectar la imparcialidad en la actuación de sus deberes y responsabilidades.

CONTEXTO ESTRATÉGICO: es un documento en donde se indican las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

CONTROL: cualquier medida que tome la dirección y/o líder de proceso (actividad, práctica, dispositivo u otra acción existente) para prevenir los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. Es una medida que permite reducir o mitigar un riesgo.

DESCRIPCIÓN: se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

DISPONIBILIDAD: propiedad de la información de estar accesible y utilizable a demanda por la Entidad.

EFECTOS (Consecuencias): es el resultado de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja, frente a la consecución de los objetivos institucionales.
Generalmente se dan sobre los productos o servicios derivados del proceso, las personas o los bienes materiales o inmateriales con incidencias importantes tales como sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio, daños físicos o daño ambiental.

EFECTO DAÑOSO[8]: 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.

[6] Ibid. Pág 13.
[7] Ibid. Pág 12.
[8] Ibid. Pág 68

EVALUACIÓN DEL RIESGO: busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final.

EVALUACION DE IMPACTO DE PROTECCIÓN DE DATOS: proceso ligado a los principios de protección de datos desde el diseño y protección de datos por defecto concebido para describir, de manera anticipada y preventiva, un tratamiento de datos personales, evaluar su necesidad y proporcionalidad y gestionar los potenciales riesgos para los derechos y libertades a los que estarán expuestos los datos personales en función de las actividades de tratamiento que se lleven a cabo con los mismos, determinando las medidas necesarias para reducirlos hasta un nivel de riesgo aceptable.

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. En esta guía, el evento potencial es equivalente a la causa raíz[9].

FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.[10]

GESTIÓN DEL RIESGO FISCAL: Son las actividades que debe desarrollar la Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos.[11]

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. A título de ejemplo son gestores fiscales, entre otro: representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.[12]

GESTOR PÚBLICO: Es todo servidor público, contratista, interventor o supervisor que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública,

[9] Ibid. Pág 69
[10] Ibid. Pág 12
[11] Ibid. Pág 12
[12] Ibid. Pág 12

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.[13]

IDENTIFICACIÓN DEL RIESGO: es una etapa del proceso de administración de riesgos en donde se determina qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.

INTEGRIDAD: propiedad de la información relacionadas con su exactitud y completitud.

IMPACTO: son las consecuencias que puede ocasionar a la organización la materialización del riesgo.

LÍNEAS DE DEFENSA: es el esquema que plantea el MECI a través del MIPG, que permite definir la responsabilidad y autoridad frente al control, y de sus 5 componentes (ambiente de control, evaluación del riesgo, actividades de control, información y comunicación y actividades de monitoreo), establecer al interior de las entidades, la efectividad de los controles diseñados desde la estructura de las demás dimensiones de MIPG. [14]

- LÍNEA ESTRATÉGICA: está bajo la responsabilidad de la alta dirección y del comité institucional de coordinación de control interno; su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes de la entidad.

- PRIMERA LÍNEA DE DEFENSA: está bajo la responsabilidad, principalmente, de los líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos y/o contratistas en todos los niveles de la organización); su rol principal es el mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol".

- SEGUNDA LÍNEA DE DEFENSA: esta línea está bajo la responsabilidad, principalmente, de los Jefes de planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, comités de riesgos (donde existan), comité de contratación, áreas financieras, de TIC, entre otros que respondan de manera directa por el aseguramiento de la operación; su rol principal es asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de

[13] Ibid. Pág 12
[14] Manual Operativo Modelo Integrado de Planeación y Gestión - MIPG

Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces; así mismo, consolidar y analizar información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos, todo lo anterior enmarcado en la "autogestión".

- TERCERA LÍNEA DE DEFENSA: esta línea está bajo la responsabilidad de los jefes de control interno o quienes hagan sus veces; desarrollaran su labor a través de los siguientes roles a saber: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento.

MAPA DE RIESGOS: matriz que representa los riesgos identificados para un proceso y describe las etapas adelantadas para su administración.

MONITOREO: comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el fin de identificar posibles cambios.

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.[15]

OBJETIVO DEL PROCESO: hace referencia al objetivo que se ha definido para el proceso (caracterización) al cual se le están identificando los riesgos.

PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.[16]

PLAN DE TRATAMIENTO DEL RIESGO: actividades tendientes a mejorar los controles identificados para mitigar los riesgos o las causas que originan el riesgo, los responsables de ejecutar dichas actividades y las fechas de ejecución.

PROBABILIDAD: posibilidad de ocurrencia del riesgo; ésta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de factibilidad teniendo en cuenta la presencia de factores

[15] Ibid. Pág 13
[16] Ibid. Pág 13

internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

PROCESO: conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

RIESGO: posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

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.[17]

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).[18]

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.[19]

RIESGO INHERENTE: nivel de riesgo propio de la actividad. Es el riesgo al que se enfrenta una entidad o proceso en ausencia de acciones que mitiguen su probabilidad de ocurrencia o el posible impacto de su materialización.

RIESGO RESIDUAL: nivel de riesgo que permanece luego aplicar controles al riesgo inherente.

TOLERANCIA DEL 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.[20]

VALORACIÓN DEL RIESGO: es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas.

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

[17] Ibid. Pág 12
[18] Ibid. Pág 13
19 Ibid. Pág 12
[20] Ibid. Pág 13

4 REFERENCIAS

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
Ley	610 de 2000	Por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías.	Artículos 3, 4, 5, 6, 7	Gestión fiscal Responsabilidad fiscal Daño patrimonial al Estado Pérdida, daño o deterioro de bienes
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.	Artículo 73	El Plan Anticorrupción y de Atención al Ciudadano que deben elaborar anualmente todas las Entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.
Ley	1437 de 2011	Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Artículo 11 y Artículo 12	Artículo 11 y Artículo 12
Ley	1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	Aplicación total	Aplicación total
Ley	1952 de 2019	Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario.	Artículo 44	Artículo 44
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.	Artículo 31	Artículo 31
Decreto	124 de 2016	Por el cual se sustituye el Titulo 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al Plan Anticorrupción y Atención al Ciudadano	Aplicación total	Aplicación total
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	Aplicación total	Aplicación total

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
		establecido en el artículo 133 de la Ley 1753 de 2015		
Decreto	612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.	Aplicación total	Aplicación total
Decreto	620 de 2020	"Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"	Capítulo 5	Capítulo 5

5 GENERALIDADES

Todas las actividades de una organización implican riesgo. Las organizaciones gestionan el riesgo mediante su identificación y análisis, para posteriormente evaluar si el riesgo se debería modificar por medio de la definición de controles y del tratamiento del riesgo con el fin de reducir la probabilidad de ocurrencia o prevenir y mitigar los impactos derivados de su materialización. La administración del riesgo es un proceso liderado por la Alta Dirección de la Entidad con la participación y compromiso de todos los servidores públicos y/o contratistas. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.

Para la implementación de esta metodología, se deben tener en cuenta los lineamientos definidos en la Política de Administración del Riesgo (Ver anexo 1), así como la Guía para la Administración del Riesgo y Diseño de Controles del Departamento Administrativo de la Función Pública.

La Superintendencia de Industria y Comercio administra sus riesgos a través del módulo de riesgos del Sistema Integrado de Gestión Institucional.

Los riesgos son identificados a través de los siguientes elementos:

- **Mapa de Riesgos de gestión:** Contiene los riesgos de la categoría “gestión” (contempla los riesgos fiscales y los riesgos de seguridad de la información) a los cuales están expuestos los procesos de la Entidad, el registro del mapa de riesgos por proceso se debe realizar en el módulo de riesgos del Sistema Integrado de Gestión Institucional.

- **Mapa de Riesgo de Corrupción:** Contiene el consolidado de los riesgos de la categoría “corrupción” y “fraude” a los cuales están expuestos los procesos de la Entidad. El registro del mapa de riesgos por proceso se debe realizar en el módulo de riesgos del Sistema Integrado de Gestión Institucional. **Mapa de Riesgo Institucional:** Contiene el consolidado de los riesgos (riesgos de gestión + riesgos de corrupción) a los cuales están expuestos los procesos de la Entidad.

5.1 CONTEXTO ESTRATÉGICO DEL RIESGO

La administración del riesgo requiere de un análisis inicial desde un punto de vista estratégico, por ello, se hace necesario estudiar el contexto del riesgo que es fundamental para identificar las fuentes que pueden dar origen al mismo. El contexto estratégico es analizado mediante la ejecución de la etapa 1 del proceso de Formulación de la Planeación Institucional DE01-P01, del cual se genera un documento para consulta y constituye el punto de partida para la planeación estratégica de la Entidad y la administración de riesgos.

Así mismo, el contexto estratégico del riesgo contempla el análisis de la misión, visión, objetivos estratégicos, los planes (Plan Estratégico Institucional, Plan de Acción, entre otros), los proyectos de inversión, los requisitos legales, quejas, denuncias o sugerencias realizadas por la ciudadanía, los indicadores, los mapas de riesgos anteriores, los resultados de las auditorías internas y externas del SIGI, las evaluaciones independientes realizadas por la OCI, los informes de seguimiento, los hallazgos de la auditoría gubernamental de la CGR, los procesos disciplinarios abiertos y los procesos del SIGI, todo lo anterior, define los límites sobre los cuales la Entidad va a centrar sus esfuerzos para la administración del riesgo.

5.2 ACTUALIZACIÓN DE LOS MAPAS DE RIESGO

Los mapas de riesgos de la Superintendencia de Industria y Comercio deberán ser revisados y en caso de ser necesario actualizados una vez al año, o antes si se presenta materialización del riesgo o el líder del proceso así lo solicita, de acuerdo con las fechas de corte definidas por la Oficina Asesora de Planeación.

Para la revisión periódica anual, el líder del proceso debe evaluar la información proveniente de quejas y denuncias presentadas por los ciudadanos para la identificación de riesgos de fraude y corrupción.

Así mismo, los planes de tratamiento de riesgos cuyas actividades finalicen en una vigencia, se deberán revisar con el propósito de formular nuevas actividades que permitan fortalecer los controles, eliminar las posibles causas generadoras de riesgos, identificar nuevos mecanismos de prevención, detección o corrección y continuar con el enfoque preventivo que permita la mitigación de los riesgos identificados.

De otra parte, el mapa de riesgos debe ser revisado y actualizado (en caso de ser necesario) así:

- Cuando se presenten, resultados de las evaluaciones llevadas a cabo por los organismos de control.
- Cuando se presenten, resultados de las evaluaciones llevadas a cabo por la Oficina de Control Interno Cuando haya cambios en el Direccionamiento Estratégico, Líder de proceso o cambios significativos en el entorno de la Entidad (cambio de gobierno, surgimiento de normativa, asignación de nuevas funciones, etc.) o al interior de la entidad (reestructuración, cambios en la planta de personal, modificaciones de funciones de los grupos de trabajo, creación de grupos, etc).

En cualquier caso, se deben atender los lineamientos del Procedimiento SC01-P05 Gestión del Cambio en el Sistema Integral de Gestión Institucional.

Nota 1: En caso de que uno o más criterios de revisión se presenten al mismo tiempo o en periodos de tiempo cortos, por ejemplo, cambios en el direccionamiento estratégico, cambios de líderes de proceso, cambios de gobierno, el proceso de planeación estratégica y la revisión anual de los mapas de riesgo, entre otros, la Oficina Asesora de Planeación definirá una única fecha en la que se realice la revisión de los mapas de riesgos, para evitar reprocesos.

5.3 ROLES Y RESPONSABILIDADES

Tabla 1. Responsables y responsabilidades frente al riesgo

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDADES FRENTE AL RIESGO
Estratégica	Comité Directivo y Comité Institucional de Gestión y Desempeño	• Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la Entidad y que puedan generar cambios en la estructura de riesgos y controles. • Garantizar el cumplimiento de los planes de la Entidad. • Generar recomendaciones de mejora a la política de administración del riesgo. • Promover la divulgación de la política de administración de riesgo en todos los niveles de la Entidad, de tal forma que se conozca claramente los niveles de responsabilidad y autoridad de las líneas de defensa frente a la gestión de riesgos de la Entidad.
	Comité Institucional de Coordinación de Control Interno.	• Establecer y aprobar la Política de administración del riesgo, la cual incluye los niveles de responsabilidad y autoridad. • Retroalimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes. que se deban hacer frente a la gestión del riesgo. • Realizar seguimiento y análisis periódico a los riesgos institucionales. • Realizar recomendaciones frente a la prevención y detección de situaciones indeseadas que puedan generar afectación económica o reputacional a la Entidad.
Primera Línea	Líderes de procesos y proyectos y equipos de trabajo (en general servidores públicos y contratistas de todos los niveles de la Entidad).	Líder del proceso: • Apoyar a la línea estratégica con la divulgación y socialización de la política de administración de riesgos, al interior de su equipo de trabajo. • Identificar y valorar los riesgos que pueden afectar los procesos a su cargo y actualizarlos cuando se requiera. • Definir, aplicar y hacer seguimiento a los controles diseñados para mitigar la probabilidad e impacto de la materialización de los riesgos identificados. • Proponer mejoras a la administración del riesgo en su proceso. • Supervisar la ejecución de los controles aplicados por su equipo de trabajo en la gestión diaria y detectar las deficiencias que éstos presenten e implementar las acciones

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDADES FRENTE AL RIESGO
		preventivas, correctivas y de mejora a que haya lugar. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. • Revisar que los controles diseñados se evidencien en los manuales, procedimientos o instructivos del proceso. • Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los procesos a su cargo e informar el avance de la implementación de los controles correctivos. • Realizar la medición y análisis a la gestión efectiva de los riesgos. • Revisar las acciones del plan de tratamiento establecido para cada uno de los riesgos, con el fin de que se ejecuten de forma adecuada. • Realizar y reportar el monitoreo correspondiente a los riesgos, con la oportunidad requerida, de acuerdo con el procedimiento establecido para el efecto por la Entidad. • Actualizar los mapas de riesgo de acuerdo con las autoevaluaciones, observaciones o informes de las auditorías internas o externas. • En caso de la materialización de un riesgo **no identificado**, este debe ser gestionado e incluido en el mapa de riesgo institucional. • En caso de materialización de riesgos, determinar la necesidad de implementar o no un plan de mejoramiento que aborde actividades preventivas y correctivas oportunas y eficaces para minimizar la posibilidad de nuevas materializaciones. • Revisar y actualizar en caso de ser necesario los riesgos con el acompañamiento de la OAP o en caso de los riesgos de seguridad de la información con la OTI. Servidores públicos y contratistas: • Participar en la administración de riesgos del proceso (identificación, valoración y tratamiento). • Ejecutar los controles que tiene a su cargo, conforme a lo establecido en su diseño. • Proponer mejoras a los controles a su cargo.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDADES FRENTE AL RIESGO
		• En caso de detectar riesgos materializados, informar al líder del proceso, con el propósito de implementar las acciones a que haya lugar. • En caso de identificar situaciones indeseadas que puedan afectar el objetivo o las actividades del proceso, informar al líder del proceso, con el propósito implementar las acciones a que haya lugar, con el acompañamiento de la OAP.
Segunda Línea	Oficina Asesora de Planeación	• Consolidar el Mapa de riesgos institucional, conformado por los mapas de riesgo de gestión y de corrupción. • Presentar al Comité de Coordinación de Control Interno, el seguimiento a los riesgos de mayor criticidad (riesgos residuales ubicados en zonas alta y extrema). • Actualizar la versión del mapa de riesgos de gestión y corrupción, de acuerdo con las solicitudes de modificación aprobadas. • Consolidar el reporte de monitoreo suministrado por los líderes de procesos. • Capacitar a los servidores públicos o contratistas designados en el módulo de administración del riesgo del SIGI.
	Oficina Asesora de Planeación Oficina de Tecnología e Informática (en lo referente a los riesgos de seguridad de la información) Líderes de los Sistemas de Gestión	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Acompañar, orientar y entrenar a los líderes de procesos y encargados de la identificación, análisis, valoración y monitoreo del riesgo. • Revisar los riesgos identificados en los procesos y realizar recomendaciones para el fortalecimiento de estos. • Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones para el fortalecimiento de estos. • Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología. • Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de sus procesos. • Recomendar a las áreas los ajustes a que haya lugar, con base en el monitoreo suministrado por los líderes de procesos.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDADES FRENTE AL RIESGO
		• Monitorear los riesgos identificados por la primera línea de defensa acorde con la información suministrada por los líderes de proceso.
Tercera Línea	Oficina de Control Interno	• Verificar y evaluar, a través de seguimientos o de auditorías internas, la adecuada identificación de riesgos, la efectividad de los controles y el plan de tratamiento, la implementación de controles correctivos, cuando aplique, el reporte oportuno y consistente del monitoreo e informar los resultados a los líderes de proceso y al Comité de Coordinación de Control Interno. • Proporcionar información sobre la efectividad del Sistema de Control Interno con un enfoque basado en riesgos. • Recomendar mejoras a la política de administración del riesgo. • Reportar en el Sistema de Alertas de Control Interno de la Contraloría General de la República hechos u operaciones, actos, contratos, programas, proyectos o procesos en ejecución, en donde, en el ejercicio de sus funciones, evidencien un riesgo de afectación o pérdida de los recursos públicos y/o de bienes o intereses patrimoniales de naturaleza pública.

