SuperSubsidio
Vigilamos tu caja de compensación

MANUAL INSTITUCIONAL DE GESTIÓN INTEGRAL DE RIESGO 2020

Oficina Asesora de Planeación

Edificio World Business Port
Carrera 69 # 25 B - 44 Pisos 3, 4 y 7

Teléfonos: 3487777 - PBX: 3487800
www.ssf.gov.co - e-mail: ssf@ssf.gov.co
Bogotá D.C, Colombia

1. INTRODUCCIÓN

Para la Superintendencia del Subsidio Familiar es de primordial importancia asegurar razonablemente el logro de los objetivos estratégicos, así como el de los objetivos de los procesos 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 con controles efectivos los riesgos de gestión, corrupción y de seguridad de la información.

Lo anterior enmarcado en los lineamientos que establece el Departamento Administrativo de la Función Pública a través de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas versión 4 y en respuesta a lo que en materia de gestión del riesgo dispone el Modelo Integral de Planeación y Gestión en su manual operativo versión 3. A su vez la metodología desarrollada por la entidad toma como base técnica las directrices para la gestión del riesgo de la norma ISO 31000 versión 2018.

El Manual Integral de Administración del Riesgo de la SSF tiene como propósito presentar la metodología que la entidad aplica para reconocer y gestionar los riesgos que pueden impedir o dificultar el logro de sus objetivos estratégicos y los de sus procesos, los riesgos de corrupción y los riesgos de seguridad de seguridad de la información.

2. GLOSARIO

A continuación, se presentan los términos y definiciones más relevantes frente a la gestión integral del riesgo.

Activo: Elemento que tenga valor para la organización.

Activo de información: Activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos del negocio, servicio y soporte.

Análisis del riesgo inherente: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo, sin considerar los controles existentes.

Análisis del riesgo residual: Corresponde al nivel de riesgo que permanece después de haber identificado y evaluado la eficacia de los controles para mitigar los riesgos.

Causa: Medios, circunstancias o motivos que originan el riesgo y permiten su posible materialización.

Beneficio: Impacto positivo generado por el aprovechamiento de una oportunidad y que puede afectar el logro de los resultados previstos.

Confidencialidad de la información: hace referencia a la 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.

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 o mecanismo que busca disminuir o mitigar el nivel de riesgo, actuando sobre las causas o sobre las consecuencias.

Consecuencia o impacto: Efecto negativo generado por la materialización de un riesgo y que puede afectar los resultados previstos.

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

Disponibilidad de la información: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Evaluación del riesgo: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo para determinar si el riesgo se asume o se trata a través de una acción preventiva.

Factor del contexto: Subcategoría del contexto sobre la que se analizan los aspectos específicos que dificultan o facilitan el logro de los objetivos de la Entidad.

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

Identificación del riesgo: Proceso sistemático para encontrar, reconocer y describir los riesgos surgidos del contexto que pueden dificultar u obstaculizar el logro de los resultados previstos.

Identificación de la oportunidad: Proceso sistemático para encontrar, reconocer y describir las oportunidades surgidas del contexto que pueden facilitar o potenciar el logro de los resultados previstos.

Integridad de la Información: Mantenimiento de la exactitud y completitud de la información y los métodos de proceso.

Gestión del riesgo de corrupción: Conjunto de actividades coordinadas para dirigir y controlar la Entidad en lo relacionado al riesgo de corrupción.

Matriz de riesgos: Herramienta que permite visualizar cuáles son los riesgos y oportunidades 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: Magnitud de un riesgo, expresada en términos de la combinación de las consecuencias y su probabilidad.

Nivel de aceptación del riesgo: Nivel de riesgo que la entidad está dispuesta a aceptar en la búsqueda de la misión, visión y objetivos.

Nivel de tolerancia al riesgo: Variación con respeto al nivel de aceptación del riesgo definido por la entidad. Es la cantidad máxima de riesgo que la entidad está dispuesta a aceptar para logar su objetivo.

Oportunidad: efecto de la incertidumbre sobre los objetivos, entendido como la posibilidad de que suceda algún evento que tendrá un impacto positivo sobre los objetivos de la Entidad, de un subsistema o de un proceso

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: Medida para estimar el grado de exposición a un riesgo. Se mide según la frecuencia (número de veces en que se ha presentado el riesgo en un período determinado) o por la factibilidad (factores internos o externos que pueden facilitar que el riesgo se presente).

Riesgo: Efecto de la incertidumbre sobre los objetivos, entendido como la posibilidad de que suceda algún evento que tendrá un impacto negativo sobre los objetivos de la entidad, de un subsistema o de un proceso.

Riesgo inherente: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

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 Eficaces Versión 4, la NTC ISO 31000 versión 2018.

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.

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, de corrupción y de seguridad de la información en todas las etapas a partir del análisis y monitoreo 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.

5. ALCANCE

Las directrices establecidas en el presente manual son de obligatoria aplicación para todos los riesgos que aborda la entidad en todos los procesos y en todos los niveles, desde el análisis del contexto interno y externo, hasta la identificación, evaluación, tratamiento, monitoreo y reporte del seguimiento a los mapas de riesgos. Así mismo esta metodología aplica para la administración de los riesgos en el sistema de gestión de

calidad, el sistema de gestión de seguridad y salud en el trabajo, el sistema de gestión de seguridad de la información, los riesgos ambientales y los riesgos de la gestión documental.

