CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Laura Forero Torres Cargo: Contratista OAP Nombre: German Beltran Constain Cargo: Contratista OTI Nombre: Jhon Jairo Arias Cargo: Contratista OAP	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: 29-05-2019

1 OBJETIVO

Establecer la metodología para la identificación, análisis, valoración, definición de acciones de prevención, mitigación y seguimiento a los riesgos relacionados con 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 los mismos, ésta 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, identificada en la caracterización del mismo en el HACER, en la que 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].
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.

[1] Guía para la administración del riesgo y diseño de controles. Departamento Administrativo de la Función Publica

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].

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.

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]

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.

[2] Ibid. Pág 8.
[3] Ibid. Pág 8.
[4] Ibid. Pág 36.

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.

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	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.
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

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 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 ésta metodología, se debe tener en cuenta lo declarado en la Política de Administración del Riesgo (Ver anexo 1).

La Superintendencia de Industria y Comercio administra sus riesgos a través del aplicativo SIGI módulo de riesgos y las matrices de identificación de riesgos y monitoreos en el formato SC01-F07 Mapa de Riesgos por Procesos.

Los riesgos son identificados a través de los siguientes elementos:

- **Mapa de Riesgo Institucional:**

Contiene la consolidación de los riesgos a los cuales están expuestos los procesos de la Entidad y los presenta de acuerdo al grado de exposición. En el aplicativo SIGI módulo de riesgos, se observa la matriz de evaluación, donde se puede distinguir que riesgos se encuentran en cada una de las zonas: baja, moderada, alta y extrema, según se califique el riesgo.

- **Mapa de Riesgo de Corrupción:**

Contiene la consolidación de los riesgos de la categoría corrupción a los cuales están expuestos los procesos de la Entidad, permitiendo conocer la aplicación de la Política de Administración del Riesgo asociada a los procesos a través de las opciones de tratamiento definidas. 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.[5]

- **Mapa de Riesgo de Gestión[6]**:

Contiene una síntesis de las etapas desarrolladas para la administración de riesgos, presentando los riesgos a los cuales está expuesto un proceso y la aplicación de la Política de Administración del Riesgo asociada a los procesos a través de las

[5] Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, 2018. Departamento Administrativo de la Función Pública.
[6] Los riesgos de gestión incluyen los riesgos de seguridad de la información y los riesgos de habeas data.

opciones de manejo definidas. Para el registro de este mapa se debe diligenciar el Formato SC01-F07 Mapa de Riesgos por proceso.

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, el cual 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 su 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 de la Entidad, 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.

Por su parte, los planes de tratamiento de riesgos deberán ser actualizados con la periodicidad que para el efecto defina la Oficina Asesora de Planeación, e identificarán las actividades a realizar durante la vigencia fiscal, responsables y mecanismos de detección de materialización.

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 Formato: Mapa de riesgos por proceso SC01-F07	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: Formato: Mapa de riesgos por proceso SC01-F07
2	**ANALIZAR Y CALIFICAR EL RIESGO ANTES DE CONTROLES**	Riesgos Identificados: Formato: Mapa de riesgos por proceso	Esta etapa consiste en analizar el riesgo inherente sin considerar los controles que	Líder de proceso Servidores Públicos y/o	Análisis del riesgo antes de controles: Formato:

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
	(RIESGO INHERENTE)	SC01-F07	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	contratistas que realizan actividades del proceso	Mapa de riesgos por proceso SC01-F07
3	**IDENTIFICAR, CLASIFICAR Y VALORAR LOS CONTROLES**	Análisis del riesgo antes de controles: Formato: Mapa de riesgos por proceso SC01-F07	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: Formato: Mapa de riesgos por proceso SC01-F07
4	**ANALIZAR Y CALIFICAR EL**	Identificación y valoración de	En esta etapa se determina el riesgo	Líder de proceso	Análisis y calificación

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
	RIESGO DESPUÉS DE CONTROLES (RIESGO RESIDUAL)	controles: Formato: Mapa de riesgos por proceso SC01-F07	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	Servidores Públicos y/o contratistas que realizan actividades del proceso	del riesgo después de controles: Formato: Mapa de riesgos por proceso SC01-F07
5	**FORMULAR PLAN DE TRATAMIENTO DEL RIESGO**	Análisis y calificación del riesgo después de controles: Formato: Mapa de riesgos por proceso SC01-F07	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	Líder de proceso Servidores Públicos y/o contratistas que realizan actividades del proceso	Plan de tratamiento del riesgo formulado: Formato: Mapa de riesgos por proceso SC01-F07