Nota 2: La Oficina de Tecnología e Informática acompañará y asesorará todas las etapas de este procedimiento, cuando se trate de un riesgo de seguridad de la información.

Nota 3: Específicamente, la Oficina Asesora Jurídica es la responsable de brindar asesoría a los funcionarios y contratistas que presenten inquietudes respecto a la identificación y declaración de conflicto de intereses.

5.4 GENERALIDADES DEL CONFLICTO DE INTERÉS[21]

Es la confrontación entre el deber público y los intereses privados de un servidor público y/o contratista, es decir, que éste tiene intereses personales y privados que podrían influenciar indebidamente alguna decisión o afectar la imparcialidad en la actuación de sus deberes y responsabilidades.

[21] Guía para la identificación y declaración del conflicto de intereses en el sector público colombiano, 2019. Departamento Administrativo de la Función Pública.

5.3.1 Tipología de los conflictos de intereses

- **Real:** cuando el servidor y/o contratista se encuentra actualmente en una situación en la que debe tomar una decisión, pero, en el marco de esta, existe un interés particular que podría influir en sus obligaciones y responsabilidades.
- **Potencial:** cuando el servidor y/o contratista tiene un interés particular que podría influir en sus obligaciones y responsabilidades, pero aún no se encuentra en aquella situación en la que debe tomar una decisión. No obstante, esta situación podría producirse en el futuro.
- **Aparente:** cuando el servidor público y/o contratista no tiene un interés privado, pero alguien podría llegar a concluir, aunque sea de manera tentativa, que sí lo tiene. Una forma práctica de identificar si existe un conflicto de intereses aparente es porque el servidor puede ofrecer toda la información necesaria para demostrar que dicho conflicto no es ni real ni potencial.

5.3.2 Características:

- Son inevitables y no se pueden prohibir, ya que todo servidor público tiene familiares y amigos que eventualmente podrían tener relación con las decisiones o acciones de su trabajo.
- Pueden ser detectados, informados y desarticulados voluntariamente, antes que, con ocasión de su existencia se provoquen irregularidades o corrupción
- Se puede constituir en un riesgo de corrupción y, en caso de que se materialice, generar ocurrencia de actuaciones fraudulentas o corruptas.
- Afecta la imagen de transparencia y el normal funcionamiento de la administración pública.
- Mediante la identificación y declaración se busca preservar la independencia de criterio y el principio de equidad de quien ejerce una función pública, para evitar que el interés particular afecte la realización del fin al que debe estar destinada la actividad del Estado.

5.3.3 Materialización del conflicto de intereses y corrupción

La identificación, declaración y gestión del conflicto de intereses son prácticas preventivas y complementarias a los principios de acción basados en valores establecidos en el Código de Integridad. Es importante aclarar que el conflicto de intereses no representa, en sí mismo, corrupción; sin embargo, estos sí se constituyen como posibles fuentes generadoras (causas) de riesgos de corrupción o disciplinarios.

Ahora, en caso de que el juicio o la decisión profesional del servidor o contratista termina sesgada por el interés particular y, en consecuencia, obtenga un beneficio

directo o indirecto, la situación de conflicto se materializaría y esto se constituiría en un hecho de corrupción.

5.3.4 Diferencias entre conflicto de intereses y corrupción

	Conflicto de interés (riesgo de corrupción)	**Corrupción**
¿Qué es?	Una situación	Acción u omisión voluntaria
¿Por qué sucede?	Interés particular (legítimo)	Beneficio particular (ilegítimo)
¿Qué produce?	Tendencia o riesgo de sesgo en el juicio/decisión profesional	Decisión o juicio ya sesgado

Finalmente, a pesar de las diferencias abordando ambas líneas se puede emplear un enfoque moderno de la política de conflicto de intereses, a través de la identificación de riesgos, prohibiendo formas inaceptables de interés privado, dar a conocer las circunstancias en que pueden surgir conflictos y la garantía de procedimientos eficaces para resolver aquellas situaciones de conflicto de intereses con herramientas pedagógicas, detectivas y preventivas.

5.4 GENERALIDADES DEL CONTROL FISCAL INTERNO Y PREVENCIÓN DEL RIESGO FISCAL

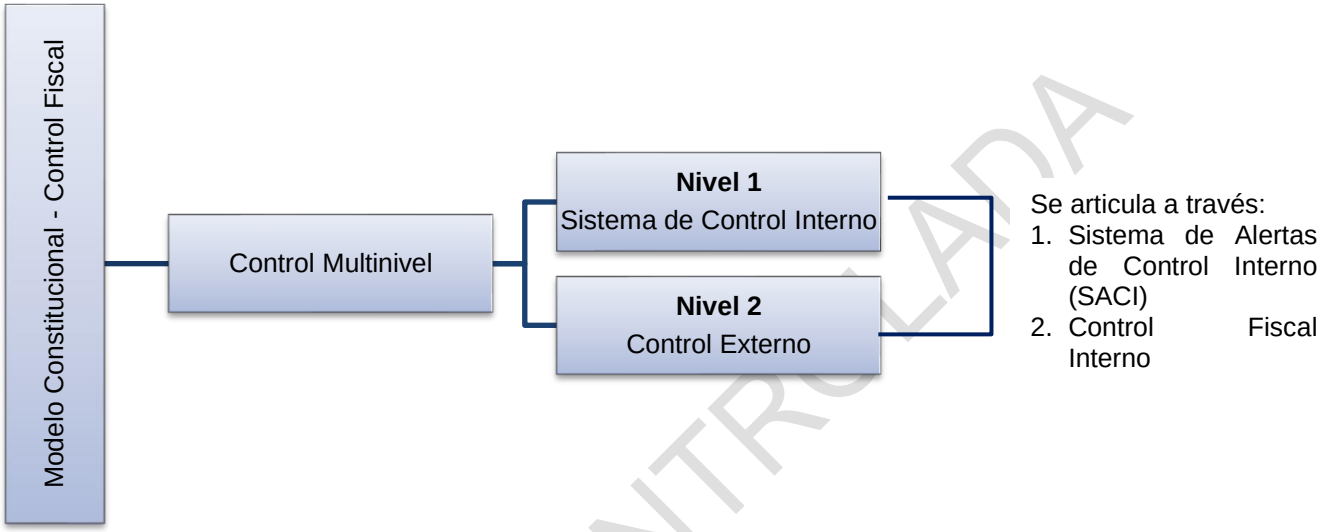
La gestión fiscal se entiende como el *conjunto de actividades económicas, jurídicas y tecnológicas, que realizan los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, tendientes a la adecuada y correcta adquisición, planeación, conservación, 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, con sujeción a los principios de legalidad, eficiencia, economía, eficacia, equidad, imparcialidad, moralidad, transparencia, publicidad y valoración de los costos ambientales* (Ley 610, 2000, Artículo 3).

De otra parte, la responsabilidad fiscal tiene como finalidad subsanar *los daños ocasionados al patrimonio público como consecuencia de la conducta dolosa o culposa de quienes realizan la gestión fiscal* (Ley 610, 2000, Artículo 3).

En este sentido, el propósito de la identificación, control y tratamiento de los riesgos fiscales es que la alta dirección y los gestores fiscales adopten acciones orientadas a prevenir el daño al patrimonio público, que se entiende como, *el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica* (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas).

5.4.1 Articulación entre el Control Fiscal y el Sistema de Control Interno

Ilustración 1. Articulación entre el modelo constitucional de control fiscal y el sistema de control interno



Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP), 2022

- Control Fiscal Multinivel: Es la articulación entre el control interno, el control externo y el control social.
- Control Fiscal Interno: Hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos, los gestores fiscales y de las líneas de defensa. *El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta.*

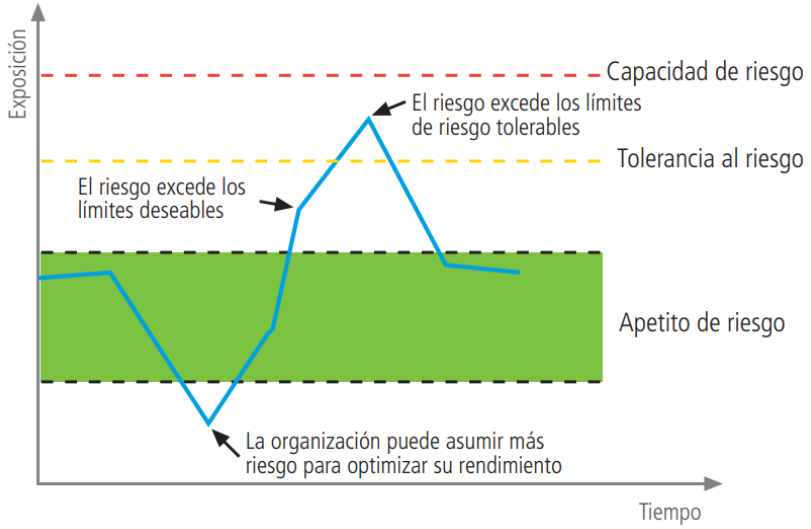
5.5 MARCO CONCEPTUAL PARA EL APETITO DEL RIESGO[22]

Tabla 2. Marco conceptual para el apetito del riesgo

CONCEPTO	¿A QUE HACE REFERENCIA?	DETERMINACIÓN
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.	Combinación de la probabilidad de ocurrencia e impacto de un riesgo
Capacidad de riesgo	Es el nivel máximo de riesgo que la Entidad puede soportar.	Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
Tolerancia del riesgo	Es la desviación máxima admisible del nivel del riesgo respecto al valor del apetito del riesgo. Sirve de alerta para no llegar al nivel que establece su capacidad.	Valor entre la capacidad y el apetito del riesgo.
Apetito de riesgo	Nivel de riesgo que la Entidad puede aceptar.	Valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos.

Fuente: Adaptación de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013 y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP), 2022.

Ilustración 2. Capacidad, tolerancia y apetito de riesgo



Fuente: Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013

22 Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, 2022. Departamento Administrativo de la Función Pública.

En este sentido, cuando el nivel de riesgo de gestión se encuentre en la zona moderada, alta o extrema, la opción para el tratamiento será reducir o compartir el riesgo y en el caso de los riesgos de gestión ubicados en zona baja, podrán ser asumidos o aceptados.

Para los riesgos de corrupción no hay aceptación del riesgo.

6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
1	**IDENTIFICAR EL RIESGO**	Contexto estratégico Caracterización del proceso Política de administración de Riesgos Módulo de riesgos SIGI	Esta etapa permite conocer los riesgos que pueden afectar el logro del objetivo o la gestión de cada proceso documentado, permite determinar las causas que originan el riesgo y/o los eventos no deseables con base al contexto y su tipología. Esta etapa está constituida por las siguientes actividades: - Analizar el objetivo del proceso - Establecer contexto estratégico del proceso - Identificar los activos de información del proceso - Identificar las actividades críticas del proceso - Establecer y priorizar los riesgos - Estructurar el riesgo identificado - Describir el Riesgo Identificado - Clasificar la tipología del Riesgo - Analizar Causas o vulnerabilidades	Líder de proceso Servidores Públicos y/o contratistas que realizan actividades del proceso	Riesgos Identificados: Módulo de riesgos SIGI

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
			- Analizar Consecuencias Potenciales		
2	**ANALIZAR Y CALIFICAR EL RIESGO ANTES DE CONTROLES (RIESGO INHERENTE)**	Riesgos Identificados: Módulo de riesgos SIGI	Esta etapa consiste en analizar el riesgo inherente sin considerar los controles que pudieran existir, estableciendo la probabilidad de ocurrencia y el nivel de consecuencia o impacto con el fin de estimar la zona de riesgo. En esta etapa se desarrollan las siguientes actividades: - Analizar y determinar la probabilidad - Analizar y determinar el impacto - Generar calificación y zona del riesgo inherente	Líder de proceso Servidores Públicos y/o contratistas que realizan actividades del proceso	Análisis del riesgo antes de controles: Módulo de riesgos SIGI
3	**IDENTIFICAR, CLASIFICAR Y VALORAR LOS CONTROLES**	Análisis del riesgo antes de controles: Módulo de riesgos SIGI	Esta etapa consiste en identificar los controles que en la actualidad se ejecutan con el fin de prevenir la materialización de los riesgos o mitigar los efectos de su materialización, clasificarlos y valorarlos de acuerdo al nivel de formalidad del control. En esta etapa se desarrollan las siguientes actividades: - Identificar controles - Valorar los controles	Líder de proceso Servidores Públicos y/o contratistas que realizan actividades del proceso	Identificación y valoración de controles: Módulo de riesgos SIGI

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
4	**ANALIZAR Y CALIFICAR EL RIESGO DESPUÉS DE CONTROLES (RIESGO RESIDUAL)**	Identificación y valoración de controles: Módulo de riesgos SIGI	En esta etapa se determina el riesgo no cubierto por los controles establecidos, una vez estos se han valorado, es decir el riesgo residual. Para ello, se desarrolla la siguiente actividad: - Calificar el riesgo residual - Seleccionar Opciones de Manejo	Líder de proceso Servidores Públicos y/o contratistas que realizan actividades del proceso	Análisis y calificación del riesgo después de controles: Módulo de riesgos SIGI
5	**FORMULAR PLAN DE TRATAMIENTO DEL RIESGO**	Análisis y calificación del riesgo después de controles: Módulo de riesgos SIGI	Consiste en formular el plan de tratamiento del riesgo residual, el cual comprende: opciones de manejo, actividades, responsable, fecha inicio y fecha terminación. El plan se formula a través de la ejecución de las siguientes actividades: - Formular actividades - Establecer responsables y fechas de ejecución de las actividades - Establecer mecanismo de detección de materialización - Modificar el plan de tratamiento, en caso de ser necesario	Líder de proceso Servidores Públicos y/o contratistas que realizan actividades del proceso	Plan de tratamiento del riesgo formulado: Módulo de riesgos SIGI

