CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Laura Forero Torres Cargo: Profesional Universitario OAP Nombre: Jhon Jairo Arias Cargo: Profesional Universitario OAP Nombre: Leidy Katterine Pauna Diaz Cargo: Profesional Universitario Secretaría General Nombre: Mauricio Ortiz Coronado Cargo: Cargo: Profesional Universitario Secretaría General	Nombre: Angélica María Acuña Porras Cargo: Secretaria General Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Jefe Oficina Asesora de Planeación Nombre: Francisco Rodríguez Eraso Cargo: Jefe Oficina de Tecnología e Informática	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2021-12-23

1 OBJETIVO

Establecer la metodología para la identificación, análisis, valoración, definición de acciones de prevención, 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 administración de riesgos de la Superintendencia de Industria y Comercio-SIC, aplica para todos los procesos y actividades que se ejecuten en desarrollo de estos, y debe ser aplicada y apropiada por los servidores públicos y/o contratistas.

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.

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[1].

[1] DAFP. Guía para la administración de riesgos y diseño de controles

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).

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[2].

CONFIDENCIALIDAD: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados[3].

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.

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.

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.

[2] Ibid. Pág 8.
[3] Ibid. Pág 8.

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.[4]

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.

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. [5]

- 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

[4] Ibid. Pág 36.
[5] Manual Operativo Modelo Integrado de Planeación y Gestión - MIPG

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 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.

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

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 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 RESIDUAL: nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.

RIESGO INHERENTE: es el riesgo al que se enfrenta una entidad en ausencia de acciones que mitiguen su probabilidad de ocurrencia o el posible impacto de su materialización.

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.

4 REFERENCIAS

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
Ley	734 de 2002	Por la cual se expide el Código Disciplinario Único	Artículo 40	Artículo 40
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	Artículo 11 y Artículo 12	Artículo 11 y Artículo 12

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
		Contencioso Administrativo		
Ley	1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	Aplicación total	Aplicación total
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 establecido en el artículo 133 de la Ley 1753 de 2015	Aplicación total	Aplicación total
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	Capítulo 5	Capítulo 5

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
		Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"		

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 debe 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 Riesgo de gestión** (incluye riesgos de seguridad de la información, conflicto de interés y de protección de datos) y **corrupción** por cada uno de los procesos.

Contiene los riesgos a los cuales está expuesto un proceso, 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.

- **Mapa de Riesgo de Corrupción:**

Contiene el consolidado de los riesgos de la categoría "corrupción" a los cuales están expuestos los procesos de la Entidad. Para la identificación y tratamiento de los Riesgos de Corrupción para la SIC, se atiende la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP.[6]

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 actualizados cada dos años, 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.

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

[6] Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, 2018. Departamento Administrativo de la Función Pública.

permitan fortalecer los controles, eliminar las posibles causas generadoras de riesgos y continuar con el enfoque preventivo que permita la mitigación de los riesgos identificados.

5.3 ROLES Y RESPONSABILIDADES

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDADES FRENTE AL RIESGO
Estratégica	Alta Dirección, el Comité De Dirección, el Comité Institucional de Gestión y Desempeño y el 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. • 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. • Realizar seguimiento y análisis periódico a los riesgos institucionales. • Retroalimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión 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.
Primera Línea	Líderes de procesos y proyectos, y de sus equipos de trabajo (en general servidores públicos y contratistas de todos los niveles de la Entidad).	• 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 para mitigar la probabilidad e impacto de la materialización de los riesgos identificados, alineados con las metas y objetivos de la Entidad y proponer mejoras a la gestión 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 preventivas, correctivas y de mejora a que haya lugar. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDADES FRENTE AL RIESGO
		• Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los procesos a su cargo e informar el avance del plan de contingencia. • 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.
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.
	Oficina Asesora de Planeación Secretaría General (en lo referente a los riesgos de protección de datos personales y conflicto de interés) 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. • Recomendar a las áreas los ajustes a que haya lugar, con base en el monitoreo suministrado por los líderes de procesos. • 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

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDADES FRENTE AL RIESGO
		efectividad de los controles y el plan de tratamiento, la identificación e implementación, cuando aplique, de planes de contingencia, 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.