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
6	**ELABORAR PLAN DE CONTINGENCIA/ PROTOCOLO EN CASO DE MATERIALIZACIÓN DE RIESGOS**	Análisis y calificación del riesgo después de controles: Formato: Mapa de riesgos por proceso SC01-F07 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 - Elaborar plan de mejoramiento - Ejecutar el protocolo en caso de materialización de un riesgo de corrupción	Líder de proceso Servidores Públicos y/o contratistas que realizan actividades del proceso	Plan de tratamiento en caso de materialización del riesgo formulado: Formato: Mapa de riesgos por proceso SC01-F07
7	**APROBAR Y PUBLICAR EL MAPA DE RIESGOS EN EL APLICATIVO SIGI**	Formato: Mapa de riesgos por proceso SC01-F07 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 a 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	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	-Líder de proceso	- Informe registrado en el Aplicativo SIGI- módulo de riesgos - Evaluación

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
		formulado: Formato: Mapa de riesgos por proceso SC01-F07	de riesgos. Las actividades a realizar en esta etapa son: - Realizar monitoreo - Realizar evaluación y seguimiento - Formular Plan de mejoramiento (si aplica)	- Oficina de Control Interno	y seguimiento de los mapas de riesgo por proceso en aplicativo SIGI- módulo de riesgos - Correo electrónico con solicitud de plan de mejoramiento (si aplica)
9	**REALIZAR DIVULGACIÓN, 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 que involucra el proceso (líder y responsable de las actividades), acompañado por el equipo de administración de riesgos de la Oficina Asesora de Planeación - OAP.

Cada líder de proceso junto con los servidores públicos y/o contratistas que hacen parte del proceso, desarrollan 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 incluir 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

Con base en el contexto estratégico establecido para la entidad, derivado de la ejecución de la etapa 1 del proceso de Formulación de la Planeación Institucional DE01-P01, se debe establecer el contexto interno, externo del proceso y sus activos de seguridad de la información.

En esta actividad 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

El contexto estratégico del proceso se encuentra documentado en la caracterización de cada uno de los procesos, 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 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 la misma, 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 que se encuentre en forma impresa, escrita, papel, trasmitida por cualquier medio electrónico, almacenada en equipos de cómputo, software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes, entre otros.

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 aquellas a las cuales se les realizará el análisis de riesgos, actividades críticas. Estas actividades son identificadas como críticas porque requieren de especial atención debido a que su ejecución tiene un mayor impacto sobre el resultado final esperado del proceso. Es importante centrarse en los riesgos más significativos para la Entidad relacionados con los objetivos de los procesos y los objetivos institucionales.

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 del mismo.
- 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 1: *Las actividades críticas tienen directa relación con la generación del producto identificado en el procedimiento CI02-P03 Producto No Conforme, en el caso de ser un proceso misional.*

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 contiene 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 formato: mapa de riesgos por proceso-SC01-F07, en la primera columna titulada 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 2: *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 y uno de seguridad de la información*

Preguntas clave para la identificación del riesgo

Para orientar la identificación de los riesgos, a continuación se relacionan unas preguntas a tener en cuenta que facilitan 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 o administrativas cuando se materializa el riesgo?*
- *¿Podría propiciar quejas o reclamos de los usuarios o partes interesadas?*

Nota 3: *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, protección de datos personales o seguridad de la información), se debe estructurar de la siguiente manera en el formato Mapa de riesgos por proceso-SC01-F07:

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

a. Situación no deseada:

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[7].
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.

