MANUAL DE ADMINISTRACIÓN INTEGRAL DEL RIESGO

Superintendencia del subsidio Familiar

Abril 2024

Edificio World Business Port
Carrera 69 # 25 B - 44 – Pisos 3, 4 y 7
Teléfonos: (601)3487777
PBX: (601)3487800
www.ssf.gov.co – e-mail: ssf@ssf.gov.co
Bogotá D.C, Colombia

1 INTRODUCCIÓN

Para la Superintendencia del Subsidio Familiar (SSF) es de primordial importancia asegurar razonablemente el logro de los objetivos estratégicos, así como el de los objetivos de los procesos, programas y proyectos, para de esta manera cumplir con su misión de ejercer la inspección, vigilancia y control de las entidades encargadas de recaudar los aportes y pagar las asignaciones del subsidio familiar. Por tal motivo ha desarrollado una metodología adecuada a su condición de entidad pública, a las características de los procesos, a la normatividad aplicable y a la naturaleza de los servicios que presta, que le permita identificar, analizar, evaluar y tratar efectivamente los riesgos de gestión, fiscales, de corrupción y de seguridad de la información.

La versión 6 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP), la cual adicionalmente a los cambios ya incluidos en la versión 5 en donde se modificaron y actualizaron los elementos metodológicos para mejorar la identificación y valoración de los riesgos, incluye también un acápite especial en donde se establecen los lineamientos para la gestión de los riesgos fiscales que tiene como propósito prevenir y mitigar eventos que puedan generar daño al patrimonio público que implique perjuicio, perdida o deterioro de los bienes o recursos públicos.

En este sentido la SSF actualiza su propia metodología para la administración integral de los riesgos de la entidad alineándola a los nuevos lineamientos que en materia de gestión del riesgo imparte el Departamento Administrativo de la Función Pública.

Por otra parte, la metodología propuesta en el presente manual se articula con lo establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1.) en el marco del Plan Anticorrupción y de Atención al Ciudadano que define las estrategias de lucha contra la corrupción y de atención al ciudadano y por lo tanto establece los lineamientos para la identificación y valoración de riesgos de corrupción que hacen parte del componente 1: gestión del riesgo de corrupción como parte de las acciones de la entidad en la lucha contra la corrupción.

Así mismo el presente manual da respuesta a lo establecido en la Política de Seguridad Digital y en el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

2 GLOSARIO

A continuación, se presentan los términos y definiciones más relevantes frente a la gestión integral del riesgo los cuales son tomados de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Apetito al Riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Capacidad del Riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Confidencialidad de la información: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Contexto. Factores externos e internos que pueden afectar la capacidad de la Entidad para alcanzar los objetivos y metas.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas

Contexto externo: Factores externos a la entidad sobre los cuales no tiene control directo pero que pueden afectar positiva o negativamente su capacidad para alcanzar los objetivos y metas.

Contexto interno: Factores internos a la entidad sobre los cuales tiene control directo y pueden afectar positiva o negativamente su capacidad para alcanzar los objetivos y metas.

Control: Medida que permite reducir o mitigar un riesgo.

Corrupción: Uso del poder, por acción o por omisión, para desviar la gestión de lo público hacia el beneficio particular.

Disponibilidad de la información: Propiedad de la información de ser accesible y utilizable a demanda por una entidad.

Factor de riesgo: Son las fuentes generadoras de riesgos.

Fuente generadora de riesgos: Elemento del factor del contexto que solo en combinación tiene el potencial intrínseco de originar un riesgo o una oportunidad.

Integridad de la Información: Propiedad de la exactitud y completitud de la información.

Matriz de riesgos: Herramienta que permite visualizar cuáles son los riesgos que han sido identificados por la entidad y su estado de gestión

Modelo Integrado de Planeación y de Gestión: Marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, de acuerdo con el Decreto1499 de 2017.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo está dada por Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las Entidades del orden nacional, departamental y municipal.

Privacidad: Derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete y que tiene obligación de proteger dicha información en observancia del marco legal vigente.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Está asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Riesgo de Gestión: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo Fiscal: Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo Inherente: Nivel de riesgo propio de la actividad, es el resultado de combinar la probabilidad con el impacto, permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: Resultado de aplicar la efectividad de los controles al riesgo inherente.

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

Tratamiento del riesgo: acciones que define la Entidad, tendientes a establecer o fortalecer un control que permita evitar, reducir o transferir un riesgo.

Fuente: Guía Para La Administración del Riesgo y El Diseño de Controles en Entidades Públicas, Versión 5.

3 MARCO NORMATIVO

A continuación, se presenta el conjunto de normas aplicables a las entidades y organismos del estado en el marco de la gestión integral del riesgo.

- **LEY 87 DE 1993** "*Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"*: Artículo 2 literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Artículo 2 literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

- **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 *"Plan Anticorrupción y de Atención al Ciudadano"*. Cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos, las estrategias anti trámites y los mecanismos para mejorar la atención al ciudadano.

- **DECRETO 2641 DE 2012** *"Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011":* ARTÍCULO 1. Señálese como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano".

- **DECRETO 1083 DE 2015** *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública"*: CAPÍTULO 5 *"Elementos técnicos y administrativos que fortalezcan el Sistema de Control Interno en las entidades y organismos del Estado*", ARTÍCULO 2.2.21.5.4 *"Administración de riesgos"*. Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspecto tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos.

- **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 de Atención al Ciudadano": TÍTULO 4 *"Plan Anticorrupción y de Atención al Ciudadano"*. ARTÍCULO 2.1.4.2. *"Mapa de Riesgos de Corrupción*". Señálense come metodología para diseñar y hacer

seguimiento al Mapa de Riesgo de Corrupción de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el documento "Guía para la Gestión del Riesgo de Corrupción".

- **DECRETO 648 DE 2017** *"Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública":* SECCIÓN 2 *"Protección Especial"* ARTÍCULO 2.2.21.1.6 *"Funciones del Comité Institucional de Coordinación de Control Interno"*. Literal g. Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

- **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": TÍTULO 23 Articulación del Sistema de Gestión con los Sistemas de Control Interno. ARTÍCULO 2.2.23.2. "Actualización del Modelo Estándar de Control Interno". La actualización del Modelo Estándar de Control Interno para el Estado Colombiano – MECI, se efectuará a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, el cual será de obligatorio cumplimiento y aplicación para las entidades y organismos a que hace referencia el artículo 5 de la Ley 87 de 1993.

- **ACTO LEGISLATIVO 04 DE 2019** Por medio del cual se fundamenta la necesidad de un ejercicio preventivo del control fiscal, que detenga el daño fiscal e identifique los riesgos fiscales; de esta manera, la administración y el gestor fiscal pueden adoptar las medidas respectivas para prevenir la concreción del daño patrimonial de naturaleza pública

4 OBJETIVO

El objetivo del presente manual es establecer y formalizar la metodología que será aplicada en la Superintendencia del Subsidio Familiar para la administración de los riesgos de gestión, fiscales, de corrupción y de seguridad de la información en todas sus etapas tomando como base el análisis del contexto de la entidad. La metodología desarrollada en el presente manual define los detalles para llevar a cabo las actividades de identificación, análisis, evaluación, tratamiento, monitoreo y reporte de los riesgos de la Entidad. Con el desarrollo y documentación de esta metodología se da cumplimiento a lo establecido en la Política Integral de Administración de Riesgos de la Superintendencia del Subsidio Familiar.

5 ALCANCE

Las directrices establecidas en el presente manual son de obligatoria aplicación para todos los riesgos que aborda la Entidad en los procesos, programas y proyectos en todos los niveles, desde el análisis del contexto interno y externo de la Superintendencia, hasta la identificación, evaluación, tratamiento, monitoreo, seguimiento y reporte de los riesgos de gestión, fiscales, de corrupción y de seguridad de la información.

6 ARTICULACIÓN DE LA GESTIÓN DEL RIESGO CON EL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN – MIPG Y CON EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI

El Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de las Tecnologías de la Información y Comunicaciones desarrollaron la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas en su versión 5 como una herramienta con un enfoque preventivo que permite a las entidades públicas establecer sus propias directrices para gestionar de manera efectiva sus riesgos de gestión, corrupción y seguridad de la información.