Nota 1: 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 2: La Secretaría General a través del rol del Oficial de Protección de Datos Personales, acompañará y asesorará todas las etapas de este procedimiento, cuando se trate de un riesgo de protección de datos personales.

Nota 3: La Mesa de Trabajo para la Gestión de Conflictos de Interés, integrado por representantes de la Oficina Asesora Jurídica, la Oficina Asesora de Planeación, la Oficina de Control Interno, Secretaría General, el Grupo de Administración de Personal y Grupo de Contratación, acompañará todas las etapas de este procedimiento, cuando se trate de un riesgo relacionado con conflictos de interés. 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[7]

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.

[7] 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.

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 en 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.

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 - Analizar Consecuencias Potenciales	Líder de proceso Servidores Públicos y/o contratistas que realizan actividades del proceso	Riesgos Identificados: Módulo de riesgos SIGI
2	**ANALIZAR Y CALIFICAR EL RIESGO ANTES DE**	Riesgos Identificados:	Esta etapa consiste en analizar el riesgo inherente sin	Líder de proceso	Análisis del riesgo antes de controles:

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
	CONTROLES (RIESGO INHERENTE)	Módulo de riesgos SIGI	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 - Seleccionar Opciones de Manejo	Servidores Públicos y/o contratistas que realizan actividades del proceso	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	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	**ELABORAR PLAN DE CONTINGENCIA EN CASO DE MATERIALIZACIÓN DE RIESGOS**	Análisis y calificación del riesgo después de controles: Módulo de riesgos SIGI CI02-F08 - Identificación y Tratamiento Producto No Conformen por proceso	Consiste en formular el plan de tratamiento en caso de materialización del riesgo. El plan se formula a través de la ejecución de las siguientes actividades: - Formular Actividades - Establecer responsables de ejecución de las actividades	Líder de proceso Servidores Públicos y/o contratistas que realizan actividades del proceso	Plan de tratamiento en caso de materialización del riesgo formulado: Módulo de riesgos SIGI
7	**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
8	**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	-Líder de proceso - 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

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
			- Elaborar plan de mejoramiento en caso de materialización de un riesgo - Realizar evaluación y seguimiento		- Módulo de riesgos y módulo de mejora del SIGI
9	**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: - Consultar mapa de riesgos - Controlar y registrar la Administración del Riesgo	Servidores y Públicos y Contratistas de la SIC	Consulta y control del Mapa de Riesgos en el aplicativo SIGI – Modulo de Riesgos

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 cual se deriva de la ejecución de la etapa 1 del proceso de Formulación de la Planeación Institucional DE01-P01. El objetivo del proceso debe responder a el “qué”, “cómo”, “para qué”, “cuándo”, “cuánto” 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
- Activos de seguridad de la información 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”.

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 o detectivos 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.

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.

Nota 5: *Es necesario que el mapa de riesgos de cada proceso contemple dentro de sus riesgos al menos uno de la categoría de corrupción, un riesgo de la categoría protección de datos personales, uno de conflicto de interés y uno de seguridad de la información. Si en caso excepcional el proceso no contempla alguno de estos riesgos, no se identifica esa situación no deseada.*

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:

- *¿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?*

Nota 6: *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, corrupción, conflicto de interés, protección de datos personales o seguridad de la información), se debe estructurar 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[8].
Indebida Protección de datos personales	Se materializa al no atender los principios para el tratamiento de datos personales, así como los derechos y condiciones de legalidad para el tratamiento de datos establecidos en la Ley 1581 de 2012.
Uso indebido de activos físicos	Se materializa con el daño, pérdida, alteración, abandono, manipulación, uso inapropiado de los recursos físicos de la Entidad.
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.
Interrupción	Se materializa al verse interrumpida totalmente una actividad misional, incluyendo la prestación de trámites o servicios prestados por la Entidad.