[7] 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**
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.
Conflicto de interés		Se materializa cuando existe una confrontación entre el deber público y los intereses privados de un servidor público y/o contratista, es decir, éste tiene intereses personales que podrían influenciar alguna decisión o afectar la imparcialidad.
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 4: *Excepcionalmente puede presentarse que una situación no deseada, no se encuentre categorizada en el listado anteriormente definido, 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.*

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.
- Conflicto de interés: cuando, durante, mediante, por.
- Inexactitud: al, con, de, durante, en, para, sobre.
- Corrupción: al, durante, por, en.
- Indebida Protección de datos personales: al, durante, por, en.
- Seguridad de la información: al, durante, por, en, sobre, ante, de

Nota 5: *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:

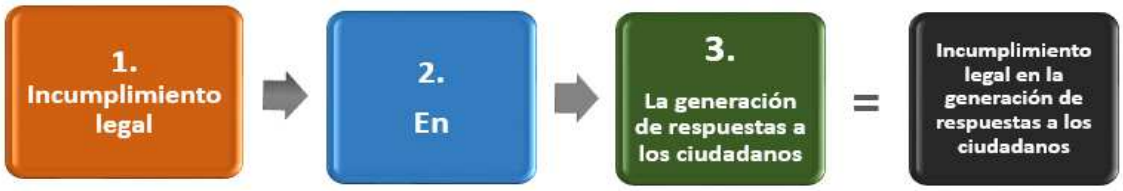
Descripción de posibles eventos	
Establecer adendas que cambian condiciones generales del proceso para favorecer a grupos determinados	Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica
Amiguismo y clientelismo	Archivos contables con vacíos de información
Cobrar por realización del trámite, (Concusión)	Concentración de autoridad o exceso poder
Concentración de información de determinadas actividades o procesos en una persona	Interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación
Decisiones ajustadas a intereses particulares	Inclusión de gastos no autorizados
Dilatación de los procesos con el propósito de obtener el vencimiento de términos o la prescripción del mismo	Restricción de la participación a través de visitas obligatorias innecesarias, establecidas en el pliego de condiciones
Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular	Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación (estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular)
Extralimitación de funciones	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	Sistemas de información susceptibles de manipulación o adulteración
Urgencia manifiesta inexistente	Soborno (Cohecho)
Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión	Tráfico de influencias, (persona influyente)

Para 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.
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, a continuación se presenta la estructura de un riesgo:

Ejemplo:



7.1.7 Describir Riesgo Identificado

Posterior a la estructuración del riesgo, se realiza la descripción del mismo, 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.	Todos los colaboradores del grupo de trabajo son administradores de la carpeta compartida que consolida la información que tramita el proceso.	Carpeta compartida en Drive.

Para el caso de los riesgos de corrupción, en la descripción se debe 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 los mismos 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 de la organización pública 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 de la entidad, de la articulación entre dependencias o de la falta de control o manejo erróneo de las bases de datos que contengan 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:** posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

- **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 [8].

- **Riesgos de seguridad de la información:** Posibilidad Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

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 las causas se conocen como vulnerabilidades. Para identificarlas se debe realizar un análisis de las amenazas que pueden generar la vulnerabilidad, a continuación se presenta un listado de posibles amenazas de seguridad de la información.

AMENAZAS DE SEGURIDAD DE LA INFORMACIÓN	
Abuso de los derechos	Fallo de servicios de información
Acceso no autorizado	Falta de disponibilidad del personal
Agua	Fuego
Atentado terrorista	Gestión ineficiente de la seguridad de la información
Ausencia de personal	Hackers
Ausencia del suministro de agua	Información de fuentes no confiables
Ausencia del suministro de energía	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

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

AMENAZAS DE SEGURIDAD DE LA INFORMACIÓN	
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	Revelación de contraseñas
Espionaje	Saturación de los sistemas de información
Estafadores	Software malicioso
Empleado descontento	Suplantación de identidad
Falla en el software	Terremoto
Fallo de equipos	

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.
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
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.
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.

CATEGORIZACIÓN DE SITUACIÓN NO DESEADA	EJEMPLOS DE CAUSAS
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.
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 confidencial 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.
Conflicto de interés	- Tener un interés particular y directo sobre la regulación, gestión, control o decisión. - Que no se presente declaración de impedimento para actuar en el mismo, por parte del empleado público.