Lo anterior permite la articulación con el MSPI (Modelo de Seguridad y Privacidad de la Información), debido a que integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad de la información, ya que esta práctica constituye su base fundamental. La guía para la gestión del riesgo de función pública, junto con el *Anexo 4. Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC)*, conllevan a cumplir dichas tareas de gestión de riesgo de seguridad de la información requeridas en el MSPI.

En este sentido el presente manual fija las bases metodológicas para la Superintendencia del Subsidio Familiar y de esta manera se garantice la articulación de la Entidad con las disposiciones que en materia de gestión del riesgo determina el Modelo Integrado de Planeación y Gestión en su manual operativo versión 3, lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas en su versión 5 y el Modelo se Seguridad y Privacidad de la Información.

La articulación se presenta de la siguiente manera:

1. Las actividades de identificación de activos de información así como la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información se alinean con la fase de Planificación del MSPI.
2. Las actividades de implementación de los planes de tratamiento para los riesgos de seguridad de la información se reflejan en la fase de Implementación del MSPI.
3. Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de medición del desempeño del MSPI.
4. Las actividades de mejoramiento continuo en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de medición del desempeño para identificar aspectos a mejorar en la implementación de ambos modelos.

7 DECLARACIÓN DE LA POLÍTICA INTEGRAL DE ADMINISTRACIÓN DEL RIESGO DE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR

"La Superintendencia del Subsidio Familiar consciente de la importancia del logro de la misión, de la visión, de los objetivos estratégicos y de los objetivos de los procesos, se compromete a identificar, analizar, evaluar, tratar y hacer seguimiento a los riesgos de gestión, fiscales, de corrupción y de seguridad de la información a los que está expuesta, a través del diseño y aplicación de controles efectivos y aplicando una metodología propia y adecuada a sus características".

La Política Integral de Administración del riesgo de la entidad se encuentra formalizada en la entidad a través de un documento con su mismo nombre y el cual contiene los siguientes componentes definidos por la Guía de Administración del Riesgo y Diseño de Controles en Entidades Públicas versión 5:

- Alcance de la política
- Objetivo de la política
- Responsabilidades frente a la gestión de acuerdo con las líneas de defensa.
- Niveles de Apetito al riesgo
- Tolerancia al riesgo
- Capacidad del riesgo
- Criterios de evaluación del riesgo
- Tratamiento del riesgo

8 TIPOS DE RIESGOS EN LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR

La Guía de Administración del Riesgo y Diseño de Controles para Entidades Públicas versión 5, ha establecido para las entidades públicas tres tipos principales de riesgos:

- **RIESGO DE GESTIÓN**: Efecto que se causa sobre los objetivos de la entidad, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de eventos externos.

- **RIESGO FISCAL**: Se define como el efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial

- **RIESGO DE CORRUPCIÓN:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- **RIESGO DE SEGURIDAD DE LA INFORMACIÓN:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

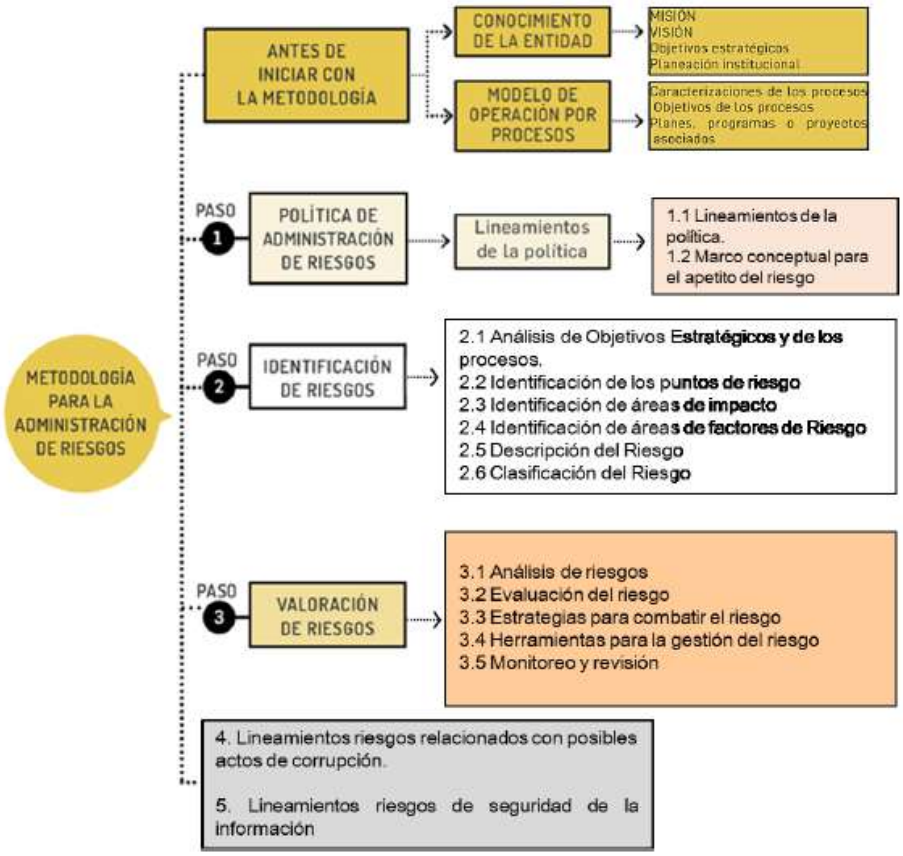
9 METODOLOGÍA PARA LA GESTIÓN DE LOS RIESGOS EN LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR

La metodología implementada por la SSF está diseñada para responder a las necesidades particulares de la Entidad y se adapta a las características propias de su estructura orgánica, los procesos y la naturaleza de las actividades que desarrolla para cumplir su misión.

La metodología para la gestión del riesgo está estructurada en la aplicación sistemática de etapas que van desde el establecimiento del contexto hasta las actividades de seguimiento y revisión e informe de los resultados de la gestión.

A continuación, se presenta el esquema en donde se ilustran los pasos propuestos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6 para la gestión de los riesgos en entidades públicas

Figura 1. pasos para la gestión del riesgo de acuerdo con la Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas v5



9.1 Identificación del Riesgo

La identificación de los riesgos consiste en encontrar, reconocer y describir los posibles eventos pueden afectar positiva o negativamente el logro de los objetivos de la entidad, sus procesos, planes o proyectos.

La identificación de los riesgos de gestión se realiza con base en el resultado del análisis de los elementos del contexto interno y externo que pueden tener impacto en el logro de los objetivos de la Entidad; a partir de este análisis se determinan los posibles eventos que pueden afectar negativa o positivamente los objetivos, se establecen sus causas potenciales y sus consecuencias potenciales.

En la SSF, la Oficina Asesora de Planeación realizará el acompañamiento metodológico en los ejercicios de identificación de los riesgos de gestión en todos los niveles.

Es responsabilidad del equipo directivo (línea estratégica) revisar los objetivos estratégicos e identificar los riesgos y oportunidades que pueden afectar esos objetivos.

El ejercicio de identificación de los riesgos de gestión para los procesos se realiza por parte de los responsables de los procesos y sus equipos (primera línea de defensa) con base en la posible afectación a los objetivos de cada proceso.

Para realizar una correcta identificación de los riesgos en la SSF es necesario llevar a cabo los siguientes pasos:

- Análisis de los Objetivos Estratégicos y de los Procesos.
- Identificación de los puntos de Riesgo.
- Identificación de las áreas de impacto.
- Identificación de las áreas de factores de riesgo.
- Identificación de puntos de riesgo fiscal.

9.1.1 Análisis de los Objetivos Estratégicos y de los Procesos

Los objetivos estratégicos son la base para la identificación de los riesgos estratégicos que corresponden a los eventos que pueden dificultar o impedir el logro de estos objetivos.