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
6	**APROBAR Y PUBLICAR EL MAPA DE RIESGOS EN EL APLICATIVO SIGI**	Módulo de riesgos SIGI totalmente diligenciado	En esta etapa se registra el mapa de riesgos en el aplicativo SIGI y el Líder lo aprueba para su posterior publicación. Las actividades por desarrollar son: - Enviar mapa de riesgos a revisión metodológica - Revisar metodológicamente el mapa de riesgos	Funcionario designado por el Líder de Proceso que ejerce el rol de "Enlace de Riesgos" Líder de proceso analizado Servidor Público o contratista designado de la OAP	Nueva versión del Mapa de Riesgos en el aplicativo SIGI – Módulo de Riesgos
7	**REALIZAR MONITOREO EVALUACIÓN Y SEGUIMIENTO**	Mapa de Riesgos por proceso en el Aplicativo SIGI- Módulo de Riesgos Plan de tratamiento del riesgo formulado: Módulo de riesgos SIGI	En esta etapa se realiza el monitoreo, evaluación y seguimiento de los riesgos documentados, así como la ejecución de las actividades establecidas en el plan de tratamiento de riesgos. Las actividades por realizar en esta etapa son: - Realizar monitoreo - Elaborar plan de mejoramiento en caso de materialización de un riesgo - Realizar evaluación y seguimiento	Líder de proceso Servidor Público o contratista designado de la OAP Oficina de Tecnología e Informática (Riesgos Seguridad de la Información) Oficina de Control Interno	Informe registrado en el Aplicativo SIGI- módulo de riesgos Evaluación y seguimiento de los mapas de riesgo por proceso en aplicativo SIGI- módulo de riesgos Módulo de riesgos y módulo de mejora del SIGI
8	**REALIZAR DIVULGACIÓN, COMUNICACIÓN, CONSULTA Y CONTROL DE LOS MAPAS DE RIESGOS**	Nueva versión del Mapa de Riesgos en el aplicativo SIGI – Modulo de Riesgos	En esta etapa se describen las actividades para hacer la consulta de los mapas de riesgo aprobados y publicados. En esta etapa se desarrollan las actividades de:	Servidores y Públicos y Contratistas de la SIC	Consulta y control del Mapa de Riesgos en el aplicativo SIGI – Modulo de Riesgos

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
			- Consultar mapa de riesgos - Controlar y registrar la Administración del Riesgo		

7 DESCRIPCION DE ETAPAS Y ACTIVIDADES

7.1 ETAPA 1: IDENTIFICAR EL RIESGO

La etapa de identificación del riesgo es recurrente y debe estar en permanente revisión y actualización, de acuerdo con la dinámica de los procesos de la Entidad. Esta etapa es desarrollada por el equipo de trabajo del proceso (líder y responsable de las actividades), acompañado por el equipo de administración de riesgos de la Entidad. Deben desarrollar las siguientes actividades:

7.1.1 Analizar el objetivo del proceso

El objetivo del proceso debe ser revisado con base en el marco estratégico de la Entidad (misión, visión y objetivos estratégicos). El objetivo del proceso debe responder a él "¿Qué hace el proceso?", "¿Para qué lo hace? y "¿Cómo lo hace?" y debe estar alineado con los objetivos estratégicos de la Entidad.

Si como resultado de este análisis se concluye la necesidad de ajustar el objetivo del proceso, se adelanta el respectivo ajuste conforme a lo establecido en el procedimiento SC01-P01 Documentación y Actualización del Sistema Integral de Gestión Institucional – SIGI.

7.1.2 Establecer contexto estratégico del proceso

Para determinar el contexto estratégico del proceso se determinan las características o aspectos esenciales del proceso y sus interrelaciones considerando:

- Objetivo del proceso
- Alcance del proceso
- Interrelación con otros procesos
- Procedimientos asociados
- Responsables del proceso

Las características anteriores conforman el contexto estratégico del proceso, se encuentran documentadas en la caracterización de cada uno de los procesos de la Entidad, para tal fin se encuentra el formato SC01-F09 Caracterización de Procesos.

7.1.3 Identificar los activos de información del proceso

La identificación de activos de información es una actividad previa requerida para la categorización de los riesgos de seguridad de la información y hace referencia a la identificación de la información o elementos de procesamiento de esta, que se recibe o produce en el ejercicio de las funciones asignadas a cada dependencia y es fundamental para desarrollar las actividades críticas del proceso. Incluye la información documental, software, servicios, hardware, elementos de red y personas.

Para identificar los activos de información del proceso se debe consultar el instructivo SC05-I02 “Metodología para la identificación, clasificación y valoración de activos de información” y registrarlos en el formato SC05-F03 “Registro de activos de información”.

Los líderes de los procesos de la SIC, son los responsables de identificar y mantener actualizados los activos de información que requieren de mayor protección para el cumplimiento misional de la Entidad, con el apoyo de la OTI a través de la Coordinación del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces.

7.1.4 Identificar las actividades críticas del proceso

Aunque en todas las actividades de un proceso se pueden presentar riesgos de diferente índole, es necesario priorizar las actividades críticas, a las cuales se les realizará el análisis de riesgos. Estas actividades son identificadas como críticas porque su ejecución tiene un mayor impacto sobre el resultado final esperado del proceso.

Las actividades críticas se identifican en la caracterización del proceso, en las actividades del HACER y la documentación relacionada en las mismas (procedimientos e instructivos), para su identificación se aplican los siguientes criterios:

- El resultado de la actividad tiene alta incidencia en el objetivo del proceso, es decir la actividad es clave para la ejecución de este.
- La materialización de algún riesgo en esa actividad afecta directamente el cumplimiento del objetivo del proceso (producto y/o servicio).

- La actividad tiene asociados controles preventivos, detectivos o correctivos que evitan situaciones no deseadas, o por sí misma es un control.
- En actividades posteriores no se ejercen controles más efectivos.
- Los controles que se aplican en estas actividades son recurrentes, se cuenta con evidencia de su aplicación y están definidos los responsables de aplicarlos.
- En la actividad se genera un registro (evidencia o un entregable final).

Nota 4: **En el caso de los procesos misionales,** *las actividades críticas tienen directa relación con la generación del producto no conforme.*

Las actividades críticas identificadas para el riesgo de la categoría *Indebida protección de datos personales* corresponden a aquellas actividades del proceso en donde se da tratamiento a bases de datos que contienen datos personales.

Las actividades críticas identificadas para el riesgo de la categoría *daño al patrimonio público* corresponden a aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas[23]. Es decir, son todas las actividades que representan gestión fiscal.

Una vez identificada(s) la(s) actividad(es) crítica(s) del proceso se copia la redacción de la(s) misma(s) en el módulo de riesgos del SIGI, en el espacio titulado “Actividad Crítica”.

7.1.5 Establecer y priorizar los riesgos

La identificación de riesgos se realiza en la(s) actividad(es) que han sido señalada(s) como crítica(s) y consiste en generar una lista de los eventos indeseados que pueden **entorpecer el cumplimiento de los objetivos**.

La identificación de riesgos se realiza a partir de juicios por parte de los ejecutores de las actividades de los procesos, basados en su experiencia, los registros generados del mismo, lluvia de ideas, análisis de la información reportada en sistemas de información y análisis de escenarios.

Preguntas clave para la identificación del riesgo

Para orientar la identificación de los riesgos, a continuación, se relacionan unas preguntas para tener en cuenta y que facilitarán el ejercicio:

[23] Ley 610 de 2000

- *¿La materialización del riesgo afecta el cumplimiento del objetivo del proceso?*
- *¿La materialización del riesgo afecta el producto y/o servicio de la actividad?*
- *¿La materialización del riesgo afecta la realización de otras actividades (subsiguientes a la señalada como critica)?*
- *¿Al materializarse ese riesgo, es necesario repetir actividades anteriores?*
- *¿La materialización del riesgo impide el cumplimiento de alguna normativa?*
- *¿La materialización del riesgo afecta la imagen de la Entidad?*
- *¿La materialización del riesgo interrumpe la operación de la Entidad?*
- *¿Se generan sanciones económicas, administrativas o disciplinarias cuando se materializa el riesgo?*
- *¿Podría propiciar quejas o reclamos de los usuarios o partes interesadas?*
- *¿La materialización del riesgo afecta el desempeño imparcial y objetivo de las funciones del servidor público?*
- *¿La materialización del riesgo afecta la confianza ciudadana en la administración pública?*
- *¿La materialización del riesgo podría afectar el cumplimiento del marco estratégico (misión, visión y objetivos estratégicos) de la Entidad?*
- ¿La materialización del riesgo tiene un efecto dañoso sobre el patrimonio público?
- ¿La materialización del riesgo tiene un efecto dañoso sobre los recursos públicos?
- ¿La materialización del riesgo tiene un efecto dañoso sobre los bienes públicos?

Nota 5: *Cuando el riesgo de gestión identificado no está relacionado directamente con el objetivo, este puede ser la causa o la consecuencia.*

7.1.6 Estructurar el riesgo identificado

Una vez identificado el enfoque del riesgo (gestión o corrupción), se debe estructurar el riesgo de la siguiente manera en el módulo de riesgos del SIGI:

a) Situación no deseada (seleccionar una categoría de riesgo)
b) Preposición
c) Evento

a. <u>Situación no deseada:</u>

Seleccionar la categoría en la cual se puede clasificar el riesgo. A continuación, se describen las situaciones no deseadas identificadas para los riesgos en la Superintendencia de Industria y Comercio:

CATEGORIZACIÓN	
SITUACIÓN NO DESEADA	**DESCRIPCIÓN**
Decisiones erróneas	Se manifiestan en diferentes ámbitos y se podría presentar cuando se definen lineamientos, políticas, estrategias, directrices que no son adecuadas o convenientes para la Entidad, la escogencia de alternativas que no son adecuadas, acertadas u oportunas. Esta categoría incluye errores de valoración los cuales hacen referencia, en forma exclusiva, a aquellas condiciones en las que una indebida valoración de elementos de prueba puede alterar los actos administrativos que resuelven situaciones jurídicas que le atañen al ciudadano. Ejemplo: Inadecuada programación, la inapropiada asignación de recursos, aplicación errónea de criterios o instrucciones, errores de juicio**,** errores de valoración, etc.
Incumplimientos legales	Se materializan con el no acatamiento de la normativa externa o interna.
Incumplimientos de compromisos (operativos, técnicos, presupuestales, otros)	Se materializan al pasar por alto los compromisos de la Entidad, incluyendo la imposibilidad de realizar las actividades del proceso, planes de acción o proyectos, demoras o retrasos en la ejecución, baja cobertura o falta de oportunidad.
Inexactitud	Se materializa al presentar datos o estimaciones equivocadas, incompletas, o desfiguradas, así como la inconsistencia e incoherencia en los actos administrativos y otros documentos de gestión.
Corrupción	Posibilidad de que, por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado[24].
Indebida Protección de datos personales	Se materializa al realizar un tratamiento de datos personales que desconozca todos los principios consagrados en la Ley 1581 de 2012, especialmente aquellas actuaciones desplegadas por la Entidad en donde se realice un acceso o una recolección de datos personales sin contar con una legitimidad legal para ello y sin el respeto mínimo por las reglas para obtener el consentimiento de las personas naturales, así como realizar un tratamiento respetuoso del principio de confidencialidad que asegure la reserva de la información por parte de los funcionarios y los contratistas, quienes solo deben acceder a información personal con ocasión de las actividades autorizadas por la Ley y el Manual de Funciones. El Riesgo también se materializa cuando datos personales de carácter privado, semiprivado y sensible se encuentran disponibles en internet. Se materializa cuando la Entidad no atiende oportunamente las consultas y los reclamos sobre protección de datos personales - Derecho Constitucional Habeas Data, en los términos establecidos por los artículos 14 y 15 de la Ley 1581 de 2012, debido a una clasificación errónea sobre las peticiones impidiendo de esta forma que la Oficina Asesora de Planeación conozca y tramite este tipo de peticiones en los tiempos establecidos por la ley. Igualmente, el riesgo se materializa cuando las áreas no realizan una gestión de bases de datos teniendo en cuenta las obligaciones administrativas que existen frente al Registro Nacional de Bases de Datos.

[24] Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, 2020. Departamento Administrativo de la Función Pública.

CATEGORIZACIÓN		
SITUACIÓN NO DESEADA		**DESCRIPCIÓN**
Uso indebido de activos físicos		Se materializa con el daño, pérdida, alteración, abandono, manipulación, uso inapropiado de los recursos físicos de la Entidad.
Daño al patrimonio público		Se materializa cuando se presenta menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado.
Hurto		Se materializa con la apropiación indebida, por parte de un servidor o de terceros de propiedad física, financiera e intelectual de la Entidad.
Fraude		Se materializa al inducir a cometer un error para obtener una resolución contraria a la ley; así como evitar el cumplimiento de obligaciones impuestas. También al obtener mediante maniobras engañosas una ventaja en detrimento de alguien – sustracción maliciosa que alguien hace a las normas de la ley o a las de un contrato en perjuicio de otro.
Seguridad de la Información	**Pérdida de confidencialidad**	La pérdida de confidencialidad se presenta cuando información sensible se expone a personas no autorizadas, ya sea por brechas de seguridad como hackeos o phishing, errores humanos al compartir datos por accidente, fallas en políticas de seguridad, robo o extravío de dispositivos que contienen datos sensibles, o incluso filtraciones deliberadas, destacando la importancia de medidas como encriptación, controles de acceso y políticas claras para prevenir y mitigar este tipo de exposición no autorizada de información.
	Pérdida de disponibilidad	La pérdida de disponibilidad ocurre cuando la información o los recursos no están accesibles para aquellos que tienen autorización para usarlos. Esto puede suceder por diversos motivos, como ataques cibernético, ataques de denegación de servicio (DDoS) que sobrecargan los sistemas, fallos en la infraestructura tecnológica, interrupciones del servicio debido a desastres naturales o incluso errores humanos al realizar mantenimiento o actualizaciones incorrectas. La pérdida de disponibilidad puede tener impactos significativos en la operatividad de sistemas y organizaciones, resaltando la importancia de medidas como la redundancia, sistemas de respaldo, protocolos de recuperación de desastres y mantenimiento adecuado para garantizar la continuidad operativa.
	Pérdida de integridad	La pérdida de integridad se produce cuando la información sufre modificaciones no autorizadas o no deseadas, afectando su precisión, confiabilidad o consistencia. Esto puede ocurrir debido a ataques informáticos como alteraciones maliciosas de datos, errores en la transmisión o almacenamiento de información, corrupción de archivos debido a fallas en el hardware o software, manipulación no autorizada de datos por parte de usuarios internos o externos, entre otros factores. La pérdida de integridad subraya la necesidad de implementar medidas como controles de acceso, sistemas de detección de intrusiones, firmas digitales, copias de seguridad y verificación periódica para garantizar que la información mantenga su integridad y sea precisa y fiable.