Para el caso de 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	

EJEMPLOS DE CAUSAS INTERNAS	EJEMPLOS DE CAUSAS EXTERNAS
Herramientas informáticas poco confiables y oportunas	
Gran demanda de información personalizada por la ciudadanía	
Insuficiente capacidad instalada	
Infraestructura física no adecuada para la atención de usuarios	
Bajo nivel de automatización al seguimiento de los proceso	

Para el caso de riesgos de seguridad de la información, a continuación se presenta un listado con posibles causas:

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 la 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

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 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.	Todos los colaboradores del grupo de trabajo son administradores de la carpeta compartida que consolida la información que tramita el proceso, por lo cual puede alterarse el estado completo de la información.	Carpeta compartida en Drive.	Empleado descontento	Ausencia de revisión de derechos de acceso.
PROCESO: Gestión Documental					

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 corresponden cia de entrada, permitiendo que información clasificada y reservada pueda ser consultada.	Corresponde ncia diaria	Acceso no autorizad o	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.
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

CATEGORIZACIÓN DE SITUACIÓN NO DESEADA		EJEMPLOS DE CONSECUENCIAS POTENCIALES
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.
Conflicto de interés		- Pérdida de credibilidad y de confianza en la Entidad. - Investigaciones disciplinarias - Quejas y reclamos de los clientes (internos y/o externos)
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 que involucra el proceso (líder y responsable de las actividades), acompañado por el equipo de administración de riesgos de la OAP. Consiste en analizar el riesgo inherente al que se enfrenta la Entidad en ausencia de acciones para modificar su probabilidad o impacto, 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

Esta actividad consiste en establecer 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	-No hay interrupción de las operaciones de la Entidad. -No se generan sanciones económicas o administrativas.

IMPACTO			
CALIFICA-CIÓN	**DESCRIPTOR**	**DESCRIPCIÓN**	**CONSECUENCIAS**
		efectos mínimos sobre la Entidad	-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 consecuencias o efectos sobre la Entidad	-Interrupción de las operaciones de la Entidad por más de cinco días. -Intervención por parte de un ente de control u otro ente regulador. -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.

IMPACTO			
CALIFICA-CIÓN	**DESCRIPTOR**	**DESCRIPCIÓN**	**CONSECUENCIAS**
			-Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

Para los riesgos de Seguridad de la Información la calificación de probabilidad e impacto se determina con base a las amenazas, no en las vulnerabilidades.

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 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 a 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 6: *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 formato: mapa de riesgos por proceso - SC01-F07, automáticamente el archivo 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: ⇨ Asumir el riesgo, no continuar con el ejercicio e identifique otro riesgo

M: Zona de riesgo Moderada
A: Zona de riesgo Alta
E: Zona de riesgo Extrema
} **Continúe con la etapa 3**

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 lo anterior y de acuerdo a lo establecido en el numeral 6 de la Política de Administración de Riesgos (Ver Anexo 1), se debe realizar un monitoreo trimestral.

7.2.4 Seleccionar Opciones de Manejo

De acuerdo con la zona en la que se encuentre ubicado el riesgo inherente, se debe seleccionar una de las siguientes 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. **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 controles y acciones preventivas 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 controles y acciones preventivas que permitan reducir la probabilidad de ocurrencia y/o el impacto del riesgo, **ó** **COMPARTIR O TRANSFERIR.** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.

		Monitoreo: Realizar un monitoreo **TRIMESTRAL** frente al desempeño y reportar los avances a la Oficina Asesora de Planeación.

Tipo de Riesgo	Zona de Riesgo (Riesgo Inherente)	Opciones de Manejo
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 controles y acciones preventivas 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 controles y acciones preventivas 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. *Los riesgos de corrupción se pueden compartir pero no se puede transferir su responsabilidad. **Monitoreo:** Realizar un monitoreo **TRIMESTRAL** frente al desempeño y reportar los avances a la Oficina Asesora de Planeación.

- **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).

7.3 ETAPA 3: IDENTIFICAR, CLASIFICAR Y VALORAR LOS CONTROLES

Esta etapa es desarrollada por el equipo de trabajo que involucra el proceso (líder y responsables de las actividades), acompañado por el equipo de administración de riesgos de la OAP, y consiste en identificar, y valorar los controles que en la actualidad se aplican en el proceso y/o definir nuevos a fin 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 7: *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 la actividad, los documentos asociados, registros, entre otros.*

Nota 8: *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 9: *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 bien sea en algún procedimiento o instructivo.

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: 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.