Antes de iniciar la identificación de los riesgos estratégicos, la entidad debe asegurarse a través de los ejercicios de Planeación Estratégica de la alineación de los objetivos estratégicos con la misión y la visión de la entidad, así como de su adecuada formulación, por lo que los objetivos estratégicos son un insumo del proceso de Direccionamiento Estratégico para el ejercicio de la identificación de los riesgos estratégicos.

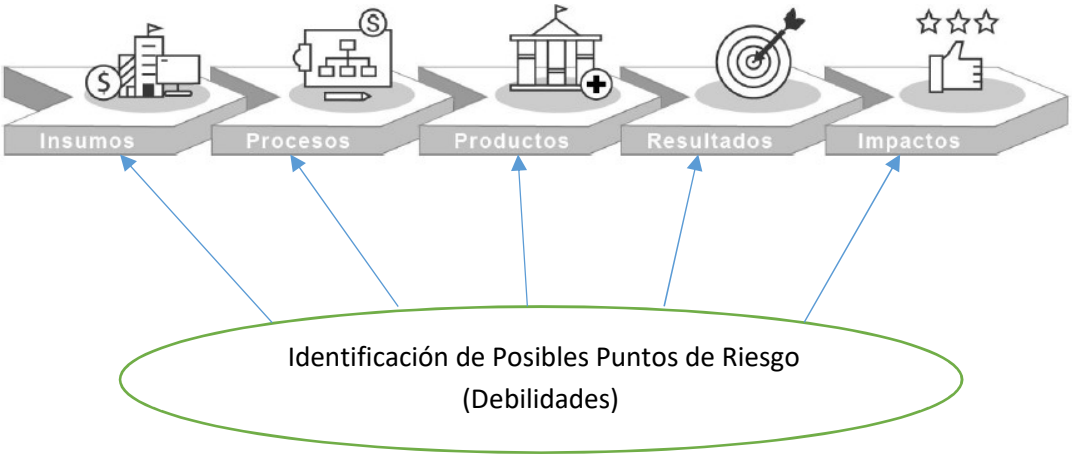
Los objetivos de los procesos establecen el propósito de cada proceso que debe estar alineado con los objetivos estratégicos y por ende con la visión y misión de la entidad. La identificación de los riesgos de los procesos se realiza con base en los posibles eventos que pueden afectar el cumplimiento de los objetivos asociados a estos procesos.

9.1.2 Identificación de los Puntos de Riesgo

Los puntos de los puntos de riesgo son las actividades dentro del flujo de procesos en donde se pueden presentar eventos de riesgo que pueden afectar el cumplimiento de los objetivos de los procesos.

La identificación de los puntos de riesgo se realiza sobre la cadena de valor del proceso, por lo que la realización de este paso en la SSF se debe realizar con base en los documentos de caracterización de los procesos, en dónde se pueden

identificar puntos de riesgo en las entradas, las actividades, las salidas o en los recursos del proceso. Estos puntos de riesgos pueden definirse como debilidades del proceso dentro de un ejercicio de análisis interno, el cual puede sustentarse a partir de un estudio de capacidades del proceso y determinarse como estas debilidades pueden afectar los resultados de los procesos o a los usuarios de estos resultados.



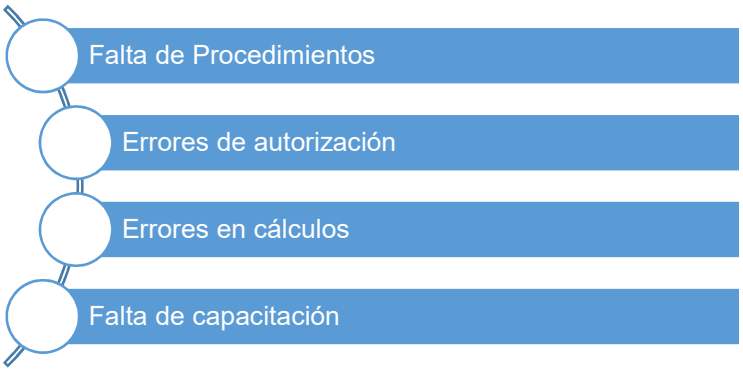
9.1.3 Identificación de Áreas de Impacto

Las áreas de impacto corresponden a los efectos o consecuencias de la materialización de un evento de riesgo, de acuerdo con lo establecido por la Guía para la Administración del Riesgo y el Diseño de Controles Eficaces versión 5, para las entidades públicas las únicas consecuencias que aplican son las de tipo reputacional o presupuestal. Por lo que al momento de realizar la valoración del riesgo se deben considerar estos dos tipos de afectaciones para determinar los niveles de criticidad del riesgo.

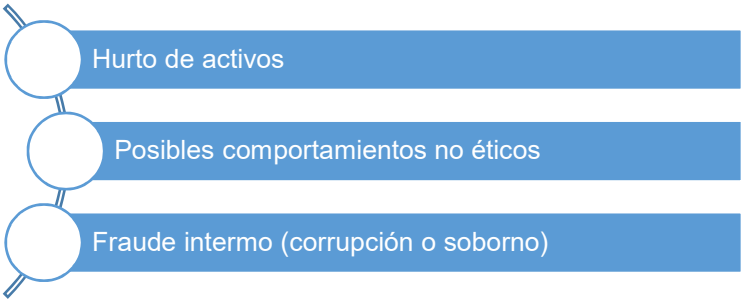
9.1.4 Identificación de Áreas de Factores de Riesgo

Los factores de riesgo corresponden a las fuentes generadores de los riesgos y factores de, las cuales pueden presentarse como causas de materialización de eventos de riesgos. De acuerdo con la Guía para la Administración del Riesgo y el Diseño de Controles Eficaces versión 5. Las fuentes generadoras de riesgos en las entidades públicas pueden ser:

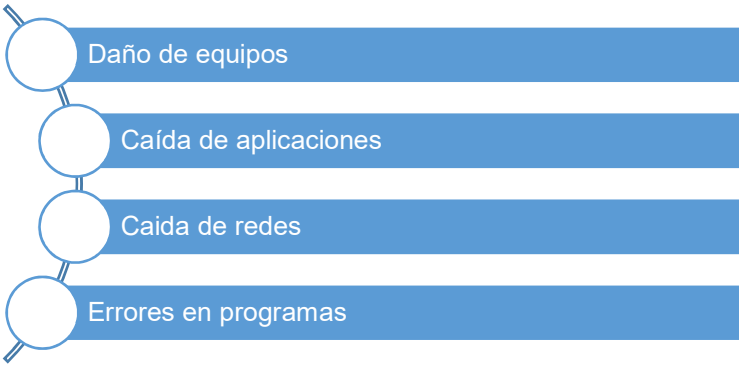
- **PROCESOS**: Eventos relacionados con errores o fallas en la ejecución de las actividades de los procesos



- **TALENTO HUMANO:** Eventos asociados al desempeño del personal o a su comportamiento, se incluyen factores asociados a la seguridad y salud en el trabajo y a actos intencionales frente a situaciones de corrupción.

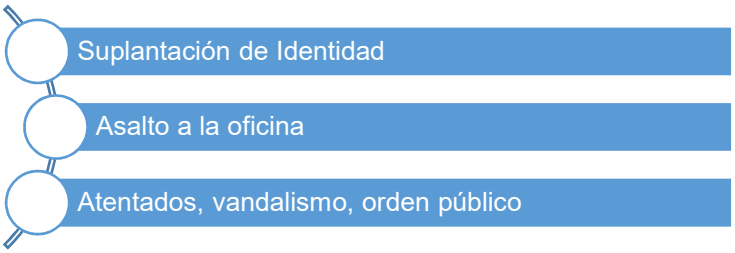


- **TECNOLOGÍA:** Eventos relacionados con la infraestructura tecnológica de la entidad



- **INFRAESTRUCTURA:** Eventos relacionados con la infraestructura física de la entidad

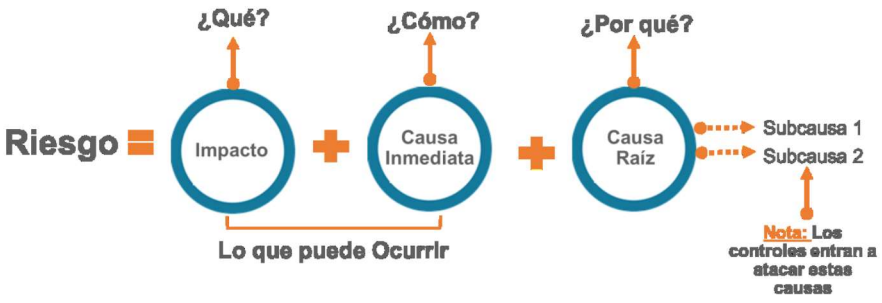
- **FACTORES EXTERNOS:** Son situaciones externas que pueden afectar a la entidad



Nota: Durante los ejercicios de análisis y monitoreo que realiza la Entidad a su contexto, se pueden identificar factores o fuentes generadoras de riesgos que no estén incluidas en el listado anterior y las cuales también pueden ser tomadas para la identificación y análisis de los riesgos en la SSF.