[8] Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, 2018. Departamento Administrativo de la Función Pública.

CATEGORIZACIÓN		
SITUACIÓN NO DESEADA		**DESCRIPCIÓN**
Seguridad de la Información	**Pérdida de confidencialidad**	Se materializa cuando la información es revelada a personas no autorizadas.
	Pérdida de disponibilidad	Se materializa cuando la información no está accesible y utilizable por el personal autorizado.
	Pérdida de integridad	Se materializa cuando la información es alterada o se pierde su exactitud y estado completo.

Nota 7: *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 8: *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 cualquier otra categoría.*

En el caso de la identificación de los 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 descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
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

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.
- 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.

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.

Para el caso de los riesgos de corrupción, a continuación, se detallan posibles eventos a utilizar:

Posibles eventos de corrupción			
No.	**Conducta**	**Descripción**	**Valor afectado**
1	Peculado por apropiación	Apropiación en provecho suyo o de un tercero de bienes del Estado o de bienes de particulares cuya administración, tenencia o custodia se le haya confiado por razón o con ocasión de sus funciones.	Honestidad
2	Peculado por uso	Usar o permitir que otro use bienes del Estado o bienes de particulares cuya administración, tenencia o custodia se le haya confiado por razón o con ocasión de sus funciones.	Honestidad Justicia

Posibles eventos de corrupción			
No.	**Conducta**	**Descripción**	**Valor afectado**
3	Peculado por aplicación oficial diferente	Dar a los bienes del Estado, cuya administración, tenencia o custodia se le haya confiado por razón o con ocasión de sus funciones, aplicación oficial diferente de aquella a que están destinados, o comprometa sumas superiores a las fijadas en el presupuesto, o las invierta o utilice en forma no prevista en éste, en perjuicio de la inversión social o de los salarios o prestaciones sociales de los servidores.	Honestidad Diligencia Justicia
4	Peculado culposo	Extravío, pérdida o daño de bienes del Estado, o bienes de particulares cuya administración, tenencia o custodia se le haya confiado por razón o con ocasión de sus funciones, de manera culposa.	Diligencia
5	Abuso de autoridad por omisión de denuncia	No dar cuenta a la autoridad del conocimiento de la comisión de una conducta punible cuya averiguación deba adelantarse de oficio.	Honestidad Diligencia
6	Revelación de secreto o uutilización de asunto sometido a secreto o reserva.	Indebidamente dar a conocer documento o noticia que deba mantener en secreto o reserva. Utilizar en provecho propio o ajeno, descubrimiento científico, u otra información o dato llegados a su conocimiento por razón de sus funciones y que deban permanecer en secreto o reserva.	Honestidad Compromiso Justicia
7	Concusión	Constreñir o inducir a alguien a dar o prometer al mismo servidor o a un tercero, dinero o cualquier otra utilidad indebidos, o los solicite,	Honestidad Justicia
8	Cohecho propio o impropio	Recibir para sí o para otro, dinero u otra utilidad, o aceptar promesa remuneratoria, directa o indirectamente, para retardar u omitir un acto propio de su cargo, o para ejecutar uno contrario a sus deberes oficiales.	Honestidad Justicia
9	Violación del régimen legal o constitucional de inhabilidades e incompatibilidades	Intervención en la tramitación, aprobación o celebración de un contrato con violación al régimen legal o a lo dispuesto en normas constitucionales, sobre inhabilidades o incompatibilidades	Honestidad
10	Interés indebido en la celebración de contratos	Interés en provecho propio o de un tercero, en cualquier clase de contrato u operación en que deba intervenir por razón de su cargo o de sus funciones.	Honestidad Diligencia Justicia