Nota 6: *Excepcionalmente puede presentarse que una situación no deseada, no se encuentre categorizada en el listado anterior, en tal caso, se debe informar a la OAP, para que se realice la correspondiente inclusión como una nueva categoría, en caso de ser necesario.*

Nota 7: El conflicto de interés es entendido como una situación que se puede presentar a cualquier servidor público y/o contratista de la Entidad, por lo que en sí mismo no constituye un riesgo o una situación indeseada. Por lo anterior, el conflicto de interés y la no declaración oportuna de este, se configura como una causa que puede generar una situación indeseada o riesgo, bien sea de corrupción o de gestión.

Nota 8: Es posible que situaciones no deseadas como i) incumplimientos legales, ii) incumplimiento de compromisos, y iii) uso indebido de activos, puedan tener efectos dañosos sobre el patrimonio público, en este caso el riesgo se deberá clasificar en la tipología de "Riesgo Fiscal", de acuerdo con el numeral 7.1.8.

b. Preposición:

A continuación, se debe establecer una preposición que permita relacionar la situación no deseada, escogida, con el evento. Se recomienda utilizar las siguientes preposiciones según la situación no deseada:

- Decisiones erróneas: al, durante, en, para, sobre.
- Incumplimientos legales: al, ante, con, durante, en.
- Incumplimientos de compromisos: al, ante, con, durante, en, hacia.
- Uso indebido de activos: al, de, durante, en, para, sobre.
- Hurto: de, durante, en, mediante, para.
- Fraude: de, durante, en, mediante, para.
- Inexactitud: al, con, de, durante, en, para, sobre.
- Corrupción: al, durante, por, en, para.
- Indebida Protección de datos personales: al, durante, por, en.
- Interrupción: al, durante, por, ante, de.
- Seguridad de la información: al, durante, por, en, sobre, ante, de.
- Daño al patrimonio público: al, durante, mediante, en

Nota 9: *Se recomienda analizar cuidadosamente el uso de la preposición "por" debido a que se podría asimilar el complemento con una causa.*

c. Evento:

El evento describe el hecho asociado al riesgo que se está analizando, teniendo en cuenta la categoría y preposición escogida, por lo general coincide con la ejecución de la actividad crítica o el objetivo del proceso o procedimiento.

Posibles eventos de corrupción:

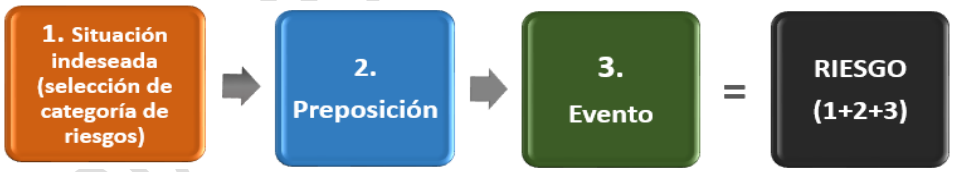
Descripción de posibles eventos	
Establecer adendas que cambian condiciones generales del proceso para favorecer a grupos determinados	Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica
Amiguismo y clientelismo	Archivos contables con vacíos de información
Cobrar por realización del trámite, (Concusión)	Concentración de autoridad o exceso poder
	Interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación
Decisiones ajustadas a intereses particulares	Inclusión de gastos no autorizados
Dilatación de los procesos con el propósito de obtener el vencimiento de términos o la prescripción del mismo	Restricción de la participación a través de visitas obligatorias innecesarias, establecidas en el pliego de condiciones
Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular	Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación (estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular)
Extralimitación de funciones, abuso de función pública: realizar funciones públicas diversas de las que legalmente le correspondan	Fallos amañados
Ocultar a la ciudadanía la información considerada pública	Imposibilitar el otorgamiento de una licencia o permiso
Inadecuada supervisión de contratos	Exceder las facultades legales en los fallos
Pliegos de condiciones hechos a la medida de una firma en particular	Soborno (Cohecho)
Urgencia manifiesta inexistente	
Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión	Tráfico de influencias, (persona influyente)
Fallos en el suministro de cualquier servicio público (agua, energía, comunicaciones) por parte de un proveedor	Eventos sísmicos / incendios / inundaciones/ pandemia que impidan acceder a la sede física de la SIC

En el caso de los riesgos de seguridad de la información, a continuación, se detallan posibles eventos a utilizar:

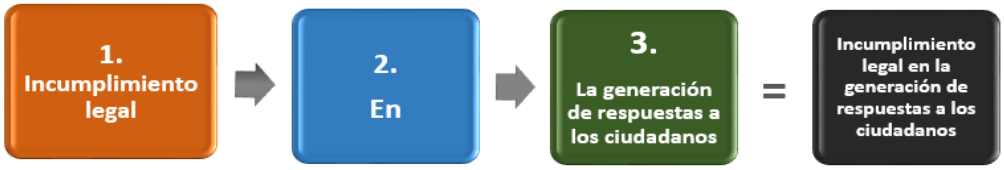
Descripción de posibles eventos de seguridad de la información	
Compartir información clasificada o reservada de forma accidental o deliberada.	Ataques informáticos.
Asignar inadecuadamente permisos de acceso a la información.	Suplantación de identidad.
Teletrabajo con insuficientes medidas de protección de la información.	Recuperación de información desde los backups.
Contratar personal sin la suficiente verificación de antecedentes.	Ingreso a las oficinas de personal externo no autorizado.

Descripción de posibles eventos de seguridad de la información	
Finalizar los contratos sin revocación de permisos de acceso.	Mantenimiento inadecuado de equipos de cómputo.
Transferencia de información física o electrónica sin medidas de protección adecuadas.	Dejar la información expuesta en sitio de trabajo y equipo de cómputo sin bloquear
Almacenar información sensible en medios extraíbles sin protección (USB, Disco duro).	Utilizar programas no confiables o no autorizados.
Fallas técnicas de los sistemas de información	Compartir información con proveedores sin el establecimiento de cláusulas o acuerdos de confidencialidad.
Retirar de la Entidad documentación física sin protección.	Divulgar las contraseñas de acceso.
Usar correos electrónicos personales para tratar información institucional.	Omitir la asignación de deberes y responsabilidades sobre la información.
Clasificar erróneamente la información clasificada y reservada.	Renuncia de personal clave sin empalme adecuado.
Ocurrencia de eventos naturales como; Fuego o agua, sin medidas de preparación suficiente.	Contar con colaboradores con falta de conciencia en seguridad de la información.
Alteración de información de los sistemas clave del proceso.	Uso de componentes con vulnerabilidades conocidas.

En resumen, esta es la estructura con la que se debe construir un riesgo:



Ejemplo:



Para facilitar la identificación de riesgos de corrupción se debe analizar la “matriz de definición de riesgo de corrupción”, de acuerdo con la matriz, si se marca con una x en la estructura del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

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

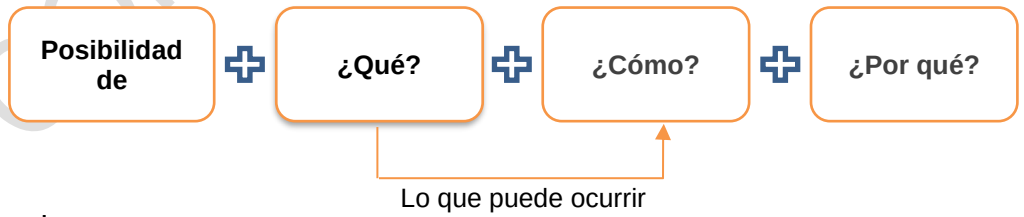
7.1.7 Describir Riesgo Identificado

Posterior a la estructuración del riesgo, se realiza la descripción de este, en la cual se indican las características generales o las formas en que se observa o manifiesta el riesgo identificado. Se debe redactar allí la especificidad de lo que se quiere controlar.

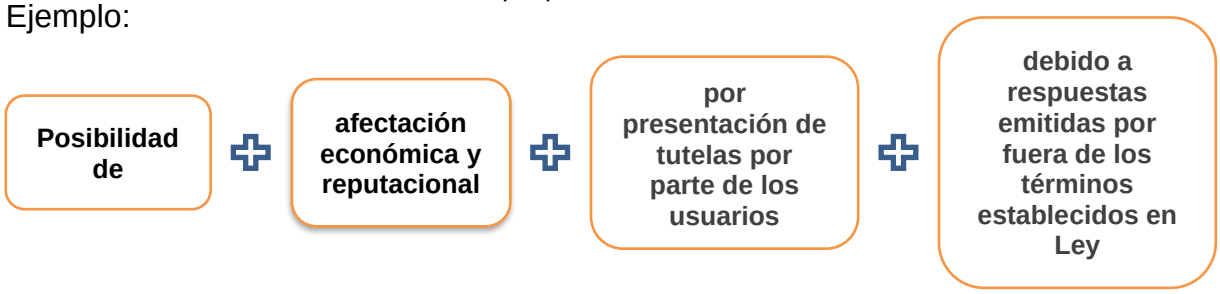
La descripción del riesgo debe ser redactada tal forma que sea clara y comprensible para el líder de proceso, para los servidores públicos y contratistas, para la ciudadanía, grupos de valor y partes interesadas. En este sentido, se deben tener en cuenta la siguiente estructura:

Debe iniciar con la frase	¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de	Afectación económica o Afectación reputacional	Circunstancia que puede dar origen al riesgo	La razón principal por la que se puede presentar el riesgo.

En resumen, la descripción del riesgo se debe estructurar de la siguiente manera:



Ejemplo:



Para el caso de la redacción riesgos de Seguridad de la Información, se presenta un ejemplo:

PROCESO: Atención al Ciudadano			
Actividad Critica	**Riesgo**	**Descripción del Riesgo**	**Activo de información afectado**
Brindar información a los ciudadanos del estado de los trámites que se encuentran en proceso y de los procedimientos a seguir.	Perdida de la integridad al asignar inadecuadamente permisos de acceso a la información.	La información que se tramita en el proceso puede sufrir alteraciones, dado que todos los colaboradores del grupo de trabajo son administradores de la carpeta compartida donde es consolidada.	Carpeta compartida en Drive.

En el caso de los riesgos de corrupción, en la descripción se deben comprender los componentes de su definición, así: Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado, es decir: **La posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.**

Para la redacción de la descripción de los riesgos fiscales, se debe tener en cuenta la siguiente estructura:

Debe iniciar con la frase	**¿Qué?**	**¿Cómo?**	**¿Por qué?**
Posibilidad de	Efectos dañosos sobre bienes públicos Efectos dañosos sobre recursos públicos O Efectos dañosos sobre intereses patrimoniales de naturaleza pública	Circunstancia que puede dar origen al riesgo	La razón principal por la que se puede presentar el riesgo. En su descripción se debe redactar claramente el evento, es decir acción u omisión

Se presentan los siguientes ejemplos, para la redacción de los riesgos fiscales:

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 (DAFP), 2022

Nota 10: no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales representan un efecto económico.

7.1.8 Clasificar la tipología del Riesgo

Para facilitar el proceso de identificación del riesgo se realiza la clasificación de estos teniendo en cuenta las siguientes tipologías:

- **Riesgo Estratégico:** se asocia con la forma en que se administra la Entidad. Es la posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos y por tanto impactan toda la Entidad.

- **Riesgo de imagen o reputacional:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de la Entidad, ante sus clientes, usuarios, ciudadanos o partes interesadas.

- **Riesgos Operativos:** posibilidad de ocurrencia de eventos que afecten los procesos misionales de la Entidad. Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la

definición de los procesos, de la estructura organizacional, de la articulación entre dependencias o de la falta de control.

- **Riesgos Protección de Datos Personales:** posibilidad de ocurrencia que afecten la información de bases de datos que contengan datos personales por un manejo erróneo de éstas y que tienen el potencial de afectar los derechos y libertades de los titulares de los datos personales.

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

- **Riesgos tecnológicos:** Fallas en la planificación, gestión y monitoreo de la ejecución de proyectos, relacionados con la tecnología, productos, servicios, procesos, personal y canales de envío.

- **Riesgo de continuidad de negocio:** Se asocia a la posibilidad de presentarse interrupciones en la prestación de trámites y servicios de carácter misional de la Entidad, debido a incidentes o desastres originadas por la naturaleza, el hombre, la tecnología o la cadena de suministros.

- **Riesgos de Cumplimiento:** se asocian con la capacidad de la Entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad. Es la posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

- **Riesgos de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado [25].

- **Riesgos de seguridad de la información:** Posibilidad de ocurrencia de modificaciones no autorizadas de la información, pérdida de disponibilidad o uso inadecuado de la información.

- **Riesgos Fiscales:** Posibilidad de que por acción u omisión exista un efecto dañoso sobre los recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

[25]Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, 2020. Departamento Administrativo de la Función Pública.

7.1.9 Analizar Causas o Vulnerabilidades

Posterior a la descripción del riesgo se analizan las causas, es decir, los medios, las circunstancias y agentes generadores del mismo, lo cual se entiende como todos los sujetos u objetos que tienen la capacidad de originar un riesgo. Estas causas pueden ser internas al ser atribuidas a personas, métodos, equipos, materiales e instalaciones, directamente involucradas en los procesos; o externas cuando provienen del entorno en el que la Entidad desarrolla sus funciones.

En el entorno de los riesgos de seguridad de la información y protección de datos personales las causas se conocen como vulnerabilidades. Para identificarlas, se debe realizar un análisis de las amenazas que pueden generar la vulnerabilidad, a continuación, se presenta un listado de posibles amenazas de seguridad de la información y de protección de datos personales.