9.1.5 Descripción de los Riesgos

Consiste en detallar las características del riesgo para determinar la información necesaria de manera que se pueda comprender el riesgo por parte del líder del proceso como por otras personas de la entidad o externas a la misma. Por lo anterior la estructura para la descripción de los riesgos en la Entidad es la siguiente:



Se debe iniciar con las palabras" **Posibilidad de…",** posteriormente se redacta el **Impacto**, la **Causa Inmediata** y las **Causas Raíz.** A continuación, se presenta un ejemplo de redacción de un riesgo de gestión en la SSF:

Ejemplo Redacción Riesgo de Gestión en la SSF

Posibilidad de afectación reputacional por perdida de oportunidad en la atención a las solicitudes y necesidades de los grupos de interés internos y externos debido a la ausencia de un plan de continuidad que permita responder ante eventuales escenarios de interrupción

De acuerdo con lo anterior el riesgo puede desglosarse de la siguiente manera para facilitar su análisis

Impacto: Son las consecuencias para la entidad resultantes de la materialización del riesgo y estas deben establecerse solamente a nivel de la afectación reputacional o presupuestal.

Causa Inmediata: Constituye el evento propio de riesgo que de maternizarse puede afectar los objetivos del proceso, programa o proyecto en dónde se presenta o incluso podría llegar a afectar los objetivos institucionales generando los impactos reputacionales o presupuestales referenciados en el punto anterior.

Causa Raíz: Es la causa o causas básicas que en caso de no controlarse pueden originar la materialización del riesgo. Estas causas son las bases para el establecimiento de controles en la etapa de valoración.

9.1.6 Clasificación de los Riesgos

La siguiente tabla muestra las categorías de riesgos propuestas la Guía para la Administración del Riesgo y el Diseño de Controles Eficaces versión 5 permiten la agrupación y consolidación de los diferentes tipos de riesgos de acuerdo con su naturaleza.

Tabla 1. Categorías de Riesgos

CATEGORIA DEL RIESGO	FACTOR DE RIESGO ASOCIADO	DESCRIPCIÓN
Ejecución y Administración de Procesos	Procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude Externo	Evento Externo	Pérdidas derivadas de actos de fraude por persona ajenas a la entidad

CATEGORIA DEL RIESGO	FACTOR DE RIESGO ASOCIADO	DESCRIPCIÓN
Fraude Interno	Talento Humano	Pérdida debido a actos de fraude, actos irregulares, comisión de hechos delictivos, abuso de confianza, aprobación indebida, incumplimiento de regulaciones legales o internas de la entidad, en dónde hay participación de servidores o funcionarios de la SSF.
Fallas Tecnológicas	Tecnología	Errores de hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones Laborales	Factores Varios	Pérdidas originadas de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, Productos y Prácticas Organizacionales	Factores Varios	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a estos.
Daños Activos Físicos	Infraestructura Evento Externos	Pérdida por daños o extravío de los activos físicos por desastres naturales u otros eventos.

9.1.7 Identificación de los Riesgos Fiscales

La identificación de riesgo fiscal se basa en el establecimiento de puntos de riesgos fiscales los cuales se pueden presentar en los diferentes procesos de la entidad y que corresponden a las actividades donde se gestionan o manejan recursos y bienes públicos y que por ende puedan generar eventos de pérdida o detrimento de los mismos.

A continuación, se presenta una tabla con los posibles puntos de riesgo fiscal en la superintendencia del subsidio familiar.

Tabla 2. Puntos de Riesgo Fiscal en la SSF

Referencia	Puntos de Riesgo Fiscal	Circunstancia Inmediata	Proceso Relacionado en la SSF
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción	Contratación, Gestión Jurídica y Gestión Financiera y Presupuestal
2	Cumplimiento de obligaciones	Pago de Intereses moratorios	Gestión Financiera y Presupuestal
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio dela entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente	Talento Humano , Gestión administrativa
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos	Gestión Financiera y Presupuestal
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados	Sin especificar
6	Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad	Recursos físicos almacén e inventarios
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público	Sin especificar
8	Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad	Recursos físicos almacén e inventarios
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado	Gestión Jurídica
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones	Gestión Jurídica
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad	Gestión Jurídica

Referencia	Puntos de Riesgo Fiscal	Circunstancia Inmediata	Proceso Relacionado en la SSF
		de recuperar los recursos pagados por el Estado	
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios	Gestión Jurídica
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad	Contratación.
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos	Contratación.
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad	Cada contrato
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia	Cada contrato
17	Suscripción de contratos	Sobrecostos en precios contractuales	Cada contrato
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron	Cada contrato
19	Suscripción de contratos	No incluir en el contrato de seguros - amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad	Cada contrato
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual	Cada contrato
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley	Cada contrato

Línea Atención al Ciudadano +57 (601) 348 77 77
Línea Gratuita Nacional 018000 910 110
PBX :+57 (601) 348 78 00
Portal Institucional www.ssf.gov.co
Correo electrónico ssf@ssf.gov.co
Carrera 69 No. 25 B – 44 Pisos 3, 4 y 7
Bogotá - Colombia

Referencia	Puntos de Riesgo Fiscal	Circunstancia Inmediata	Proceso Relacionado en la SSF
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.	Cada contrato
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio	Cada contrato
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante	Cada contrato
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo	Contratación.
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público	Contratación.
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad	Contratación.
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final	Cada contrato
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto	Cada contrato
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato	Cada contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal	Contratación.

Línea Atención al Ciudadano +57 (601) 348 77 77
Línea Gratuita Nacional 018000 910 110
PBX :+57 (601) 348 78 00
Portal Institucional www.ssf.gov.co
Correo electrónico ssf@ssf.gov.co
Carrera 69 No. 25 B – 44 Pisos 3, 4 y 7
Bogotá - Colombia

Referencia	Puntos de Riesgo Fiscal	Circunstancia Inmediata	Proceso Relacionado en la SSF
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra	Cada contrato
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato	Cada contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado	Cada contrato
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio	Cada contrato
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista	Gestión Financiera y Presupuestal
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación	Gestión Financiera y Presupuestal
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo	Cada contrato
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratistas	Cada contrato
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad	Cada contrato
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades	Cada contrato
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento	Recursos físicos almacén e inventarios
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo	Cada contrato
43	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)	Gestión Financiera y Presupuestal

Línea Atención al Ciudadano +57 (601) 348 77 77
Línea Gratuita Nacional 018000 910 110
PBX :+57 (601) 348 78 00
Portal Institucional www.ssf.gov.co
Correo electrónico ssf@ssf.gov.co
Carrera 69 No. 25 B – 44 Pisos 3, 4 y 7
Bogotá - Colombia

Referencia	Puntos de Riesgo Fiscal	Circunstancia Inmediata	Proceso Relacionado en la SSF
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas	Recursos físicos almacén e inventarios
45	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad	Recursos físicos almacén e inventarios
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones	Sin determinar
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas	Sin determinar
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley	Sin determinar
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado	Sin determinar
50	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial	Gestión Jurídica

Redacción del Riesgo Fiscal:

De acuerdo con las Guía para la administración del riesgo y diseño de controles eficaces V6 Para redactar un riesgo fiscal se debe tener en cuenta:

Iniciar con la oración: Posibilidad de, debido a que es un evento potencial

Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.

Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada.

9.1.8 Identificación de Riesgos de Corrupción

La identificación de los riesgos de corrupción se realiza de la misma manera que para los riesgos de gestión. Para la identificación de los riesgos de corrupción, es necesario validar que el riesgo identificado corresponda con la definición del riesgo de corrupción mediante la utilización del esquema guía de validación de riesgos de corrupción que se presenta a continuación. Si el riesgo identificado no cumple con todas las características definidas en dicha matriz, no se considera riesgo de corrupción.

La redacción de los riesgos de corrupción debe considerar las características que se presentan en la siguiente tabla:

Tabla 2. Esquema de Validación de Riesgos de Corrupción

Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo publico	Beneficio Privado
Ejemplo: Adendas que cambian condiciones generales del proceso de contratación para favorecer a terceros	Ejemplo: Modificar el pliego de condiciones mediante Adendas expedidas antes del vencimiento del plazo para presentar ofertas.	Ejemplo: Favorecer a terceros	Ejemplo: Injerencia de externos sobre la Entidad para favorecer intereses particulares Detrimento particular	Ejemplo: Intereses personales Favorecimiento a terceros

Los resultados de la identificación de los riesgos de corrupción se registran en la matriz de riesgos de corrupción de la entidad.

9.1.9 Identificación de Riesgos de Seguridad de la Información

Para realizar la identificación de los riesgos de seguridad de la información es necesario primero realizar la identificación de los activos de seguridad de la información entendiendo por estos los elementos que utiliza la Entidad para funcionar en el entorno físico o digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, entre otros.

Después se procederá a valorar el activo determinando la importancia de los mismos en el logro de los objetivos de los procesos y de la Entidad y bajo este criterio se establece la criticidad y los controles adecuados para su protección.

Para cada activo evaluado como crítico se identificarán los riesgos de seguridad de la Información, estos pueden ser de tres tipos según al atributo de la seguridad de la Información que impacte:

a. Afectación de la Confidencialidad
b. Afectación de la Integridad
c. Afectación de la Disponibilidad

Posteriormente a la identificación de los riesgos de Seguridad de la Información para cada activo, se agrupan los activos por tipo de riesgo para realizar el análisis de las amenazas y vulnerabilidades que podrían causar su materialización.

9.1.9.1 *Identificación y Valoración de los Activos de Información*

La identificación y valoración de activos de información debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo un ejercicio orientado por el responsable de seguridad de la información de la Entidad con el acompañamiento de la Oficina Asesora de Planeación como segunda línea de defensa para la gestión del riesgo.

Así mismo los activos de información pueden ser clasificados en diferentes tipos de acuerdo con su naturaleza. En la siguiente tabla se presenta la clasificación de los tipos de activos de seguridad de la información.

Tabla 3. Activos de Información

TIPO DE ACTIVO	DESCRIPCIÓN
DATOS / INFORMACIÓN	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
SOFTWARE	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades

TIPO DE ACTIVO	DESCRIPCIÓN
HARDWARE	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
SERVICIOS	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
COMPONENTES DE RED	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
PERSONAS	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
INFRAESTRUCTURA	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la entidad
PROCESOS	Procedimientos, buenas prácticas, directrices, políticas y lineamientos de la entidad para la realización o ejecución de sus funciones misionales

9.1.9.2 *Identificación de Vulnerabilidades de Seguridad de la Información*

Las vulnerabilidades se entienden como las debilidades en los activos de seguridad de la Información o en su administración lo que incrementa el grado de exposición ante las posibles amenazas facilitando de esta manera la materialización de los riesgos.

Para identificar la vulnerabilidad se puede tomar como base la tabla de vulnerabilidades comunes definida en la ISO /IEC 27005: 2009.

Tabla 4. Vulnerabilidades Comunes de Seguridad de la Información

TIPO	VULNERABILIDADES
HARDWARE	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
SOFTWARE	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso

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

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

A continuación, se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas.

Tabla 5. Ejemplo de Vulnerabilidades Vs Amenazas

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Almacenamiento de medios sin protección	Hurto de medios o documentos
SOFTWARE	Ausencia de parches de seguridad	Abuso de los derechos
RED	Líneas de comunicación sin protección	Escucha encubierta
INFORMACIÓN	Falta de controles de acceso físico	Hurto de información
PERSONAL	Falta de capacitación en las herramientas	Error en el uso
ORGANIZACIÓN	Ausencia de políticas de seguridad	Abuso de los derechos

A continuación, se presenta un ejemplo de Identificación de riesgos de seguridad de la información.

Ejemplo de Riesgo de Seguridad de la Información

ACTIVO	RIESGO	DESCRIPCIÓN	TIPO	CAUSAS		CONSECUENCIAS
				Amenazas	Vulnerabilidades	
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	S.I.	Modificación no autorizada	Falta de políticas de Seguridad digital Ausencia de políticas de control de acceso Contraseñas sin protección Autenticación débil	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización de riesgos (legales, económicos, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.

Los riesgos de seguridad de la información se basan en la afectación de tres principios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”.

Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización; las cuales son denominadas como “causas” en la identificación de los riesgos de gestión y de corrupción.

9.2 Valoración del Riesgo

Esta etapa consiste en comprender la naturaleza y el nivel del riesgo, lo anterior permite conocer el perfil de riesgo de la SSF en términos de criticidad, así mismo permite establecer prioridades para intervenir los riesgos. Para tal fin es necesario determinar el nivel de riesgo el cual resulta de analizar el nivel de probabilidad de ocurrencia y el nivel de impacto o consecuencias de cada riesgo identificado, con el fin de estimar la zona de riesgo inicial o (RIESGO INHERENTE), lo cual indica que se trata del nivel de riesgo sin aplicación de controles.

Para realizar el análisis de los riesgos se deben seguir los siguientes pasos.

9.2.1 Determinación del Nivel de Probabilidad del Riesgo

Consiste en evaluar de la manera más objetiva posible que tan expuesta esta la Entidad frente al riesgo que se está analizando. Para efectos del cálculo del nivel de probabilidad y para evitar la subjetividad en el ejercicio, el nivel de probabilidad se determinará considerando el número de veces que se realiza la actividad en dónde se presenta el riesgo durante un periodo de un año. De acuerdo con lo anterior em la siguiente tabla se presentan los criterios para determinar el nivel de probabilidad de los riesgos.

Tabla 6. Tabla Niveles de Probabilidad

Nivel de Probabilidad	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo dos veces al año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta de 501 a 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces al año	100%

9.2.2 Determinación del Nivel de Impacto del Riesgo

Consiste en estimar de la manera más objetiva posible los efectos en caso de que el riesgo se materialice. Para determinar el nivel de impacto se deben considerar las consecuencias relacionadas para cada riesgo en la etapa de identificación las cuales están definidas en función de la afectación reputacional o presupuestal para que con base en ellas se establezca el nivel de afectación que representa la materialización del riesgo para la Entidad.

De acuerdo con lo anterior em la siguiente tabla se presentan los criterios para determinar el nivel de impacto de los riesgos.

Tabla 7. Tabla Niveles de Impacto

Nivel de Impacto	Afectación económica	Afectación Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de un área de la entidad
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente.
Moderado 60%	Entre 51 y 100 SMLMV	El riesgo afecta la imagen de la entidad externamente con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 101 y 500 SMLMV	El riesgo afecta la imagen de la entidad externamente con efecto publicitario negativo a nivel del sector trabajo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional con efecto publicitario negativo sostenido

Nota: Con el propósito de minimizar el grado de subjetividad al momento de estimar los niveles de probabilidad e impacto en los ejercicios de análisis de riesgos, es necesario la utilización de fuentes de información confiables basadas en datos históricos, estadísticas de los procesos o el uso de bases confiables para la realización de proyecciones en caso de que sea necesario.