Posibles eventos de corrupción			
No.	**Conducta**	**Descripción**	**Valor afectado**
11	Contrato sin cumplimiento de requisitos legales	Tramitar contrato sin observancia de los requisitos legales esenciales o lo celebre o liquide sin verificar el cumplimiento de los mismos.	Honestidad
12	Tráficos de influencias de servidor público	Utilizar indebidamente, en provecho propio o de un tercero, influencias derivadas del ejercicio del cargo o de la función, con el fin de obtener cualquier beneficio de parte de servidor público en asunto que éste se encuentre conociendo o haya de conocer.	Honestidad Diligencia Justicia
13	Prevaricato por acción u omisión	Proferir resolución, dictamen o concepto manifiestamente contrario a la ley u omitir, retardar, rehusar o denegar un acto propio de sus funciones.	Honestidad Justicia
14	Materialización del conflicto de interés	Proferir un juicio o tomar una decisión por parte del servidor y/o contratista de manera sesgada por el interés particular y, en consecuencia, se obtenga un beneficio directo o indirecto.	Honestidad Justicia

Otros 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)

Descripción de posibles eventos	
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

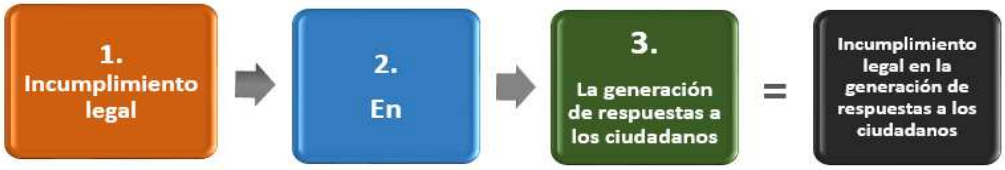
En el caso de los riesgos de seguridad de la información, a continuación, se detallan posibles eventos a utilizar:

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.
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.

Descripción de posibles eventos de seguridad de 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:



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.

Ejemplo:

PROCESO: Atención al Ciudadano		
Actividad Critica	**Riesgo**	**Descripción del Riesgo**
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	No se generan las respuestas dentro del término establecido en la normativa aplicable (ver procedimiento CS01-P01 Servicios de Atención al Ciudadano)

Ejemplo redacción riesgos de Seguridad de la Información:

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 detallar 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.**

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 [9].

- **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.

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

[9] Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, 2018. Departamento Administrativo de la Función Pública.

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	
Legal	Incumplimiento de la legislación sobre protección de datos personales
Legal	Incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento
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.

AMENAZAS DE DATOS PERSONALES	
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 diseminada en diversas secciones y apartados que hagan muy difícil su acceso conjunto y detallado

AMENAZAS DE DATOS PERSONALES	
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.

AMENAZAS DE DATOS PERSONALES	
DEBER DE SECRETO	
Legal /Organizacional /Técnico	Accesos no autorizados a 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

AMENAZAS DE DATOS PERSONALES	
	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
PROCEDIMIENTOS	
Técnico	Inexistencia de Procedimiento de copia de seguridad
Técnico	Errores en la ejecución de Copias de Seguridad y almacenamiento y gestión de soportes.
Técnico	Inexistencia de Procedimiento de acceso Lógico
Técnico	Inexistencia de Procedimiento de gestión de incidentes
Técnico	Reintentos fallidos en acceso lógico
Técnico / Organizacional	Inexistencia de Políticas de correo electrónico
Organizacional	Inexistencia de Procedimiento de custodia de documentos
Organizacional	Inexistencia de Procedimiento de entrada y salida de soportes y documentos
Organizacional	Inexistencia de Inexistencia de Procedimiento de archivo
Organizacional	Inexistencia de Procedimiento de áreas restringidas
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.
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.
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.
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.
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. - La no declaración oportuna de un conflicto de interés se puede constituir en una causa de corrupción por conflicto de intereses