AMENAZAS DE SEGURIDAD DE LA INFORMACIÓN	
Abuso de los derechos	Fallo de servicios de información
Acceso no autorizado	Falta de disponibilidad del personal
Revelación de contraseñas	Gestión ineficiente de la seguridad de la información
Saturación de los sistemas de información	Hackers
Software malicioso	Información de fuentes no confiables
Suplantación de identidad	Interrupción de los procesos
Cambio en permisos de acceso	Investigados o vigilados
Denegación de servicios	Manipulación de sistemas de información
Desastres naturales	Pérdida de la información
Destrucción de la información	Pérdida de los registros
Deterioro de los soportes	Pérdida de servicio de comunicaciones de datos
Divulgación no autorizada	Pérdida o modificación de la información
Entes de control	Personal externo no autorizado
Errores operativos	Empleado descontento
Espionaje	Falla en el software
Estafadores	Fallo de equipos

AMENAZAS DE DATOS PERSONALES	
TIPO	**AMENAZA**
GENERALES	
Técnico	Carencia de procedimientos y medidas de seguridad adecuadas o de la ineficacia de estas, en el tratamiento de datos personales
Organizacional	Deficiente gestión de la privacidad de las personas
Organizacional	Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.
Organizacional	Incorporación tardía del responsable en protección de datos al proyecto o definición deficiente de sus funciones y competencias
LEGITIMACIÓN DE LOS TRATAMIENTOS Y CESIONES DE DATOS PERSONALES	
Legal	Tratar o ceder datos personales cuando no es necesario para la finalidad perseguida
Legal	Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales
Legal	Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales
Organizacional	Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión
Organizacional	Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros
Legal /Organizacional	Solicitar y tratar datos sensibles sin adoptar las salvaguardias necesarias
Técnico	Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada.
Legal	Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable
TRANSFERENCIAS Y TRANSMISIONES INTERNACIONALES	
Legal	Acceso secreto a los datos personales por parte de autoridades de terceros países
Organizacional / técnico	Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transmisión
Legal	Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados
Organizacional	Incapacidad de ayudar a los ciudadanos en el ejercicio de sus derechos ante el encargado de tratamiento internacional.
NOTIFICACIÓN DE LOS TRATAMIENTOS	
Organizacional	Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe notificarse la creación, modificación o cancelación de un tratamiento de datos personales al RNBD o a la autoridad de protección de datos competente
TRANSPARENCIA DE LOS TRATAMIENTOS	
Legal	Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada.
Legal	En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o

AMENAZAS DE DATOS PERSONALES	
	diseminada en diversas secciones y apartados que hagan muy difícil su acceso conjunto y detallado
Legal	Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales
CALIDAD DE LOS DATOS	
Legal	Solicitar datos o categorías de datos innecesarios para las finalidades
Técnico / Organizacional	Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas
Legal	Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos
Técnico /Legal	Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas —Datos transaccionales, de navegación o de geolocalización para la monitorización del comportamiento, la realización de perfiles y la toma de decisiones sobre las personas. —Toma de decisiones económicas, sociales, laborales, etc. relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables), especialmente si pueden ser adversas o discriminatorias, incluyendo diferencias en los precios y costos de servicios y productos o trabas para el paso de fronteras. —Toma de decisiones automatizadas con posibles consecuencias relevantes para las personas. —Utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas.
Legal	Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) sobre personas específicas mediante la utilización de técnicas de inteligencia artificial (en particular, minería de datos), reconocimiento facial o análisis biométricos de cualquier tipo
Legal /Organizacional	Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron
DATOS ESPECIALMENTE PROTEGIDOS	
Legal	Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando este sea la causa que legitima su tratamiento o cesión
Legal	Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos sensibles
Legal	Disociación deficiente o reversible que permita la re-identificación de datos sensibles en procesos de investigación que solo prevén utilizar datos anónimos.
DEBER DE SECRETO	
Legal /Organizacional /Técnico	Accesos no autorizados a datos personales

AMENAZAS DE DATOS PERSONALES	
Organizacional / Legal	Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización
TRATAMIENTOS POR ENCARGO	
Legal	Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas
Organizacional	Falta de diligencia (o dificultad para demostrarla) en la elección del encargado de tratamiento
Legal / Técnico	Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad
Legal / Organizacional	No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos CARS realizados ante los encargados de tratamiento
Legal	Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato
DERECHOS DE HABEAS DATA	
Legal	Dificultar o imposibilitar el ejercicio de los derechos a Conocer Actualizar Rectificar y Suprimir
Legal / Organizacional	Carencia de procedimientos y herramientas para la gestión de los derechos CARS
Organizacional / técnico	Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los titulares de los datos personales.
MEDIDAS DE SEGURIDAD	
Organizacional	Inexistencia de Responsable de Privacidad o deficiente definición de sus funciones y competencias
Legal / Organizacional	Inexistencia de Documento de Seguridad
Organizacional	Deficiencias organizativas en la gestión del control de accesos
Técnico	Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales
Técnico	Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información
Técnico	Uso de identificadores que revelan información del afectado
Técnico	Afectación de los procesos de negocio por fallas en la disponibilidad de la información, pérdida de integridad y exposición indebida de datos personales como resultado de incidentes en la organización
Técnico	Deficiencias en la protección de la confidencialidad de la información
Organizacional	Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo, enfocado a la protección de los datos personales.
Técnico	Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados

AMENAZAS DE DATOS PERSONALES	
PROCEDIMIENTOS	
Técnico	Inadecuada implementación de las Políticas de copia de seguridad SC05-POL01
Técnico	Errores en la ejecución de Copias de Seguridad y almacenamiento y gestión de soportes.
Técnico	Inadecuada implementación del Procedimiento de acceso Lógico GS01-P24
Técnico	Inadecuada implementación del Procedimiento de gestión de incidentes SC05-P01
Técnico / Organizacional	Inadecuada implementación de la Políticas de correo electrónico SC05-POL01
Organizacional	Inexistencia de Procedimiento de custodia de documentos
Organizacional	Inexistencia de Procedimiento de entrada y salida de soportes y documentos
Organizacional	Inadecuada implementación del procedimiento de archivo y retención documental GD01-P01
Organizacional	Inadecuada implementación de la Políticas Seguridad de oficinas, recintos e instalaciones SC05-POL01
Organizacional	Inexistencia de Procedimiento de copia y reproducción de documentos
Organizacional	Inexistencia de Procedimiento de desechado y reutilización de soportes en papel
Organizacional	Inexistencia de Procedimiento de desechado y reutilización de soportes automatizados
Organizacional	Inexistencia de Procedimiento de traslado de documentos
Técnico / Organizacional	Fuga de información a través de canales de correo electrónico como resultado de fallas en la definición de normas internas para el manejo de los recursos tecnológicos
Técnico	Afectación de la integridad y/o confidencialidad de los datos personales sujetos a tratamiento en la organización a causa de fallas en los mecanismos de control de acceso a nivel lógico y/o físico
Técnico / Organizacional	Pérdida de integridad de la información relacionada con datos personales como resultado de fallas en la ejecución de copias de respaldo o de la restauración de las mismas

A continuación, se presenta ejemplos de posibles causas generadoras para cada una de las situaciones no deseadas:

CATEGORIZACIÓN DE SITUACIÓN NO DESEADA	EJEMPLOS DE CAUSAS
Decisiones Erróneas	- Errores en la información que soportan las decisiones. - Errores de juicio. - Aplicación errónea de criterios o instrucciones para la realización de actividades. - La no declaración oportuna de un conflicto de interés se puede constituir en una causa de decisiones erróneas por conflicto de intereses.

CATEGORIZACIÓN DE SITUACIÓN NO DESEADA	EJEMPLOS DE CAUSAS
Incumplimientos legales	- Ejecución de operaciones desconociendo el marco legal establecido. - Actos accidentales o por descuido de los servidores públicos de la entidad o de terceros. - La no declaración oportuna de un conflicto de interés se puede constituir en una causa de decisiones erróneas por conflicto de intereses.
Incumplimientos de compromisos (operativos, técnicos, presupuestales, otros)	- Errores en la información que soportan la ejecución de los compromisos. - Inadecuada programación - Asumir responsabilidades que exceden las capacidades de la Entidad y que no se puedan realizar oportuna o adecuadamente. - La no declaración oportuna de un conflicto de interés se puede constituir en una causa de decisiones erróneas por conflicto de intereses.
Uso indebido de activos	- Accidentes y desastres naturales. - Uso inapropiado. - Falta de idoneidad o capacitación en el manejo de los activos - La no declaración oportuna de un conflicto de interés se puede constituir en una causa de uso indebido de activos por conflicto de intereses. - La no declaración oportuna de un conflicto de interés se puede constituir en una causa de decisiones erróneas por conflicto de intereses.
Daño al patrimonio público	- Errores en la supervisión de contratos - Inadecuada gestión de activos tangibles de la Entidad - Inadecuada gestión de activos intangibles de la Entidad - Error en avalúos
Hurto	- Desviación de los activos de la Entidad para usos diferentes a los establecidos - Sustracción deliberada de activos.
Fraude	- Alterar, ocultar o desviar la información de las operaciones y transacciones de la Entidad. - La no declaración oportuna de un conflicto de interés se puede constituir en una causa de fraude por conflicto de intereses.
Inexactitud	- Errores en la información que soportan la ejecución de actividades - Aplicación errónea de criterios o instrucciones para la realización de actividades. - Actos accidentales o por descuido de los servidores públicos de la entidad o de terceros. - La no declaración oportuna de un conflicto de interés se puede constituir en una causa de inexactitud por conflicto de intereses
Corrupción	En la identificación de las causas de los riesgos cuya categoría sea corrupción, se busca “identificar un conjunto sistemático de situaciones que por sus características pueden originar prácticas corruptas” así mismo, es conveniente analizar los hechos de corrupción presentados en procesos similares de otras entidades.

CATEGORIZACIÓN DE SITUACIÓN NO DESEADA	EJEMPLOS DE CAUSAS
Indebida Protección de datos personales	- Errores en seguridad de la información (en la recolección de la información- Incumplimiento al Instructivo de Seguridad de la Información y al acuerdo de confidencialidad de la información). - Aplicación errónea de criterios o instrucciones para la conservación de la información. - Aplicación errónea de criterios o instrucciones para el tratamiento de la información. - La no declaración oportuna de un conflicto de interés se puede constituir en una causa de decisiones erróneas por conflicto de intereses.
Interrupción	- Epidemias / Pandemias - Interrupción de servicios públicos esenciales - Sismos con afectación a la sede principal de la SIC - Vandalismo y atentados terroristas - Inundación - Incendio

Para los riesgos de corrupción, a continuación, se presenta un listado con posibles causas:

EJEMPLOS DE CAUSAS INTERNAS	EJEMPLOS DE CAUSAS EXTERNAS
Ausencia Cultura de Buen Gobierno	Ocurrencia de hechos de corrupción
Falta de control al poder	Cambios en la alta dirección
Baja visibilidad de las acciones	Apatía de los grupos de interés
Discrecionalidad de los servidores públicos	Ofrecimiento de dinero, regalos de un usuario a un servidor público con el fin de obtener un beneficio particular
Designar supervisores que no cuentan con conocimientos suficientes o que supervisan múltiples contratos	Desconocimiento de los usuarios en el manejo del sistema de trámites para consulta y este pueda ofrecer un pago para la realización de la solicitud.
Baja rotación del personal que atiende público al interior de la entidad	Cambios regulatorios y técnicos que generen confusiones en materia de competencias legales Impacto de las decisiones que toma la entidad
Conocimientos limitados de los funcionarios que intervienen en la elaboración de documentos relacionados con la contratación	Extorsión por parte de un usuario a un servidor público
Falta de Planeación y de coherencia en la ejecución de los planes que realiza la entidad	
Concentración de conocimiento por nivel de especialización	
Bajo desarrollo de los procesos y procedimientos institucionales	
Gestión documental deficiente	

EJEMPLOS DE CAUSAS INTERNAS	EJEMPLOS DE CAUSAS EXTERNAS
Asimetrías de la información	
Desmotivación de funcionarios	
Alta rotación de personal	
Herramientas informáticas poco confiables y oportunas	
Gran demanda de información personalizada por la ciudadanía	
Insuficiente capacidad instalada	
Concentración de información de determinadas actividades o procesos en una persona	
Sistemas de información susceptibles de manipulación o adulteración	
Infraestructura física no adecuada para la atención de usuarios	
Bajo nivel de automatización al seguimiento de los procesos	
La no declaración oportuna de un conflicto de interés	
Aceptar el ofrecimiento de dinero o regalos de un usuario	
Desconocimiento del concepto de conflicto de intereses y del procedimiento para gestionarlo preventivamente	

Para los riesgos de seguridad de la información, a continuación, se presenta un listado con posibles causas/vulnerabilidades:

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE-INFRAESTRUCTURA	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del Sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y 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	Falta de mantenimiento al aire acondicionado de los equipos.
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
SOFTWARE-APLICACIONES INFORMATICAS	Ausencia de “terminación de 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
	Ausencias 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 las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	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 controlado 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
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
REDES DE COMUNICACIONES	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	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas 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.
	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
PERSONAS	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
INSTALACIONES	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	*Hurto de medios o Documentos * Espionaje/ Phishing
	Ubicación en área susceptible de inundación	*Daños físicos en la infraestructura *Perdida de equipos y datos. *interrupción de servicios.
	Red energética inestable	*Perdida de equipos y datos. *interrupción de servicios.
	Ausencia de protección física de la edificación (Puertas y ventanas)	*Acceso no autorizado *Riesgo de intrusiones *Robo de equipos
DATOS / INFORMACIÓN	Falta de cifrado	Acceso no autorizado a los datos.
	Políticas de retención inadecuadas	Fuga de datos.
	Insuficiencia en las copias de seguridad	Pérdida o corrupción de datos por ataques de malware.
EQUIPOS AUXILIARES	Falta de mantenimiento regular	Daños físicos o fallas por condiciones inesperadas
	Configuraciones predeterminadas inseguras en dispositivos de red auxiliares	Robo o vandalismo que afecta la disponibilidad y funcionalidad
	Acceso físico no protegido a los equipos auxiliares	Robo o vandalismo que afecta la disponibilidad y funcionalidad
SERVICIOS	Falta de actualizaciones de software	Explotación de vulnerabilidades conocidas por parte de atacantes para obtener acceso no autorizado o comprometer la integridad de los servicios.
	Configuraciones por defecto inseguras	Acceso no autorizado a los servicios debido a contraseñas débiles o permisos predeterminados no seguros.
	Carencia de monitoreo y registro	Dificultad para detectar intrusiones o actividades maliciosas en los servicios, lo que podría permitir a los atacantes realizar acciones no autorizadas sin ser detectados fácilmente.
SOPORTES DE INFORMACIÓN	Almacenamiento sin cifrado	Acceso no autorizado a la información almacenada en soportes físicos (discos duros, USB) que no están cifrados, lo que podría exponer los datos a personas no autorizadas si los dispositivos se pierden o son robados.
	Falta de control de acceso físico	Posible manipulación, robo o acceso no autorizado a los soportes de información debido a la ausencia de restricciones de acceso físico a los lugares donde se almacenan.

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	Falta de respaldo y redundancia	Riesgo de pérdida total de información si no se realizan copias de seguridad de los datos almacenados en estos soportes, ya que no habría forma de recuperar la información en caso de daño o pérdida del soporte principal.
BASES DE DATOS	Falta de parches de seguridad y actualizaciones	Explotación de vulnerabilidades conocidas en la base de datos por parte de atacantes para obtener acceso no autorizado, modificar o robar información.
	Contraseñas débiles o mal gestionadas	Acceso no autorizado a la base de datos debido a contraseñas débiles, compartidas o mal gestionadas, lo que podría permitir a atacantes comprometer la seguridad de los datos.
	Falta de cifrado de datos sensibles	Acceso no autorizado o robo de datos sensibles almacenados en la base de datos, ya que la información no está cifrada, lo que facilita su exposición si se produce un acceso no autorizado.

Nota 11: Las causas, pueden ser actualizadas, teniendo en cuenta el análisis del contexto estratégico que se identifica o actualiza en la planeación estratégica. Ejemplo del análisis de causas:

PROCESO: Atención al Ciudadano			
Actividad Critica	**Riesgo**	**Descripción del Riesgo**	**Causas**
Brindar información a los ciudadanos del estado de los trámites que se encuentran en proceso y de los procedimientos a seguir.	Incumplimiento legal en la generación de respuestas a los ciudadanos	Posibilidad de afectación económica y reputacional por presentación de tutelas por parte de los usuarios, debido a respuestas emitidas por fuera de los términos establecidos en Ley	-Registros erróneos o falta de registros -Falta de personal frente al alto volumen de solicitudes

A continuación, se presentan algunos ejemplos que relaciona el riesgo de seguridad de la información con la amenaza y la vulnerabilidad.