Detectar: 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 10: *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.*

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:

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 procedimientos o instructivos 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
			Adecuado	10

NO.	CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
		¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	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
	Fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí

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
Moderado: Calificación entre 80 y 89	**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 **75**
	Control 2	Fuerte	Moderado	Moderado (50)	

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

IMPACTO: Desplaza a la izquierda

PROBABILIDAD: Desplaza hacia arriba

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: Asumir el riesgo
M: Zona de riesgo Moderada: Reducir el riesgo
A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir

Matriz de Evaluación del riesgo residual

7.5 ETAPA 5: FORMULAR PLAN DE TRATAMIENTO DEL RIESGO

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

7.5.1 Formular actividades

Son aquellas acciones que adelantará el líder del proceso para el fortalecimiento o mejora de los controles existentes o la implementación de nuevos controles. Así mismo, pueden estar orientadas a reducir o evitar las causas que podrían generar el riesgo o mitigar las consecuencias de una posible materialización.

Tener presente que para definir las actividades se debe:

- Asegurar que las actividades definidas estén orientadas a atacar, en lo posible, las causas señaladas en la identificación del riesgo, a fin de disminuir la probabilidad de su ocurrencia o a contrarrestar las consecuencias potenciales a fin de mitigar los impactos de la materialización del riesgo.
- Equilibrar los costos y los esfuerzos, así como los beneficios finales, contemplando aspectos jurídicos, técnicos, institucionales, financieros y el análisis costo- beneficio.
- Evaluar las soluciones potenciales y tener en cuenta las actividades que pueden afectar a otros procesos en el cumplimiento de objetivos, las restricciones de presupuesto, tiempo, capacidades de equipo, etc.
- Validar las actividades previstas en los planes de acción y planes de mejoramiento, con el fin de no duplicar acciones.

7.5.2 Establecer responsables y fechas de ejecución de las actividades

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

7.5.3 Establecer mecanismo de detección de materialización

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

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

7.6 ETAPA 6: ELABORAR PLAN DE CONTINGENCIA/PROTOCOLO EN CASO DE MATERIALIZACIÓN DE RIESGOS

Esta etapa es desarrollada por el equipo de trabajo que involucra el proceso (líder y responsable de las actividades), acompañado por el equipo de administración de riesgos de la OAP y consiste en formular un plan correctivo el cual ayuda a controlar una situación de materialización del riesgo y a minimizar los impactos negativos que este pueda ocasionar sobre el proceso, los servidores públicos y/o contratistas o la Entidad.

Para los procesos misionales verifique el formato CI02-F08 - Identificación y Tratamiento Producto No Conformen del proceso, el tratamiento identificado en caso de materialización de un PNC está relacionado con el riesgo.

Para el caso de los riesgos de corrupción se debe establecer un protocolo, de acuerdo con las premisas descritas en el numeral 7.6.4.

A continuación se describen los pasos requeridos para elaborar el plan de contingencia:

7.6.1 Formular actividades

Son aquellas acciones que adelantará el líder del proceso en caso de la materialización del riesgo, deben estar orientadas a corregir el hecho materializado.

7.6.2 Establecer responsables de ejecución de las actividades

Para el plan establecido se asigna un responsable de su ejecución, el cual es el líder del proceso.

7.6.3 Elaborar plan de mejoramiento

Esta actividad debe surtir el flujo del procedimiento CI02-P05 Procedimiento Acciones Correctivas y Preventivas, además una de las actividades del plan debe estar orientada a la revaloración del riesgo, iniciando desde la etapa 2 de este documento.

7.6.4 Ejecutar el protocolo en caso de materialización de un riesgo de corrupción

Cuando un riesgo de corrupción se materializa, el líder del proceso debe generar unas actividades (protocolo) orientado a preservar de manera intacta los medios en los que se presentó el hecho, por ejemplo, inhabilitar equipos de cómputo o equipos móviles, hasta tanto las autoridades correspondientes hagan presencia.

En todo caso y de acuerdo con las responsabilidades definidas en la Política de administración del riesgo (Ver Anexo 01), se debe:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente.

Adicionalmente, la Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva. Las acciones adelantadas deben orientarse a:

- Determinar la efectividad de los controles.

- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

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

7.7.1 Enviar mapa de riesgos a revisión metodológica

Una vez el líder del proceso haya diligenciado o actualizado el mapa de riesgos en el Formato SC01-F07, debe remitir al correo de la Oficina Asesora de Planeación (oplaneación@sic.gov.co) el formato diligenciado para revisión metodológica de los riesgos identificados o actualizados.