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.
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	Recortes presupuestales
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
Baja rotación del personal que atiende público al interior de la entidad	Falta de coherencia en el actuar de las entidades del sector
Conocimientos limitados de los funcionarios que intervienen en la elaboración de documentos relacionados con la contratación	Cambios regulatorios y técnicos que generen confusiones en materia de competencias legales Impacto de las decisiones que toma la entidad
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	
Asimetrías de la información	
Desmotivación de funcionarios	
Alta rotación de personal	
Herramientas informáticas poco confiables y oportunas	

EJEMPLOS DE CAUSAS INTERNAS	EJEMPLOS DE CAUSAS EXTERNAS
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	
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:

CATEGORIZACIÓN DE SITUACIÓN NO DESEADA	EJEMPLOS DE VULNERABILIDADES
Perdida de confidencialidad	Almacenamiento de información sin protección Falta de conciencia en seguridad de la información. Compartir contraseñas. Ausencia de políticas de uso aceptable de información. Trabajo no supervisado de personal externo o de limpieza. Ausencia de protección en puertas de acceso a oficinas Ausencia de procedimiento de registro/retiro de usuarios. Ausencia de proceso para supervisión de derechos de acceso.
Perdida de integridad	Ausencia o insuficiencia de pruebas de software. Ausencia de terminación de sesión Ausencia de registros de auditoría Asignación errada de los derechos de acceso Ausencia de documentación. Ausencia de mecanismos de identificación y autenticación de usuarios Ausencia del personal especializado. Entrenamiento insuficiente. Falta de monitoreo sobre las actividades de los usuarios

Perdida de disponibilidad	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad) Mantenimiento insuficiente. Monitoreo insuficiente de la plataforma tecnológica. Ausencia de actualizaciones periódicas de la plataforma tecnológica. Retiro de expedientes físicos sin autorización.

Nota 10: Los ejemplos de 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	No se generan las respuestas dentro del término establecido en la normativa aplicable (ver procedimiento CS01-P01 Servicios de Atención al Ciudadano)	-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.	Correspondencia 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:

FACTORES EXTERNOS	FACTORES INTERNOS
Se relacionan con los aspectos social, cultural, económico, tecnológico, político y legal, bien sea internacional, nacional o regional.	Se relacionan con la estructura, cultura organizacional, el modelo de operación, el cumplimiento de los planes y programas, los sistemas de información, los procesos y procedimientos, los recursos humanos y económicos con los que cuenta la Entidad.
Económicos	Competencias
Imagen	Comunicación
Legal	Cultural
Medioambientales	Documentación
Políticos	Financiero
Sociales	Infraestructura
Tecnológicos	Jurídico
Estratégicos	Logístico
	Método
	Seguridad
	Sistemas de Información
	Tecnología

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
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 tramites 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 en un espacio de tiempo
- ✓ Número de personas que intervienen en la realización de la actividad
- ✓ Grado de tecnificación, automatización de la actividad

De acuerdo con el análisis, 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:

IMPACTO			
CALIFICA-CIÓN	**DESCRIPTOR**	**DESCRIPCIÓN**	**CONSECUENCIAS**
1	Insignificante	Si el hecho llega a presentarse, tendría consecuencias o efectos mínimos sobre la Entidad	-No hay interrupción de las operaciones de la Entidad. -No se generan sanciones económicas o administrativas. -No se afecta la imagen institucional de forma significativa
2	Menor	Si el hecho llega a presentarse, tendría bajo impacto o efecto sobre la Entidad	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. -Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
3	Moderado	Si el hecho llega a presentarse, tendría medianas consecuencias o efectos sobre la Entidad	- Interrupción de las operaciones de la Entidad por un día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la Entidad. -Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. -Reproceso de actividades y aumento de carga operativa. -Imagen institucional afectada por retrasos en la prestación del servicio a los usuarios o ciudadanos. -Investigaciones penales, fiscales o disciplinarias.
4	Mayor	Si el hecho llega a presentarse, tendría altas consecuencias o efectos sobre la Entidad	-Interrupción de las operaciones de la Entidad por más de dos días. -Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. -Sanción por parte de ente de control u otro ente regulador. -Incumplimiento de metas u objetivos institucionales afectando el cumplimiento en las metas de gobierno. -Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.
5	Catastrófico	Si el hecho llega a presentarse, tendría desastrosas	-Interrupción de las operaciones de la Entidad por más de cinco días. -Intervención por parte de un ente de control u otro ente regulador.