9.2.3 Determinación del Nivel de Riesgo Inherente

El nivel de riesgo inherente es el resultado de analizar el nivel de probabilidad y el nivel de impacto. El nivel de riesgo inherente permite ubicar la Zona de Riesgo Inherente para cada riesgo, es decir la ubicación del riesgo en el mapa de calor de riesgos de la entidad, antes de la aplicación de controles.

De esta manera se puede establecer cuales riesgos se pueden aceptar y cuales necesitan la implementación de controles u otras medidas de tratamiento para mitigarlos. A este ejercicio se le conoce como evaluación del riesgo que es la siguiente etapa en la gestión del riesgo en la SSF.

9.3 Evaluación del Riesgo

Esta etapa consiste en comparar los resultados del análisis de los riesgos con los criterios de aceptación del riesgo de la Entidad.

Para lo anterior es necesario ubicar cada uno de los riesgos analizados en el mapa de zonas de calor de riesgo inherente, y de esta manera establecer cuales riesgos se pueden aceptar y cuales necesitan la implementación de controles u otras medidas de tratamiento para mitigarlos de acuerdo con los criterios de apetito, tolerancia y capacidad del riesgo definidos en la Política Integral de Administración del Riesgo de la SSF.

El mapa de zonas de calor varía para los riesgos de corrupción pues ningún riesgo de corrupción se puede aceptar.

A continuación, se presentan los mapas de zonas de calor para los riesgos de gestión y seguridad de la información y el mapa de zonas de calor para los riesgos de corrupción.

Mapa de Zonas de Calor para los Riesgos de Gestión, Fiscales y de Seguridad de la Información.

Tabla 8. Tabla Niveles de Severidad del Riesgo en la SSF y Zonas de Calor

EXTREMO	ALTO	MODERADO	BAJO

ZONAS DE CALOR MAPA DE RIESGOS DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN

		IMPACTO				
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
PROBABILIDAD	Muy baja 20 %					
	Baja 40%					

	Media 60%					
	Alta 80%					
	Muy Alta 100%					

ZONAS DE CALOR MAPA DE RIESGOS DE CORRUCIÓN

	IMPACTO	Moderado 60%	Mayor 80%	Catastrófico 100%
PROBABILIDAD	Muy baja 20 %			
	Baja 40%			
	Media 50%			
	Alta 80%			
	Muy Alta 100%			

9.4 Diseño y Evaluación de Controles

Debido a que en la Entidad el tratamiento del riesgo se realiza principalmente a través de la implementación de actividades de control, a continuación, se presenta la metodología para el diseño y evaluación de controles efectivos.

Los controles hacen referencia a las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Los controles se estandarizan y despliegan a través de la información documentada de la entidad sin embargo un documento como una política, un manual o un procedimiento no es por si solo un control.

Los controles por sí solos permiten prevenir la materialización del riesgo o mitigar los posibles impactos, por lo que actividades como sensibilizaciones, capacitaciones o acompañamientos no se consideran actividades de control.

Los controles están asociados a actividades como validaciones, verificaciones, seguimientos, chequeos, activación de planes de contingencia, activación planes de continuidad, ejecución de pólizas entre otros.

La identificación y aplicación de controles para la prevención y mitigación de los riesgos es responsabilidad de los líderes de los procesos en conjunto con sus equipos (primera línea de defensa, este ejercicio de identificación y diseño de controles debe estar acompañado desde la Oficina Asesora de Planeación (segunda línea de defensa)

Es responsabilidad de la tercera línea de defensa evaluar los controles en su efectividad.

9.4.1 Tipos de Control:

Los controles se pueden clasificar mediante dos grandes criterios: de acuerdo con su propósito y de acuerdo con su forma de ejecución

De acuerdo con su propósito, los controles se clasifican en tres tipos:

Los Controles Preventivos: Son los controles que están diseñados para evitar la materialización de un riesgo que pueda afectar el cumplimiento de los objetivos.
Los controles preventivos deben atacar las causas del riesgo, por lo que cada causa debe tener asociado al menos un control.

Los controles preventivos permiten disminuir el nivel de probabilidad del riesgo.

Ejemplo: La revisión que hace el supervisor del contrato para evitar que se presente un posible incumplimiento de las obligaciones contractuales por parte del contratista.

Los Controles Detectivos: Son los controles que están diseñados para detectar una posible materialización de un riesgo.

Al permitir la detección oportuna antes de la materialización de un riesgo, estos controles pueden evitar la materialización del mismo, pero generan reprocesos. Estos controles disminuyen la probabilidad del riesgo.

Ejemplo: Las conciliaciones que se realizan para detectar inconsistencias en la información contable o financiera antes de emitir informes financieros.

Los Controles Correctivos: Estos controles corresponden a acciones que se ejecutan después de que un riesgo se materializa.

Estos controles disminuyen el nivel de impacto de los riesgos.

Ejemplo: Las pólizas de cumplimiento que se aplican en los casos en los que se materializa el incumplimiento de un contrato y que busca mitigar el impacto económico del incumplimiento.

De acuerdo con forma de ejecución:

Los Controles Manuales: Estas actividades de control son ejecutadas directamente por los servidores de la entidad.

Ejemplo: La supervisión de la ejecución de un contrato por parte del respectivo supervisor del contrato.

Los Controles Automáticos: El control se aplica mediante un aplicativo o un sistema de información de manera automática.

Ejemplo: Conciliaciones contables automáticas realizadas por el aplicativo contable y que arroja errores que deben ser corregidos.

9.4.2 Estructura para la Redacción del Control

Responsable de ejecutar el Control: Se relaciona el cargo del servidor que realiza la actividad de control, en caso de que se trate de un control automático se identifica el sistema que ejecuta el control.

Acción: A través de los verbos apropiados se describe la actividad que se realiza para la ejecución del control.

Complemento: Se describe la información relevante que permita entender el propósito del control.

A continuación, se presenta un ejemplo de la redacción de un control bajo la estructura propuesta:

Ejemplo:

Riesgo:
Posibilidad de afectación reputacional por emitir, reglamentar y fijar directrices sobre temas financieros y contables sin la confiabilidad y razonabilidad requerida debido a errores en la información suministrada por las CCF.

Control:
El profesional especializado, verifica la veracidad y confiabilidad de la información remitida por las CCF a través de la validación frente referentes normativos y técnicos antes de la emisión de las directrices

9.4.3 Evaluación del Diseño de Controles.

Los criterios para la evaluación del diseño de controles se han estructurado a través de una lista de verificación que permite validar si los controles que la entidad aplica son fuertes o débiles en diseño.

A su vez esta lista de verificación será tomada como base por la tercera línea de defensa para evaluar la efectividad de los controles en su aplicación por parte de la primera línea de defensa.

A continuación, se presenta el instrumento de validación establecido como lista de verificación de validación de controles en el diseño.

Tabla 9. Tabla Evaluación Diseño de Controles

Atributo	Tipo / característica	Descripción	Peso
Eficiencia	Preventivo	Atacan las causas, disminuye la probabilidad de materialización del riesgo	25%
Eficiencia	Detectivo	Detecta una posible materialización antes d que esta ocurra y devuelve el proceso, disminuye probabilidad	15%
Eficiencia	Correctivo	Permiten disminuir el impacto generado por la materialización de un riesgo	10%

Atributo	Tipo / característica	Descripción	Peso
Eficiencia	Automático	El control se aplica mediante un aplicativo o un sistema de información de manera automática.	25%
Eficiencia	Manual	Estas actividades de control son ejecutadas directamente por los servidores de la entidad. Por lo cual tiene implícito el error humano	15%
Informativo	Documentado	Las actividades de control están documentadas en procedimientos, manuales o cualquier otro documento propio del proceso	No aplica
Informativo	Sin Documentar	Las actividades de control se ejecutan, pero no están documentadas en ningún documento del proceso	No aplica
Informativo	Frecuencia Aleatoria	El control se aplica de manera aleatoria en la actividad que genera el riesgo	No aplica
Informativo	Frecuencia Continua	El control se aplica siempre que se ejecuta la actividad	No aplica
Informativo	Evidencia con registro	El control deja un registro que permite evidenciar su ejecución	No aplica
Informativo	Sin registro de evidencia	El control no deja registro de su ejecución	No aplica

Nota: Los atributos informativos le dan formalidad al control y permiten un mejor conocimiento del mismo, pero no influyen de manera directa en su efectividad.