7.7.2 Revisar Metodológicamente el mapa de riesgos

Una vez recibida la solicitud del líder de proceso el Jefe de la Oficina Asesora de Planeación designa a un servidor público o contratista para que revise metodológicamente el mapa de riesgos.

El servidor público o contratista de la Oficina Asesora de Planeación revisa la propuesta del mapa de riesgos, en caso de requerir ajustes lo solicita al líder del proceso mediante correo electrónico.

Para el caso del mapa de riesgos de corrupción, una vez validado metodológicamente por la Oficina Asesora de Planeación, se genera una nueva versión y se publica en la página web de la entidad.

7.8 ETAPA 8: REALIZAR MONITOREO, EVALUACION Y SEGUIMIENTO

7.8.1 Realizar Monitoreo

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

El líder del proceso debe reportar el resultado del monitoreo al correo electrónico de la Oficina Asesora de Planeación (oplaneación@sic.gov.co), con una periodicidad definida en el numeral 6 de la Política de Riesgos de la Entidad (Anexo 1) de acuerdo con la zona inherente del riesgo, o con una periodicidad menor si el líder del proceso lo considera necesario. El reporte debe contener como mínimo:

- Nombre del proceso
- Cantidad de riesgos identificados
- Número de riesgos materializados durante el periodo
- Indicar el avance del tratamiento realizado, si se materializó el riesgo.
- Conclusiones relacionadas con la eficacia de las opciones de manejo aplicadas para tratar el riesgo
- Análisis del Líder del proceso respecto al funcionamiento de los controles implementados (eficacia y efectividad) y su incidencia frente a la materialización o no de los riesgos, indicando evidencia de la aplicación de estos controles.
- Porcentaje de cumplimiento de avance de las actividades propuestas en el plan de tratamiento del riesgo, en caso de no presentar avance se debe justificar las razones.

Materialización del riesgo y la generación de productos no conformes

La no conformidad que se presenta en un producto o servicio en la SIC, está directamente asociada con la materialización de los riesgos identificados para el proceso que genera el producto o servicio. Por esta razón se ha identificado para todos los productos y/o servicios de la SIC el formato CI02-F09, en el cual están definidos las variables y atributos que deben cumplir los productos y servicios generados por la entidad para cada proceso.

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

7.8.2 Realizar evaluación y seguimiento

La Oficina de Control Interno dentro de su rol de evaluación y seguimiento:

a) Realiza evaluación objetiva sobre la administración de los riesgos (elaboración y seguimiento del mapa por parte del líder del proceso).
b) Verifica la correspondencia entre el proceso, la actividad(es) identificada(s) como crítica(s) y el mapa de riesgos.

c) Verifica que los controles incorporados en el mapa de riesgos existen, funcionan según la periodicidad establecida y son efectivos.
d) Realiza seguimiento a la ejecución de las acciones establecidas en el plan de tratamiento del riesgo
e) Revisa la vinculación del mapa de riesgos del proceso al mapa de riesgos institucional
f) Verifica si ha existido la materialización de riesgos que pueden generar productos y/o servicios no conformes.
g) Verifica las evidencias del monitoreo realizado por el líder del proceso de acuerdo con la periodicidad establecida.
h) Verifica la aplicación de la Política de Administración de Riesgos en la SIC
i) Emite informes acerca de la gestión de riesgos, y los presenta al Comité de Coordinación de Control Interno. Estos informes pueden contener:

- Los avances de las acciones-actividades propuestas en los mapas de riesgo.
- La aplicación de la política institucional para el tratamiento de los riesgos asociados a procesos
- Conclusiones relacionadas con la eficacia de las opciones de manejo aplicadas para tratar el riesgo
- Cambios en las etapas de identificación, análisis y/o valoración del riesgo por proceso.

El resultado de la evaluación y seguimiento se debe registrar en el aplicativo SIGI-módulo de riesgos, en la opción Seguimiento. (Ver documentos Anexos, manual módulo de riesgos).

7.8.3 Formular plan de mejoramiento (si aplica)

Una vez la Oficina de Control Interno, realice la evaluación y seguimiento, informa al líder del proceso del resultado de la evaluación. Si derivado de los resultados es necesario formular un plan de mejoramiento, el líder del proceso lo formula, de acuerdo con lo establecido en el documento CI02-P05 Procedimiento Acciones Correctivas y Preventivas.