IMPACTO			
CALIFICA-CIÓN	**DESCRIPTOR**	**DESCRIPCIÓN**	**CONSECUENCIAS**
		consecuencias o efectos sobre la Entidad	-Pérdida de información crítica para la Entidad que no se puede ser recuperar. -Incumplimiento de metas u objetivos institucionales afectando de forma grave la ejecución presupuestal. -Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

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 11: *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, en el módulo de riesgos del SIGI, automáticamente el aplicativo 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:

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

B: Zona de riesgo Baja:
M: Zona de riesgo Moderada
A: Zona de riesgo Alta
E: Zona de riesgo Extrema

Matriz de Evaluación del riesgo inherente

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 a lo establecido en el numeral 7 de la Política de Administración de Riesgos (Ver Anexo 1), se debe realizar un monitoreo trimestral.

7.2.4 Seleccionar Opciones de Manejo

Tipo de Riesgo	Zona de Riesgo (Riesgo Inherente)	Opciones de Manejo
Riesgos de gestión	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 avances a la Oficina Asesora de Planeación.
	Moderada	**Nivel de aceptación:** **REDUCIR.** Se deben establecer acciones de control preventivas o detectivas, 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 de control preventivas o detectivas 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:**

Tipo de Riesgo	Zona de Riesgo (Riesgo Inherente)	Opciones de Manejo
		• 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 de control preventivas o detectivas, 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 de control preventivas o detectivas, que permitan reducir la probabilidad de ocurrencia y/o el impacto del riesgo, **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.

De acuerdo con la zona en la que se encuentre ubicado el riesgo inherente, se debe seleccionar una de las siguientes opciones de manejo:

- **Evitar el riesgo:** Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

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

- **Compartir o transferir el riesgo:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

- **Asumir el riesgo:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).

Nota 12: Cuando el riesgo residual se encuentre en zona moderada, alta o extrema, la opción de tratamiento será reducir. En el caso de los riesgos ubicados en zona baja, serán asumidos. En todos los casos se deberán plantear actividades en el plan de tratamiento del riesgo.

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 en el formato CI02-F08 Identificación y Tratamiento Producto no Conforme, en la columna “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 13: *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 14: *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.*

Nota 15: *Se considera como una buena práctica establecer un control para cada causa, no obstante, en la práctica esto no es necesariamente una regla, pues existen causas de origen externo a la Entidad para las cuales no es posible establecer controles. La OAP orientará que el establecimiento de controles este enfocado a eliminar las causas.*

Para diseñar los controles se deben tener en cuenta los siguientes pasos:

Paso 1: El control debe estar documentado

Para cada control identificado se debe tener en cuenta que este debe estar documentado.

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.) o detectar la materialización del riesgo, con el objetivo de llevar acabo los ajustes y correctivos en el diseño del control o en su ejecución.

De acuerdo con lo anterior el propósito del control está orientado a:

Prevenir[10]: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia (probabilidad) de los riesgos que puedan afectar el cumplimiento de los objetivos.

[10] DAFP. Guía para la administración de riesgos y diseño de controles. Página 74

Detectar[11]: Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido (impacto). Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

Nota 16: *El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas*, 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 se observan diferencias o aspectos que no se cumplen, la actividad no debe continuar hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, debe gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas.

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 se realiza respecto al análisis y evaluación del diseño del control de acuerdo con las siete (7) variables establecidas:

[11] Ibid.

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)

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: Calificación entre 90 y 100	**Fuerte** (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	Moderado (algunas veces)	fuerte + moderado = moderado	Sí
	Débil (no se ejecuta)	fuerte + débil = débil	Sí
Moderado: Calificación entre 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
	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.

7.4.1 Calificar el riesgo residual

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

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

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