PROCESO: Atención al Ciudadano					
Actividad Critica	**Riesgo**	**Descripción del Riesgo**	**Activo de información afectado**	**Amenaza**	**Vulnerabilidad**
Brindar información a los ciudadanos del estado de los trámites que se encuentran en proceso y de los procedimientos a seguir.	Perdida de la integridad al asignar inadecuadamente permisos de acceso a la información.	La información que se tramita en el proceso puede sufrir alteraciones, dado que todos los colaboradores del grupo de trabajo son administradores de la carpeta compartida donde es consolidada.	Carpeta compartida en Drive.	Empleado descontento	Ausencia de revisión de derechos de acceso.
PROCESO: Gestión Documental					
Actividad Critica	**Riesgo**	**Descripción del Riesgo**	**Activo de información afectado**	**Amenaza**	**Vulnerabilidad**
Recibir, verificar, registrar, radicar, digitalizar, indexar, organizar y encasillar los documentos de entrada, salida y traslado.	Perdida de la confidencialidad al clasificar erróneamente la información pública, clasificada y reservada.	Pueden ocurrir errores al momento de clasificar la correspondencia de entrada, permitiendo que información clasificada y reservada pueda ser consultada.	Corresponden cia diaria	Acceso no autorizado	Asignación errada de los derechos de acceso

Una vez identificadas las causas/vulnerabilidades, se selecciona el factor interno o externo relacionado de acuerdo con el siguiente listado:

Factor interno	Descripción
Competencias	Se refiere a la formación, experiencia y habilidades del personal
Comunicación	Se refiere a la información que fluye dentro de la Entidad, lo que se informa, los mensajes que se emiten, el tipo y medios para trasmitir información, quien y como se comunica información en la Entidad o en el proceso.
Cultural	Se refiere al conjunto de comportamientos, ideas, tradiciones y costumbres que caracterizan a los servidores públicos o contratistas de la Entidad
Documentación	Se refiere a la información que está en algún medio de soporte (físico o virtual). Procesos, procedimientos, instructivos, formatos, actos administrativos. La causa puede estar orientada a que no existe la documentación o la que existe es insuficiente, desactualizada o incompleta.
Estratégicos	Se asocia con la forma en que se administra la Entidad, se relaciona a asuntos globales relacionados con la misión y el cumplimiento de los objetivos

Factor interno	Descripción
	estratégicos, la clara definición de políticas, diseño y conceptualización de la Entidad por parte de la alta dirección.
Financiero	Se refiere a la disposición o no de recursos monetarios. Limitaciones de presupuesto, restricciones presupuestales, aplazamiento o recortes.
Infraestructura	Se refiere a la existencia y condiciones de la infraestructura con la que cuenta la entidad: espacios físicos, equipos informáticos, capacidad de archivo, implementos de trabajo.
Jurídico	Se refiere a las disposiciones legales que se han establecido dentro de la Entidad las cuales pueden o no existir, ser insuficientes, poco precisas, ambiguas, poco flexibles.
Logístico	Se refiere al conjunto de los medios necesarios para llevar a cabo un fin determinado de un proceso, las estrategias, el tiempo, la organización y disposición de recursos.
Método	Se refiere a la manera como se han establecido las formas, mecanismos, procesos para realizar determinadas funciones o tareas.
Seguridad	Se refiere a la ausencia o insuficiencia de mecanismos que permitan garantizar el resguardo, la confianza, la presencia de riesgos o eventos indeseados que pudieran provocar pérdidas de recursos de toda índole.
Sistemas de Información	Se refiere a la ausencia, disponibilidad, restricción, limitación, complejidad, insuficiencia de los sistemas de información que soportan actividades dentro de la Entidad.
Tecnología	Se refiere a la ausencia, disponibilidad, limitación, complejidad de instrumentos, recursos técnicos o procedimientos empleados en un determinado proceso.

Factor externo	Descripción
Económicos	Se refiere a la existencia de políticas monetarias, fiscales y situaciones económicas como la inflación, el aumento de salario mínimo, cambios en las tasas de interés, devaluación de la moneda, cambios en la TRM, etc, que pueden afectar o incidir en el desempeño de la Entidad.
Imagen	Se refiere a la percepción que personas u organizaciones externas tienen respecto de la función, desempeño, rol y actuaciones de la Entidad, es lo que proyecta la Entidad.
Legal	Hace referencia a los preceptos legales dictados por una autoridad competente y que pueden afectar o incidir en las actuaciones y desempeño de la Entidad.
Medioambientales	Se refiere a las condiciones del entorno, fenómenos naturales, recursos naturales escasos que podrían incidir en el desempeño de la Entidad.
Políticos	Son los referentes a todo lo que implica una posición de poder, en sus diferentes niveles, que tendrán una repercusión en la Entidad.
Sociales	Hace referencia a aspectos y modelos culturales, creencias, actitudes, etc, así como a las características demográficas.
Tecnológicos	Son los derivados de los avances científicos, el empleo de la tecnología como instrumento para competir, lo cual puede tener una incidencia positiva o adversa sobre el desempeño de la Entidad.

7.1.10 Analizar Consecuencias Potenciales

El análisis de consecuencias consiste en identificar el efecto que tiene la ocurrencia del riesgo sobre el logro de los objetivos del proceso o la Entidad. Ejemplo: sanciones, demandas, pérdida de imagen y alto nivel de quejas por parte de la ciudadanía.

Existen dos tipos de efectos, los inmediatos que afectan el desarrollo de actividades posteriores del proceso y los extremos que se relacionan con efectos legales, sanciones o afectación en la operación de la Entidad. El análisis debe realizarse considerando tres enfoques: la Entidad, los procesos y las personas.

De acuerdo con la categoría de situaciones no deseadas, a continuación, se relaciona un listado de consecuencias potenciales:

CATEGORIZACIÓN DE SITUACIÓN NO DESEADA	EJEMPLOS DE CONSECUENCIAS POTENCIALES
Decisiones Erróneas	- Pérdida de credibilidad y confianza en la Entidad. - Pérdidas económicas en la Entidad. - Quejas y reclamos de los clientes (internos y/o externos)
Incumplimientos legales	- Sanciones Legales. - Pérdidas económicas por multas a la Entidad - Incremento de costos por prórrogas y adiciones a presupuestos. - Sobrecostos por reproceso, duplicidad o inactividad y detrimento del patrimonio - Pérdida de credibilidad y confianza por incumplimiento de responsabilidades y tareas encomendadas.
Incumplimientos de compromisos (operativos, técnicos, presupuestales, otros)	- Afectación en la operación (misional y/o apoyo) de la entidad - Pérdida de credibilidad y confianza por no cumplir con responsabilidades y tareas encomendadas. - Quejas y reclamos de los clientes (internos y/o externos)
Uso indebido de activos	- Pérdida de la información. - Pérdidas económicas por desuso, reparación o reposición de instalaciones, equipos, accesorios y herramientas de trabajo. - Fallas de hardware y software. - Detrimento de seguridad de los activos que soportan la prestación de los servicios.
Hurto	- Pérdida de la información. - Pérdidas Económicas. - Detrimento del patrimonio de la Entidad. - Quejas y reclamos de los clientes (internos y/o externos)
Fraude	- Afectación en la operación (misional y/o apoyo) de la entidad - Pérdida de credibilidad y confianza a nivel de áreas - Quejas y reclamos de los clientes (internos y/o externos) - Pérdidas Económicas. - Detrimento del patrimonio de la Entidad.

CATEGORIZACIÓN DE SITUACIÓN NO DESEADA		EJEMPLOS DE CONSECUENCIAS POTENCIALES
Inexactitud		- Pérdida de credibilidad y confianza en la Entidad. - Afectación en la operación (misional y/o apoyo) de la entidad - Sobrecostos por reproceso, duplicidad o inactividad y detrimento del patrimonio
Daño al patrimonio público		- Pérdida de credibilidad y confianza en la Entidad. - Detrimento del patrimonio de la Entidad. - Detrimento de seguridad de los activos que soportan la prestación de los servicios. - Sanciones Legales - Investigaciones disciplinarias
Corrupción		- Pérdida de credibilidad y de confianza en la Entidad. - Investigaciones disciplinarias - Pérdida de transparencia y la probidad en la Entidad. - Sobrecostos por reproceso, duplicidad o inactividad y detrimento del patrimonio
Indebida Protección de datos personales		- Pérdida de credibilidad y confianza por no cumplir con responsabilidades y tareas encomendadas en la protección de datos personales. - Pérdida de la información. - Investigación disciplinaria por parte de la procuraduría.
Interrupción		- Pérdida de información. - Imposibilidad de prestar trámites y servicios - Pérdidas Económicas. - Afectación a la integridad física de personas
Seguridad de la Información	**Pérdida de confidencialidad**	- Perdida de información. - Quejas y reclamos de los clientes (internos y/o externos) - Pérdida de credibilidad y confianza en la Entidad. - Afectación en la operación (misional y/o apoyo) de la entidad - Sobrecostos por reproceso, duplicidad o inactividad y detrimento del patrimonio - Demandas - Investigaciones disciplinarias
	Pérdida de disponibilidad	
	Pérdida de integridad	

7.2 ETAPA 2: ANÁLIZAR Y CALIFICAR EL RIESGO ANTES DE CONTROLES (RIESGO INHERENTE)

Esta etapa es desarrollada por el equipo de trabajo del proceso (líder y responsable de las actividades), acompañado por el equipo de administración de riesgos de la Entidad. Consiste en analizar el riesgo inherente al que se enfrenta la Entidad en ausencia de acciones para modificar su probabilidad o impacto (controles), y considerando la naturaleza y la forma como se llevan a cabo las actividades del proceso. Para ello, se determina la probabilidad de ocurrencia y el impacto de la

materialización de cada riesgo, identificado bajo unos supuestos en donde los controles para prevenir o mitigar el riesgo no existen o no se aplican.

7.2.1 Analizar y determinar la probabilidad

En esta actividad se establece la frecuencia con la que se ha presentado (si ha pasado) o puede presentarse el riesgo o se mide en términos de la factibilidad con la que el riesgo se podría llegar a materializar, teniendo en cuenta la presencia y exposición ante factores internos y externos. Es importante tener en cuenta el análisis de aspectos como:

- ✓ Las fuentes mencionadas en este documento en el capítulo 5.1 Contexto Estratégico.
- ✓ Número de riesgos materializados (si ha pasado) en un periodo determinado, cuando se cuenta con un historial de situaciones o eventos asociados al riesgo
- ✓ **Número de veces que se realiza la actividad crítica en el periodo de un año**
- ✓ Número de personas que intervienen en la realización de la actividad
- ✓ Grado de tecnificación, automatización de la actividad

De acuerdo con el análisis, para los riesgos de gestión, se selecciona el grado de probabilidad con base en la siguiente tabla:

DESCRIPTOR	FRECUENCIA DE EJECUCIÓN DE LA ACTIVIDAD CRÍTICA	FRECUENCIA	PROBABILIDAD
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	No se ha presentado en los últimos 5 años	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	Al menos 1 vez en los últimos 5 años	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 300 veces por año	Al menos 1 vez en los últimos 2 años	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 301 veces al año y máximo 5000 veces por año	Al menos 1 vez en el último año.	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5001 veces por año	Más de 1 vez al año.	100%

De acuerdo con el análisis, para los riesgos de corrupción, se selecciona el grado de probabilidad con base en la siguiente tabla:

CALIFICACIÓN	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

En caso de no tener información documentada que pueda determinar la frecuencia se debe hacer un análisis a través de la experiencia de los responsables y colaboradores del proceso para determinar la factibilidad de ocurrencia de la materialización del riesgo.

7.2.2 Analizar y determinar el impacto

En este aspecto se establece la magnitud de los efectos ocasionados con la materialización del riesgo cuando no existen controles. De acuerdo con un análisis cualitativo, se selecciona el nivel con base en las siguientes escalas de impacto:

DESCRIPTOR	AFECTACIÓN ECONÓMICA	AFECTACIÓN REPUTACIONAL	IMPACTO
Leve	Afectación menor a 10 SMLMV	Si el hecho llega a presentarse, tendría consecuencias o efectos mínimos sobre la imagen de la Entidad	20%
Menor	Entre 11 y 50 SMLMV	Si el hecho llega a presentarse, tendría bajo impacto o efecto sobre la imagen de la Entidad	40%
Moderado	Entre 51 y 100 SMLMV	Si el hecho llega a presentarse, tendría medianas consecuencias o efectos sobre la imagen de la Entidad	60%
Mayor	Entre 101 y 500 SMLMV	Si el hecho llega a presentarse, tendría altas consecuencias o efectos sobre la imagen de la Entidad	80%
Catastrófico	Mayor a 501 SMLMV	Si el hecho llega a presentarse, tendría desastrosas consecuencias o efectos sobre la imagen de la Entidad	100%

Nota 12: Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

Para los riesgos de corrupción el impacto se mide según el efecto que puede causar el hecho de corrupción al cumplimiento de los fines de la Entidad, para determinar la calificación se debe diligenciar la siguiente encuesta:

ENCUESTA PARA DETERMINAR EL IMPACTO DEL RIESGO			
N°	**PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…**	SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de 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 calidad de vida de la comunidad por la pérdida del bien, servicios o 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?		

En la siguiente tabla se relaciona la medición del impacto para el riesgo de corrupción de acuerdo con la cantidad de respuestas afirmativas de la encuesta:

NIVEL DE IMPACTO	NO. DE RESPUESTAS AFIRMATIVAS	DESCRIPCION
MODERADO	Una a cinco	Afectación parcial al proceso y a la dependencia (genera medianas consecuencias para la entidad)

MAYOR	Seis a once	Impacto negativo de la Entidad (Genera altas consecuencias para la Entidad)
CATASTRÓFICO	Doce a diecinueve	Consecuencias desastrosas sobre el sector (genera consecuencias desastrosas para la Entidad)

Nota 13: *Si la pregunta 16 es afirmativa, el riesgo se considera catastrófico.*

Ningún riesgo de corrupción debe ser calificado como insignificante o menor, dado que estos riesgos siempre son significativos para la Entidad.

7.2.3 Generar calificación y zona del riesgo inherente

Una vez se ha determinado la probabilidad e impacto del riesgo, automáticamente el módulo de riesgos del SIGI establece la ubicación de los riesgos de acuerdo con el análisis de probabilidad e impacto realizado. A continuación, se detallan las zonas en las cuales puede ubicarse el riesgo de gestión:

PROBABILIDAD	IMPACTO				
	Leve (20%)	Menor (40%)	Moderado (60%)	Mayor (80%)	Catastrófico (100%)
Muy alta (100%)	**A**	**A**	**A**	**A**	**E**
Alta (80%)	**M**	**M**	**A**	**A**	**E**
Media (60%)	**M**	**M**	**M**	**A**	**E**
Baja (40%)	**B**	**M**	**M**	**A**	**E**
Muy baja (20)	**B**	**B**	**M**	**A**	**E**

B: Zona de riesgo Bajo
M: Zona de riesgo Moderado
A: Zona de riesgo Alto
E: Zona de riesgo Extremo

Cuando el riesgo, antes de controles, quede ubicado en una zona baja, no se debe continuar con las etapas posteriores (descritas en los siguientes capítulos de este documento). Lo anterior, considerando que es un riesgo ya controlado y será asumido y no requiere la aplicación de controles, diferentes a los propios del proceso. No obstante, y de acuerdo con lo establecido en el numeral 7 de la Política de Administración de Riesgos (Ver Anexo 1), se debe realizar un monitoreo trimestral.