7.9 ETAPA 9: REALIZAR DIVULGACIÓN, CONSULTA Y CONTROL DE LOS MAPAS DE RIESGOS

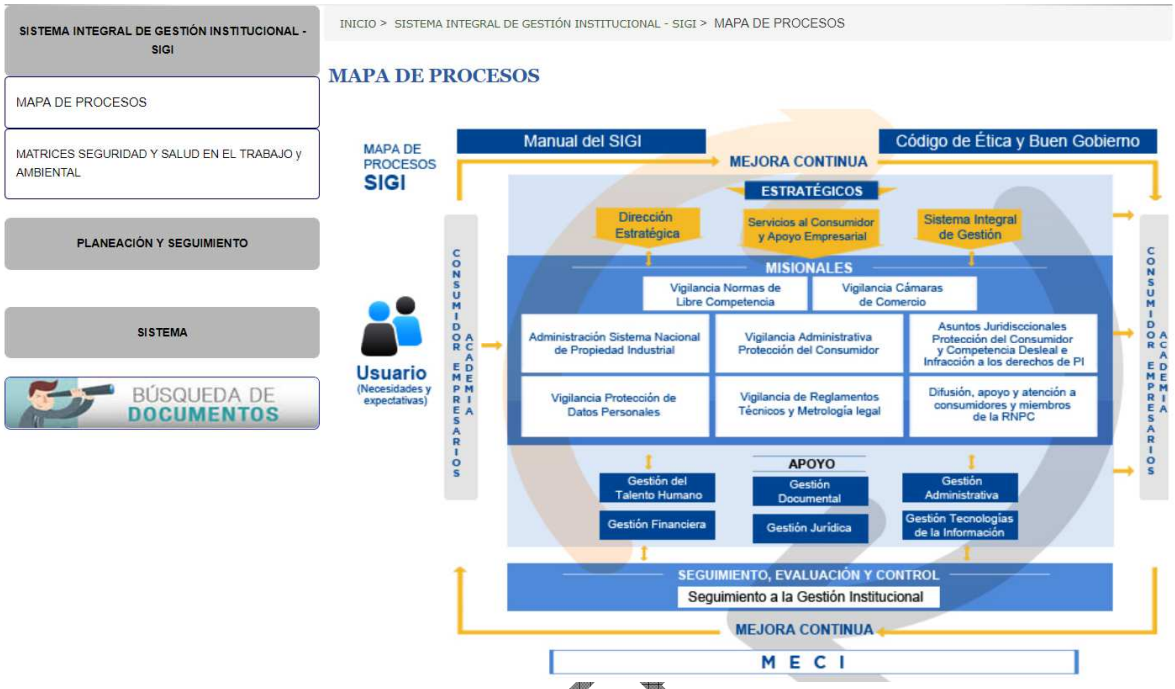
7.9.1 Consultar mapa de riesgos

En la Superintendencia de Industria y Comercio cualquier usuario interno o externo puede consultar el Mapa de Riesgo Institucional y los Mapas de Riesgo por Proceso (Mapa de Riesgo General) de la siguiente manera:

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

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

De inmediato tendrá acceso a la página principal del Sistema Integral de Gestión Institucional SIGI, en donde se selecciona el proceso del cual se quiere consultar la información de los riesgos.



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

En el botón "riesgos", al hacer clic, encontrará dos botones en donde se puede seleccionar el riesgo a consultar, corrupción o gestión:

7.9.2 Controlar y registrar la administración del riesgo

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

8 DOCUMENTOS RELACIONADOS

Anexo 1.Política de Administración del Riesgo
Anexo 2. Controles 27001
CI02-P03 Producto No Conforme
DE01-P01 Formulación de la Planeación Institucional
SC01-P01 Documentación y Actualización del Sistema Integral de Gestión Institucional SIGI
SC05-I02 Metodología para la identificación, clasificación y valoración de activos de información
SC01-F07 Mapa de Riesgos por Procesos
SC01-F09 Caracterización de Procesos
SC05-F03 Registro de activos de información.

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Se incluyen lineamientos para la gestión de riesgos de seguridad de la información y se actualizan los criterios para la identificación, análisis, evaluación y tratamiento de los riesgos de acuerdo a la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas versión 4 octubre de 2018.

_____
Fin documento