Ejemplo 1 Evaluación de Controles en el Diseño (Control Preventivo)

Control	Atributo	Característica	Peso
El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son	**Propósito**	**Preventivo**	**25%**
	Implementación	**Manual**	**15%**
	Documentación	**Documentado**	**NA**
	Frecuencia	**Continua**	**NA**

registrados en el sistema de información de contratación.	**Evidencia**	**Con Registro**	**NA**
Total, Valoración del Control			**40%**

Ejemplo 2 Evaluación de Controles en el Diseño (Control Detectivo)

Control	Atributo	Característica	Peso
El jefe de Contratos, verifica en el sistema de información de contratación la información registrada por el profesional asignado, y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias devuelve el proceso al profesional de contratos asignado.	**Propósito**	**Detectivo**	**15%**
	Implementación	**Manual**	**15%**
	Documentación	**Documentado**	**NA**
	Frecuencia	**Continua**	**NA**
	Evidencia	**Con Registro**	**NA**
Total, Valoración del Control			**30%**

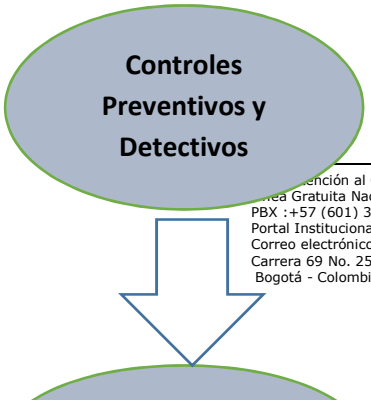
9.4.4 Desplazamiento del Riesgo en el Mapa de Calor como Resultado de la Aplicación de Controles

El peso **(%)** resultante de la evaluación del control en su diseño, es el que permitirá el desplazamiento del riesgo en el mapa de calor de las zonas de mayor severidad a zonas de calor menos severas de acuerdo con los criterios de evaluación del riesgo de la SSF.

El máximo peso que puede alcanzar un control es del **50%** cuando se trata de un control de tipo preventivo y este se ejecuta de manera automática.

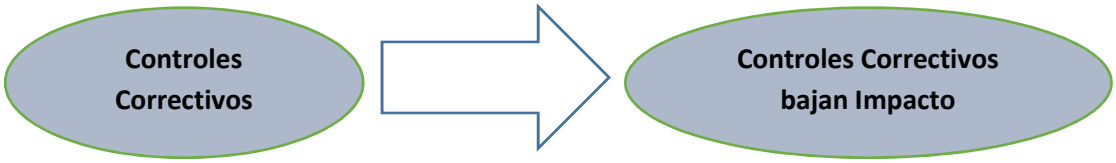
Los desplazamientos de los riesgos en función de los controles se presentan a continuación:

FIGURA1 DESPLAZAMIENTO ZONAS DE CALOR MAPA DE RIESGOS DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN



IMPACTO				
Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

PROBABILIDAD	Muy baja 20 %					
	Baja 40%					
	Media 60%					
	Alta 80%					
	Muy Alta 100%					



9.4.5 Nivel de Riesgo Residual

Es el nivel de riesgo resultante después de la aplicación de controles una vez se evalúan los mismos con base en los atributos de eficiencia para cada control.

A partir de la evaluación de los controles preventivos y detectivos se disminuye la probabilidad del riesgo y a partir de los controles correctivos se disminuye su impacto.

Para la evaluación de los controles es importante tener en cuenta que los mismos mitigan los riesgos de manera acumulativa.

El nivel de riesgo residual resulta de restar el resultado de evaluación de los controles del nivel de riesgo inherente.

La fórmula para el cálculo del riesgo residual es la siguiente:

R residual = R Inherente - (R Inherente * control)

A continuación, se presenta un ejemplo de aplicación de la evaluación de los controles y de desplazamiento del riesgo inherente al riesgo residual en el mapa de calor.

Ejemplo aplicación evaluación de controles

Riesgo	Nivel de Probabilidad Inherente	Nivel de Impacto Inherenmte	Nivel de Severidad del Riesgo Inherente
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	60%	80%	ALTO
Control 1	Preventivo	Detectivo	Correctivo
El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	25%		
	Automático	Manual	
		15%	
Evaluación del Control 1	40%		
Control 2	Preventivo	Detectivo	Correctivo
El jefe de Contratos, verifica en el sistema de información de contratación la información registrada por el profesional asignado, y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias devuelve el proceso al profesional de contratos asignado.		15%	
	Automático	Manual	
		15%	
Evaluación del Control 2	30%		
Riesgo	Nivel de Probabilidad Residual	Nivel de Impacto Residual	Nivel de Severidad del Riesgo Inherente
Eficiencia del Control 1	24%	0%	
Evaluación del Riesgo Residual con control 1	36%	80%	ALTO
Eficiencia del Control 2	10,80%	0%	
Evaluación del Riesgo Residual con control 2	25,2%	80%	ALTO

Ejemplo desplazamiento del riesgo en el mapa de calor ejemplo

IMPACTO

		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
PROBABILIDAD	Muy baja 20 %					
	Baja 40%				Riesgo Residual	
	Media 60%				Riesgo Inherente	
	Alta 80%					
	Muy Alta 100%					

Para este ejemplo, si bien el riesgo permanece en la zona de riesgo Alto, a partir de los controles se disminuyó la probabilidad de ocurrencia del mismo de un 60% a un 25,2%.

9.5 Tratamiento del Riesgo

Es la respuesta establecida por la primera línea de defensa **(ver Política Integral de Administración del Riesgo)** para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

Esta respuesta corresponde a la decisión que se toma frente a un determinado nivel de riesgo. El análisis para la toma de las decisiones se realiza tomando como base el nivel de riesgo residual a excepción de cuando el análisis se realiza sobre procesos nuevos, frente a lo cual el análisis se realiza con base en el nivel de riesgo inherente.

Los criterios de tratamiento del riesgo están enmarcados en las directrices definidas de Apetito al Riesgo, Tolerancia al Riesgo y Capacidad del Riesgo, establecidas en la **Política Integral de Administración del Riesgo de la SSF**.

9.5.1 Tipos de Tratamiento al Riesgo

Los tratamientos en la SSF pueden ser de diferentes tipos de acuerdo con su finalidad:

Aceptar el Riesgo: Bajo decisión informada y después de realizar el análisis del riesgo el responsable del proceso decide no intervenir el riesgo, aun cuando el riesgo supere los niveles de apetito y tolerancia al riesgo definidos en la **Política Integral de Administración del Riesgo,** asumiendo los posibles efectos en caso de que el riesgo se materialice. Esta decisión debe quedar registrada en el mapa de riesgos de la entidad. Para el caso de los riesgos estratégicos esta decisión debe ser tomada por el Comité Institucional de Gestión y Desempeño.

Reducir el riesgo: Después de realizar el análisis del riesgo considerando los niveles de apetito y tolerancia al riesgo para la SSF, el responsable del proceso puede adoptar dos medidas para reducir el nivel del riesgo mediante acciones para mitigar o transferir el riesgo de la siguiente manera:

Mitigar el riesgo: Consiste en tomar acciones para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general, aunque no necesariamente conlleva a la implementación de controles**.**

Compartir el riesgo: Consiste en reducir la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Puede darse a través del establecimiento de pólizas o subcontratación

Evitar el riesgo: Como resultado del análisis del riesgo por parte del responsable del proceso se decide abandonar la actividad generadora del riesgo, considerando los efectos potenciales de la materialización del mismo, así como los efectos de no continuar realizando la actividad generadora. Esta decisión debe quedar registrada en el mapa de riesgos de la entidad.