Para el caso de los riesgos de corrupción:

PROBABILIDAD	IMPACTO		
	Moderado (3)	Mayor (4)	Catastrófico (5)
Rara vez (1)	**M**	**A**	**E**
Improbable (2)	**M**	**A**	**E**
Posible (3)	**A**	**E**	**E**
Probable (4)	**A**	**E**	**E**
Casi Seguro (5)	**E**	**E**	**E**

M: Zona de riesgo Moderado
A: Zona de riesgo Alto
E: Zona de riesgo Extremo

7.3 ETAPA 3: IDENTIFICAR, CLASIFICAR Y VALORAR LOS CONTROLES

Esta etapa es desarrollada por el equipo de trabajo del proceso (líder y responsables de las actividades), acompañado por el equipo de administración de riesgos de la Entidad, y consiste en identificar, y valorar los controles que en la actualidad se aplican en el proceso y/o definir nuevos con el propósito de disminuir la probabilidad de ocurrencia del riesgo o mitigar su impacto. En ese sentido, se desarrollan las siguientes actividades:

7.3.1 Identificar controles

Consiste en identificar los controles que en la actualidad se ejecutan o definir nuevos con el fin de prevenir la ocurrencia del riesgo o mitigar los efectos de su materialización.

Para los procesos misionales se debe tener en cuenta lo establecido en el procedimiento CI02-P03 Producto No Conforme, específicamente la Identificación y Tratamiento Producto no Conforme, en la sección “PUNTO DE CONTROL”, ya que si los controles definidos en esta columna no son coherentes con los descritos en el mapa de riesgos, el líder del proceso deberá actualizar la información relacionada con los controles del proceso a su cargo y remitirla a la Oficina Asesora de Planeación, para su actualización en el SIGI.

Nota 14: *Es necesario que las personas que participan en la identificación de controles tengan conocimiento de la ejecución del proceso, así como de las herramientas informáticas utilizadas, la normativa que reglamenta las actividades, los documentos asociados, registros, entre otros.*

Nota 15: *Para el caso de los controles de seguridad de la información, ver el Anexo 2 de este documento, donde se describen los controles establecidos en la norma ISO 27001:2013.*

Para una adecuada redacción del control se deben tener en cuenta los siguientes pasos:

Paso 1: El control podría estar documentado

Teniendo en cuenta que los controles son acciones ejecutadas por los servidores públicos o contratistas de la Entidad y hacen parte de la operación del proceso, se recomienda que estos se encuentren documentados.

Paso 2: El control debe tener definido el responsable de llevar a cabo la actividad.

La persona asignada para ejecutar el control debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser segregadas o redistribuidas entre diferentes servidores públicos y/o contratistas, de esta forma minimizar el riesgo de error o de actuaciones irregulares.

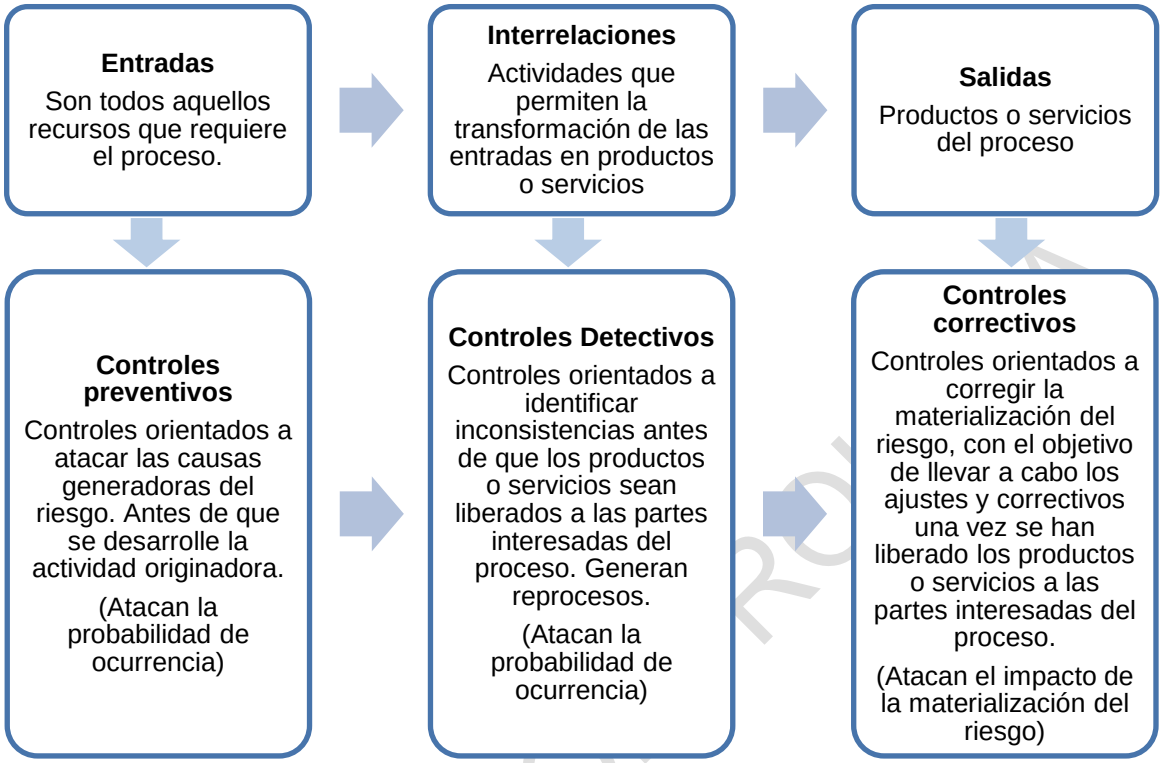
Paso 3: El control debe tener una periodicidad definida para su ejecución.

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

Paso 4: Se debe indicar cuál es el propósito del control.

El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a **prevenir** las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar, etc.), **detectar** inconsistencias antes de que los productos o servicios sean liberados a las partes interesadas del proceso y **corregir** una vez se ha materializado el riesgo, con el objetivo de llevar a cabo los ajustes a que haya lugar.

En este sentido, hay relación entre el ciclo de los procesos y las tipologías de los controles, como se presenta en la siguiente figura:



Nota 16: *El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir, detectar o corregir la materialización del riesgo*, por lo tanto, no se recomiendan como controles.

Paso 5: Se debe establecer el cómo se realiza la actividad de control.

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

Paso 6: Se debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.

El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Si como resultado de un control preventivo o detectivo se observan diferencias o aspectos que no se cumplen, la actividad no debe continuar hasta que se subsane la situación.

Paso 7: El control debe dejar evidencia de su ejecución.

El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control.

7.3.2 Valorar los controles

La valoración de los controles de los riesgos de gestión se realiza respecto a los siguientes atributos:

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 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.	-
		No documentado	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.	

La valoración de los controles de los riesgos de corrupción se realiza respecto al análisis y evaluación del diseño del control de acuerdo con las siete (7) variables establecidas:

NO.	CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1	**Documentación del control**	¿Existen documentos donde se indique la aplicación del control y su periodicidad?	Documentado	10
			No Documentado	0
2	**Responsable**	¿Existe un responsable asignado a la ejecución del control?	Asignado	10
			No Asignado	0
		¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	10
			Inadecuado	0
3	**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
4	**Propósito**	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir	15
			Detectar	10
			No es un control	0
5	**Cómo se realiza la actividad de control**	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15
			No Confiable	0
6	**Qué pasa con las observaciones o desviaciones**	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
			No se investigan y resuelven oportunamente.	0
7	**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

Resultados de la evaluación del diseño del control

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

RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO – PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 90 y 100
Moderado	Calificación entre 80 y 89
Débil	Calificación entre 0 y 79

Resultados de la evaluación de la ejecución del control

Aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurarse por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación realizadas con auditorías internas, control interno y/o seguimiento periódico por el líder del proceso.

RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	RESULTADO DE LA EJECUCIÓN DEL CONTROL
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

7.4 ETAPA 4: ANALIZAR Y CALIFICAR EL RIESGO DESPUÉS DE CONTROLES (RIESGO RESIDUAL)

7.4.1 Calificar el riesgo residual

En el caso de los riesgos de gestión, una vez valorados los controles, automáticamente el módulo de riesgos del SIGI califica el riesgo residual, para el cálculo se debe tener en cuenta que los controles mitigan el riesgo de forma acumulativa, es decir, que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante, por ejemplo:

La valoración del control corresponde a la sumatoria de la valoración del tipo de control y la valoración del tipo de implementación.

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de afectación económica y reputacional por presentación de tutelas por parte de los usuarios, debido a respuestas emitidas por fuera de los términos establecidos en Ley	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%*40%=24% 60%-24%=36%
	Valor probabilidad para aplicar el segundo control	36%	Valoración control 2 detectivo	30%	36%*30%=10,8% 36%-10,8=25,2%
	Probabilidad residual	25,20%			
	Impacto inherente	80%			
	Nose tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto residual	80%			

En el caso de los riesgos de corrupción, una vez valorados los controles, automáticamente el módulo de riesgos del SIGI califica el riesgo residual y para el cálculo del riesgo residual, se debe consolidar el conjunto de los controles, para evaluar si estos de manera individual y en conjunto sí ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución individual y promedio de los controles.

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

PESO DEL DISEÑO DE CADA CONTROL	**PESO DE LA EJECUCIÓN DE CADA CONTROL**	**SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE: 100 MODERADO: 50 DÉBIL: 0**	**DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SÍ / NO**
	Fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCIÓN DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE: 100 MODERADO: 50 DÉBIL: 0	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SÍ / NO
Fuerte: Calificación entre 90 y 100	**Moderado** (algunas veces)	fuerte + moderado = moderado	Sí
	Débil (no se ejecuta)	fuerte + débil = débil	Sí
Moderado: Calificación entre 80 y 89	**Fuerte** (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	Moderado (algunas veces)	moderado + moderado = moderado	Sí
	Débil (no se ejecuta)	moderado + débil = débil	Sí
Débil: Calificación entre 0 y 79	**Fuerte** (siempre se ejecuta)	débil + fuerte = débil	Sí
	Moderado (algunas veces)	débil + moderado = débil	Sí
	Débil (no se ejecuta)	débil + débil = débil	Sí

Solidez del conjunto de controles preventivos:

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

RIESGOS	CONTROLES	DISEÑO DEL CONTROL	EJECUCIÓN DEL CONTROL	SOLIDEZ INDIVIDUAL DEL CONTROL	SOLIDEZ DEL CONJUNTO DE CONTROLES PREVENTIVOS
Riesgo	Control 1	Fuerte	Fuerte	Fuerte (100)	(100+50+0)/3 **50**
	Control 2	Fuerte	Moderado	Moderado (50)	
	Control 3	Débil	Fuerte	Débil (0)	

Solidez del conjunto de controles detectivos:

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

RIESGOS	CONTROLES	DISEÑO DEL CONTROL	EJECUCIÓN DEL CONTROL	SOLIDEZ INDIVIDUAL DEL CONTROL	SOLIDEZ DEL CONJUNTO DE CONTROLES DETECTIVOS
Riesgo	Control 1	Fuerte	Fuerte	Fuerte (100)	(100+50)/2

RIESGOS	CONTROLES	DISEÑO DEL CONTROL	EJECUCIÓN DEL CONTROL	SOLIDEZ INDIVIDUAL DEL CONTROL	SOLIDEZ DEL CONJUNTO DE CONTROLES DETECTIVOS
	Control 2	Fuerte	Moderado	Moderado (50)	**75**

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES PREVENTIVOS/DETECTIVOS	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 90 y 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 89.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realiza de acuerdo con la siguiente tabla:

Calificación de los controles Preventivos	Puntaje a disminuir en probabilidad
Fuerte	2
Moderado	1
Débil	0

Nota 17: *Para los riesgos de corrupción únicamente hay disminución de probabilidad, para el impacto* ***no opera el desplazamiento****.*

7.4.2 Seleccionar Opciones de Manejo

Tipo de Riesgo	Zona de Riesgo	Opciones de Manejo
Riesgos de gestión **(Incluye los Riesgos Fiscales y los Riesgos de Seguridad de la Información)**	Baja	**Nivel de aceptación:** **ASUMIR.** Se asume el riesgo y se administra por medio de las actividades propias del proceso asociado, no se adopta ninguna medida de control que afecte la probabilidad o impacto del riesgo. **Monitoreo:** • Realizar un monitoreo **TRIMESTRAL** frente al desempeño y reportar los

Tipo de Riesgo	Zona de Riesgo	Opciones de Manejo
		avances a la Oficina Asesora de Planeación.
	Moderada	**Nivel de aceptación:** **REDUCIR.** Se deben establecer acciones que permitan reducir la probabilidad de ocurrencia y/o el impacto del riesgo. **Monitoreo:** • Realizar un monitoreo **TRIMESTRAL** frente al desempeño y reportar los avances a la Oficina Asesora de Planeación.
	Alta y Extrema	**Nivel de aceptación:** **REDUCIR.** Se deben establecer acciones que permitan reducir la probabilidad de ocurrencia y/o el impacto del riesgo, **ó** **COMPARTIR O TRANSFERIR.** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. **Monitoreo:** • Realizar un monitoreo **TRIMESTRAL** frente al desempeño y reportar los avances a la Oficina Asesora de Planeación.
Riesgos de corrupción	Baja	En el caso de los riesgos de corrupción, ninguno debe quedar en la zona baja,
	Moderada	**Nivel de aceptación:** **REDUCIR.** Se deben establecer acciones que permitan reducir la probabilidad de ocurrencia y/o el impacto del riesgo. **Monitoreo:** • Realizar un monitoreo **TRIMESTRAL** frente al desempeño y reportar los avances a la Oficina Asesora de Planeación.
	Alta y Extrema	**Nivel de aceptación:** **REDUCIR.** Se deben establecer acciones que permitan reducir la probabilidad de ocurrencia y/o el impacto del riesgo,

Tipo de Riesgo	Zona de Riesgo	Opciones de Manejo
		ó **COMPARTIR.** Se reduce la probabilidad o el impacto del riesgo compartiendo una parte de este. **Monitoreo:** • Realizar un monitoreo **TRIMESTRAL** frente al desempeño y reportar los avances a la Oficina Asesora de Planeación.

7.5 ETAPA 5: FORMULAR PLAN DE TRATAMIENTO DEL RIESGO

Esta etapa es desarrollada por el equipo de trabajo del proceso (líder y responsable de las actividades), acompañado por el equipo de administración de riesgos de la OAP y consiste en formular el plan de tratamiento del riesgo residual, el cual comprende: formular actividades, responsable, fecha de inicio y terminación.

Para el caso de los planes de tratamiento de los riesgos de seguridad de la información, estos deben ser consolidados y publicados por la OTI en la página web institucional, según la legislación vigente.

7.5.1 Formular actividades

Son aquellas acciones que adelantará el líder del proceso para el fortalecimiento o mejora de los controles existentes, la eliminación de las posibles causas generadoras del riesgo e identificar nuevos mecanismos de prevención, detección o corrección. Así mismo, pueden estar orientadas a reducir o evitar las causas que podrían generar el riesgo o mitigar las consecuencias de una posible materialización.
Tener presente que para definir las actividades se debe:

- Buscar que las actividades definidas estén orientadas a atacar, en lo posible, las causas señaladas en la identificación del riesgo, a fin de disminuir la probabilidad de su ocurrencia o a contrarrestar las consecuencias potenciales a fin de mitigar los impactos de la materialización del riesgo.
- Evaluar las soluciones potenciales y tener en cuenta las actividades que pueden afectar a otros procesos en el cumplimiento de objetivos, las restricciones de presupuesto, tiempo, capacidades de equipo, etc.
- Validar las actividades previstas en los planes de acción y planes de mejoramiento, con el fin de no duplicar acciones.

7.5.2 Establecer responsables y fechas de ejecución de las actividades

En cada una de las actividades se debe definir el responsable de su ejecución, así como las fechas de inicio y de finalización que deben estar comprendidas dentro de la vigencia.