9.5.2 Plan de Tratamiento al Riesgo:

Para los tratamientos relacionados con reducir el riesgo se debe establecer un plan de acción en dónde se especifiquen las acciones a realizar, el responsable, fecha de implementación y fecha de seguimiento.

9.6 Gestión de Eventos de Riesgo.

Un evento de riesgo corresponde a un riesgo materializado. Con el objetivo de tener una base histórica de eventos, la Entidad debe registrar los posibles eventos de riesgo en donde se plasman las situaciones o incidentes que se han presentado y que generan o pueden generar pérdidas económicas o afectaciones a la reputación de la entidad. Se debe establecer si la situación presentada realmente corresponde a un riesgo materializado y de ser así se deben establecer las posibles fallas en los controles. En caso de que la situación presentada no tenga asociado un riesgo previamente identificado en el mapa de riesgos de la entidad, se debe proceder a su identificación y análisis en el mapa de riesgos de la entidad.

El registro de eventos de riesgos se debe realizar en el formato establecido para tal fin en la SSF por la Oficina Asesora de Planeación.

El registro de eventos de riesgos debe ser realizado por el responsable del proceso donde se presenta la situación y en caso de determinarse que se trata de una

materialización de un riesgo, debe reportarse la Oficina de Control Interno para su seguimiento.

Algunas fuentes para identificar posibles eventos de riesgos son:

- Las PQRS
- Mesas de Ayuda.
- Resultados de auditorías internas y externas.
- Seguimiento a planes, procesos y proyectos.
- Oficina Jurídica
- Líneas internas de denuncia.

9.7 Monitoreo y Revisión del Riesgo

La Entidad debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad. De acuerdo con lo establecido en el Manual Operativo versión 4 del modelo integrado de plantación y gestión (MIPG) en la dimensión 7 “Control interno” y en alienación con lo definido en la **Política Integral de Administración del Riesgo de la SSF** la responsabilidad y los roles frente a la gestión del riesgo y control que incluyen la realización de las actividades de monitoreo y seguimiento a la efectividad de la gestión del riesgo.

9.7.1 Responsabilidades de las Líneas de Defensa Frente al Monitoreo y Revisión del Riesgo

9.7.1.1 *Responsabilidades de la Línea Estratégica*

Conformada por la Alta Dirección, Comité Institucional de Coordinación de Control Interno y Comité Institucional de Gestión y Desempeño

- A través del Comité Institucional de Coordinación de Control Interno definir y evaluar la Política Integral de Administración del Riesgo.
- Revisar cambios en el entorno y riesgos emergentes que deban ser considerados para definir ajustes en la Política Integral de Administración del Riesgo de la SSF.
- Identificar posibles dificultades para el desarrollo de la Política Integral de Administración del Riesgo de la SSF.
- Analizar la gestión del riesgo y aplicar mejoras a través del Comité Institucional de Gestión y Desempeño.

9.7.1.2 *Responsabilidades de la Primera Línea de Defensa*

Conformada por los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad

- Identificar y evaluar los riesgos que puedan afectar el logro de los objetivos de los procesos, planes o proyectos bajo su responsabilidad.
- Diseñar e implementar los controles para prevenir y mitigar los riesgos identificados para evitar su materialización
- Realizar el seguimiento los riesgos de acuerdo con el diseño de los controles para prevenir y mitigar los riesgos.

9.7.1.3 *Responsabilidades de la Segunda Línea de Defensa*

Conformada por servidores que ocupan cargos del nivel directivo o asesor, quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección. En la SSF la segunda línea de defensa la conforman la Oficina Asesora de Planeación, Oficina de las Tecnologías de la Información y las Comunicaciones, Grupo de Gestión Contractual, Oficina de Protección al Usuario, Grupo de Gestión Administrativa y Grupo de Gestión del Talento Humano

- Asegurar que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente.
- Supervisar la eficacia e implementación de las prácticas de gestión de riesgo.
- Consolidar y analizar la información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.
- Establecer los mecanismos para la autoevaluación requerida (auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora)

9.7.1.4 *Responsabilidades de la Tercera Línea de Defensa:*

Conformada por la Oficina de Control Interno

- Proporcionar aseguramiento independiente y objetivo sobre la efectividad del Sistema de Control Interno
- A través de su rol de asesoría brindar orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación para garantizar el cumplimento efectivo de los objetivos.
- Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.

9.7.2 Frecuencia para la Revisión y Monitoreo a la Gestión del Riesgo

El **monitoreo a los riesgos** es un ejercicio **continuo** que se realiza por parte de la primera línea de defensa verificando la aplicación de los controles y las posibles materializaciones de los riesgos. El **monitoreo a la gestión del riesgo** es un ejercicio que se realiza por parte de la segunda línea de defensa a través de la consolidación de la información plasmada en las matrices de riesgos de la entidad, así como en el **reporte de seguimiento a los riesgos** de acuerdo con la frecuencia establecida en la **Política Integral de Administración del Riesgo de la SSF.**

La **revisión** de los riesgos es un ejercicio en donde se establece si en el periodo de análisis se han presentado cambios en los riesgos existentes o si presentan riesgos emergentes que es necesario identificar en la matriz de riesgos, este ejercicio se realiza **como mínimo una vez al año o cada vez que se presenten cambios en el contexto** que puedan afectar el logro de los objetivos de la entidad o del proceso, la revisión de los riesgos la debe realizar la primera línea de defensa y con el acompañamiento de la Oficina Asesora de Planeación.

9.7.3 Indicadores de Gestión del Riesgo

Los Indicadores de Gestión del Riesgo es una herramienta que permite a la SSF obtener información sobre el desempeño de la gestión del riesgo en la entidad a través de la recolección de datos en periodos específicos de tiempo para establecer el comportamiento de los riesgos y el nivel de exposición de la entidad frente a los diferentes riesgos.

Los indicadores definidos para realizar seguimiento a la gestión del riesgo en la SSF son

9.7.3.1 *Cobertura de Gestión del Riesgo*

Este indicador se establece con base en los objetivos de la entidad en sus diferentes niveles (planes, procesos, programas y proyectos), en donde cada objetivo debe tener al menos un riesgo asociado, asegurando que no queden objetivos descubiertos de la gestión del riesgo.

La fórmula para este indicador es:

ICR = NORI / NOE* 100, en donde

ICR: Índice de Cobertura de Riesgos

NORI: Numero de Objetivos con Riesgos Identificados

NOE: Numero de Objetivos Establecidos

La tendencia del indicador debe ser al 100%

La frecuencia de medición del indicador es trimestral.

9.7.3.2 *Efectividad de los Controles de Riesgos de Gestión*

Este indicador permite establecer la efectividad de los controles para prevenir la materialización de los riesgos a través del registro del número de materializaciones de riesgos durante el periodo de evaluación.

La fórmula para este indicador es

IECR = 1- ((NRM / NRI)*100) en donde

IERC: Índice de Efectividad de los Controles de los Riesgos

NRM: Numero de Riesgos Materializados

NRI: Numero de Riesgos Identificados

La tendencia del indicador debe ser al 100%

La frecuencia de medición del indicador es trimestral.

10 MAPA DE RIESGOS DE LA ENTIDAD

La Oficina Asesora de Planeación es la encargada de determinar el formato del mapa de riesgos de la entidad. El formato establecido debe cumplir con la metodología definida en este manual y con la estructura propuesta para el mismo en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5.

La matriz de riesgos de la entidad puede estructurarse en la herramienta tipo aplicativo que la entidad determine para tal fin.

El mapa de riesgos de la SSF debe estar publicado en su versión vigente en el portal corporativo de la entidad, para consulta de sus grupos de interés.

El diligenciamiento del mapa de riesgos de la entidad, se debe realizar con el acompañamiento de la Oficina Asesora de Planeación dentro de su rol como segunda línea de defensa de acuerdo con lo establecido en **la Política Integral de Administración del Riesgo de la Entidad.**