7.5.3 Establecer mecanismo de detección de materialización

Como medida para detectar la posible materialización de los riesgos o como indicador del funcionamiento de los controles, se establece un mecanismo que permita obtener esta información. Para ello, se selecciona alguna de estas opciones:

- Herramienta de seguimiento: hace referencia a aplicativos, cronogramas, planes de trabajo, informes, herramientas de monitoreo, entre otros, con los cuales es posible detectar la ocurrencia de riesgos.
- Indicador: medida cuantitativa que permite verificar el cumplimiento o avance de un objetivo, su seguimiento o medición periódica permite identificar la existencia de un riesgo
- Producto No Conforme: Es el resultado de un proceso que no cumple con los requisitos establecidos, por tanto, está relacionado con la materialización de riesgos, de acuerdo con lo establecido en el documento CI02-P03 Procedimiento de Producto no Conforme. Esta opción solo aplica para los mapas de riesgos de los procesos misionales y de atención al ciudadano.
- Plan de acción del área líder del proceso: Instrumento mediante el cual se programan en concordancia con el Plan estratégico institucional, las metas de los productos estratégicos y las actividades que se deben desarrollar anualmente para darle cumplimiento a los objetivos e indicadores estratégicos de la entidad. El seguimiento a este instrumento permite identificar la materialización de riesgos, en la medida en que allí se relacionan productos y servicios generados en los procesos que adelantan las áreas de la entidad.
- Auditorías: Hace referencia al resultado de las auditorias (interna o externas) en donde se genera informes de auditoría en los cuales se pueden evidenciar la materialización de riesgos.

7.5.4 Modificar el plan de tratamiento del riesgo, en caso de ser necesario

El líder del proceso, directamente o a través de quien designe, podrá solicitar modificación de las actividades, en aquellas eventualidades en las que de manera anticipada a la fecha de vencimiento de la actividad se observe:

- Que el tiempo para la ejecución de la acción no sea suficiente

- Que las actividades planteadas presentan dificultad para su realización

Las modificaciones de las actividades se solicitan a la OAP a través del módulo de riesgos del SIGI, indicando la justificación.

Cuando la solicitud a realizar sea de un plan de tratamiento de riesgos de seguridad de la información, el canal será la OAP, quien se encargará de elevar la solicitud a la OTI.

Hasta tanto la OAP o la OTI no den la aprobación de la modificación, se entenderá que el Plan de Tratamiento inicial está vigente y activo.

Los tipos de modificaciones que se podrán solicitar:

a) Reprogramación

Consiste en solicitar el cambio en las fechas de inicio y/o finalización de la actividad. El servidor público o contratista asignado de la OAP o de la OTI aprobará o no el ajuste en el módulo de riesgos del SIGI, de acuerdo con la solicitud.

b) Reformulación

Consiste en reemplazar una actividad o todo un plan de tratamiento formulado, por una nueva actividad o un nuevo plan de tratamiento.

c) Eliminación de una o varias actividades de un plan:

La eliminación de una o varias actividades de un plan de tratamiento, se realiza en el evento en el cual no es posible llevar a cabo lo planteado por factores que están fuera del alcance del área y que impiden su realización.

Nota 18: *Todas las solicitudes de modificación de planes de tratamiento serán objeto de revisión por parte de la OAP o de la OTI, en el caso de los riesgos de seguridad de la información. La OAP y la OTI darán viabilidad o no a las solicitudes realizadas con base en el análisis de la justificación presentada.*

7.6 ETAPA 7: APROBAR Y PUBLICAR EL MAPA DE RIESGOS EN EL APLICATIVO SIGI

7.6.1 Enviar mapa de riesgos a revisión metodológica

Una vez el líder del proceso haya diligenciado o actualizado el mapa de riesgos en el módulo de riesgos del SIGI, se debe remitir para revisión metodológica de los

riesgos identificados o actualizados a la OAP o a la OTI, en el caso de los riesgos de seguridad de la información.

7.6.2 Revisar Metodológicamente el mapa de riesgos

Una vez recibida la solicitud del líder de proceso, el responsable del módulo de riesgos revisa metodológicamente el mapa de riesgos, en el caso de los riesgos de seguridad de la información serán revisados con el servidor público o contratista que designe el Jefe de la Oficina de Tecnología e Informática.

El servidor público o contratista de la OAP o de la OTI revisa la propuesta del mapa de riesgos, en caso de requerir ajustes rechaza y remite los comentarios correspondientes a través del módulo de riesgos del SIGI.

Para el caso del mapa de riesgos de corrupción, una vez validado metodológicamente por la Oficina Asesora de Planeación, se genera una nueva versión y se publica como anexo del componente 1 del Plan Anticorrupción y Atención al Ciudadano en la página web de la entidad.

7.7 ETAPA 7: REALIZAR MONITOREO, EVALUACION Y SEGUIMIENTO

7.7.1 Realizar Monitoreo

El monitoreo de los riesgos lo realiza el líder del proceso a través de la revisión permanente de la implementación de los controles determinados en el mapa de riesgo, la ejecución de las actividades formuladas dentro del plan de tratamiento del riesgo, así como de la identificación de los riesgos materializados.

El líder del proceso debe reportar el resultado del monitoreo en el módulo de riesgos del SIGI, con la periodicidad definida en el numeral 7 de la Política de Riesgos de la Entidad (Anexo 1) de acuerdo con la zona residual del riesgo, o con una periodicidad menor si el líder del proceso lo considera necesario. El reporte debe contener como mínimo:

- Nombre del proceso
- Cantidad de riesgos identificados
- Número de riesgos materializados durante el periodo
- Indicar el avance del tratamiento realizado, si se materializó el riesgo.
- Análisis del Líder del proceso respecto al funcionamiento de los controles implementados (eficacia y efectividad) y su incidencia frente a la materialización o no de los riesgos, indicando evidencia de la aplicación de estos controles.

- Porcentaje de cumplimiento de avance de las actividades propuestas en el plan de tratamiento del riesgo, en caso de no presentar avance se debe justificar las razones, si la actividad se venció.

Nota 19: La Oficina Asesora de Planeación presenta los resultados y estadísticas a partir de la consolidación del monitoreo de riesgos al igual que el listado de riesgos materializados, al Comité Institucional de Coordinación de Control Interno o al Comité Institucional de Gestión y Desempeño.

Gracias a la articulación de la gestión de riesgo con otras actividades de seguimiento y control en la Entidad, cuando se materializa un riesgo se generan alarmas en auditorias de gestión, seguridad y salud y trabajo, producto no conforme, entre otras. En el caso particular de producto no conforme la relación con es directa para los procesos misionales.

Por esta razón se ha identificado para todos los productos y/o servicios de la SIC el formato CI02-F09, en el cual están definidos las variables y atributos que deben cumplir los productos y servicios generados por la entidad para cada proceso.

Esta ficha establece, además, el mecanismo de tratamiento para los productos y/o servicios no conformes una vez sean identificados. Si durante el monitoreo se evidencia que la materialización de un riesgo genera un producto no conforme, el líder del proceso debe remitirse al proceso CI02-P03 Producto No Conforme para adelantar el tratamiento previsto, solo en el caso de los procesos misionales.

En el caso de los riesgos de seguridad de la información se debe tener en cuenta:

- El líder de proceso debe reportar a la mesa de servicios el incidente de seguridad de la información donde este comprometida la disponibilidad, confidencialidad e integridad de la información de la entidad, siguiendo el Procedimiento de Incidentes de Seguridad de la Información SC05-P01.
- El líder del proceso y el Coordinador del Grupo de Informática Forense y Seguridad Digital o quien delegue deben analizar y revisar si se presenta o no la materialización del riesgo y realizar el reporte y seguimiento, en caso de ser necesario.
- En el caso de que se presente la materialización del riesgo se procede a reportar al mapa de riesgos correspondiente, de acuerdo con los lineamientos establecidos en la Política de Administración de Riesgos SC01-POL01.

7.7.2 Elaborar plan de mejoramiento en caso de materialización de un riesgo

Una vez se haya materializado un riesgo, el líder de proceso, debe:

- Analizar las causas que dieron lugar a la materialización del riesgo para determinar si se requiere o no un plan de mejoramiento con las acciones correctivas y preventivas necesarias, teniendo en cuenta las actividades descritas del documento CI01-I04 – Instructivo Planes de Mejoramiento.
- Analizar y actualizar el mapa de riesgos correspondiente, iniciando desde la etapa 2 de este documento.

Nota 20: La OAP brindará el acompañamiento metodológico en la formulación del Plan de Mejoramiento, en caso de ser un riesgo de seguridad de la información, lo hará la OTI.

7.7.3 Realizar evaluación y seguimiento

La Oficina de Control Interno dentro de su programa anual de auditorías, enfoca la metodología en el análisis y gestión de riesgos, realizando entre otras, las siguientes actividades:

a) Evalúa de manera independiente la administración de riesgos (elaboración y seguimiento del mapa por parte del líder del proceso).
b) Evalúa que los controles incorporados en el mapa de riesgos existen, funcionan según la periodicidad establecida y son efectivos.
c) Realiza seguimiento a la ejecución de las acciones establecidas en el plan de tratamiento del riesgo, verificando las evidencias del monitoreo realizado, entre otros.
d) Verifica si ha existido la materialización de riesgos.
e) En caso de ser necesario, recomienda mejoras a la Política de Administración de Riesgos.
f) Emite informes de ley e informes de las Auditorías Internas al Representante Legal/responsable del Sistema de Control Interno Institucional y al líder del proceso.

7.8 ETAPA 8: REALIZAR DIVULGACIÓN, COMUNICACIÓN, CONSULTA Y CONTROL DE LOS MAPAS DE RIESGOS

7.8.1 Consultar mapa de riesgos

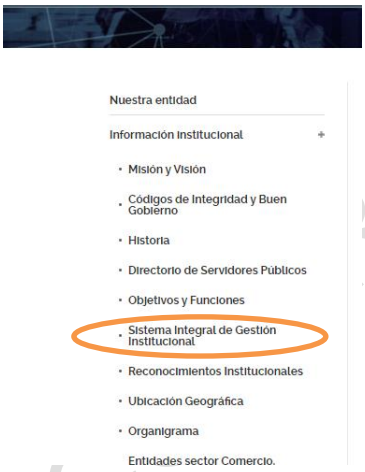
En la Superintendencia de Industria y Comercio cualquier usuario interno o externo puede consultar los Mapas de Riesgo por Proceso, tanto de gestión como de corrupción. Al ser de conocimiento público los usuarios pueden realizar sus observaciones en cualquier momento, a los correos oplaneacion@sic.gov.co o contactenos@sic.gov.co.

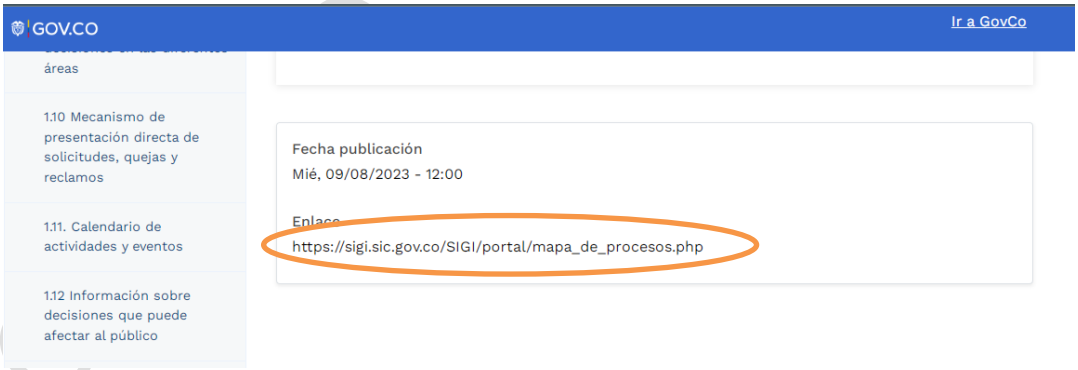
La visualización se puede realizar de la siguiente manera:

Ingrese a la Intrasic y de clic en el Sistema Integral de Gestión Institucional:

O desde la página web/ Nuestra Entidad/ Información institucional / Sistema Integrado de Gestión Institucional.

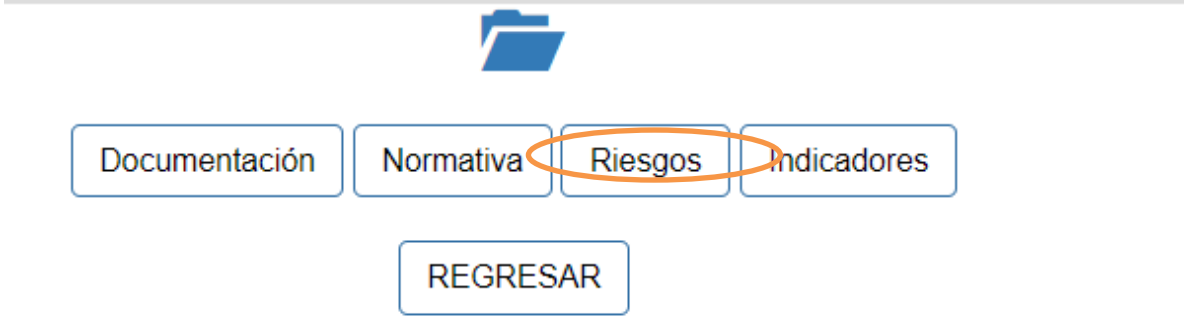
https://sigi.sic.gov.co/SIGI/portal/index.php?idcategoria=4&cat_origen=193&archivo_origen=index.php&





De inmediato tendrá acceso a la página principal del Sistema Integral de Gestión Institucional – SIGI, en donde se selecciona el proceso del cual se quiere consultar la información de los riesgos.
https://sigi.sic.gov.co/SIGI/portal/index.php?idcategoria=4&cat_origen=193&archivo_origen=index.php&

Al seleccionar un proceso, encontrara en la parte inferior el siguiente menú:



Anualmente la OAP consolida los riesgos de corrupción, este mapa es puesto a disposición de la ciudadanía y partes interesadas, para sus observaciones y comentarios, que serán tenidos en cuenta en la versión final del componente I. Mapa de riesgos de corrupción, del plan anticorrupción y atención al ciudadano de la SIC.

7.8.2 Controlar y registrar la administración del riesgo

Para garantizar la trazabilidad, la Superintendencia de Industria y Comercio mantendrá los registros asociados a los siguientes temas: monitoreo, evaluación y seguimiento, asesorías, sensibilización y divulgación.

8 DOCUMENTOS RELACIONADOS

Anexo 1. Política de Administración del Riesgo
Anexo 2. Controles 27001
CI02-P03 Producto No Conforme
DE01-P01 Formulación de la Planeación Institucional

SC01-P01 Documentación y Actualización del Sistema Integral de Gestión Institucional – SIGI
SC05-I02 Metodología para la identificación, clasificación y valoración de activos de información
SC01-F09 Caracterización de Procesos
SC05-F03 Registro de activos de información
SC05-P01 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

8.1 DOCUMENTOS EXTERNOS

Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013
Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP), 2022.

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Se realizó revisión y actualización de la metodología para la administración del riesgo, incluyendo lineamientos para la identificación de los riesgos fiscales. teniendo en cuenta las directrices establecidas en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, 2022 del Departamento Administrativo de la Función Pública. Asimismo, se actualizó el numeral 7.7.1, incluyendo las actividades para la gestión de riesgos en materia de seguridad de la información.

Fin documento