6. ARTICULACIÓN DE LA GESTIÓ 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 4 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. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas*, 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 4 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. RESPONSABILIDAD FRENTE A LA GESTIÓN DEL RIESGO DE ACUERDO CON EL ESQUEMA DE LÍNEAS DE DEFENSA

El Modelo Integrado de Planeación y Gestión (MIPG) a través del Modelo Estándar de Control Interno (MECI) establece una estructura de control para la gestión institucional que determina los parámetros necesarios para la autogestión, la autorregulación y el autocontrol. Uno de los elementos fundamentales de esta estructura es el esquema de responsabilidades integrado por cuatro líneas de defensa el cual proporciona una manera efectiva para mejorar las comunicaciones en la gestión de los riesgos y los controles mediante la aclaración de las funciones y deberes relacionados.

En la siguiente tabla se explica la aplicación de los roles y responsabilidades del esquema de líneas de defensa para la Superintendencia del Subsidio Familiar.

Tabla 1. Responsabilidades de las líneas de defensa en la SSF.

LINEA DE DEFENSA	RESPONSABLE EN SSF	RESPONSABILIDAD FRENTE A LA GESTIÓN DEL RIESGO
LÍNEA ESTRATÉGICA	• La Alta Dirección de la SSF (El Superintendente del Subsidio Familiar y su Equipo Directivo) • El Comité Institucional de Coordinación de Control Interno	• Analizar los riesgos y amenazas institucionales • Definir, aprobar y evaluar la Política de Administración del Riesgo de la Entidad • Fortalecer el Comité Institucional de Coordinación de Control Interno incrementando la periodicidad de las reuniones • Definir las líneas de reporte en temas claves para la toma de decisiones.
PRIMERA LÍNEA DE DEFENSA	• Lideres de procesos, programas y proyectos y sus equipos • Los servidores públicos de todos los niveles de la SSF	• Identificar, evaluar, controlar y mitigar los riesgos a través del autocontrol • Mantener efectivamente los controles internos y los controles del dia a dia • Conocer y apropiar las políticas, procedimientos, manuales , protocolos entre otras herramientas para el autocontrol en los puestos de trabajo

LINEA DE DEFENSA	RESPONSABLE EN SSF	RESPONSABILIDAD FRENTE A LA GESTIÓN DEL RIESGO
		• Identificar los riesgos de los procesos, programas y proyectos a su cargo , establecer los controles , hacer el seguimiento acorde con el diseño de los controles para evitar su materialización • Informar las materializaciones de los riesgos a la Oficina Asesora de Planeación (segunda línea de defensa) y a la Oficina de Control Interno (tercera línea de defensa)
SEGUNDA LÍNEA DE DEFENSA	• Jefe de la Oficina Asesora de Planeación • Comité de contratación • Jefe de la Oficina de las Tecnologías de la Información y la Comunicación • Responsable de temas transversales para toda la entidad y que reporta ante el Representante Legal	• Asegurar que los controles y procesos de gestión del riesgo de la primera línea de defensa sean aropiados funcionen correctamente • Supervisar la implementación de practicas eficaces para la gestión de los riesgos y para el diseño e implementación de controles • Evaluar y efectuar seguimiento a los controles aplicados por la 1ª línea de defensa. • Realizar asesoría a la 1ª línea de defensa en la identificación de riesgos , el establecimiento de controles efectivos y la implementación de planes de tratamiento a los riesgos • Establecer los mecanismos para la autoevaluación sobre la gestión de los riesgos (seguimiento a través de herramientas objetivas, consolidación de informes de gestión).
TERCERA LÍNEA DE DEFENSA	• Jefe de la Oficina de Control Interno	• Monitorear y revisar de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos • A través de su rol de asesoría, realizar orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación. • Realizar monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo • Realizar asesoría proactiva y estratégica a la Alta Dirección y a los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. • Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. • Informar los hallazgos sobre la gestión de riesgo y proporcionar recomendaciones de forma independiente.

8. DECLARACIÓN DE LA POLÍTICA INTEGRAL DE ADMINISTRACIÓN DEL RIESGO

"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, 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"

9. NIVELES DE ACEPTACIÓN Y TOLERANCIA DEL RIESGO

9.1 Nivel de Aceptación del Riesgo

El nivel de aceptación al riesgo es definido como el nivel de riesgo que la Entidad está dispuesta a asumir sin necesidad de establecer controles adicionales tendientes a disminuir su probabilidad o su impacto. Para el caso de la Superintendencia del Subsidio Familiar de acuerdo con su contexto, su misionalidad y la naturaleza de los procesos que desarrolla ha definido el nivel de aceptación del riesgo de acuerdo con los siguientes criterios.

En la siguiente tabla se presentan los niveles de riesgo y los criterios de decisión para la aceptación de los riesgos de acuerdo con su nivel

Tabla 2. Niveles de Riesgo y Criterios de Decisión

CONVENCIÓN	NIVEL DE RIESGO INHERENTE	CRITERIOS DE DECISIÓN DE ACEPTACIÓN DEL RIESGO	MÉTRICA	FRECUENCIA DE MONITOREO
	Riesgo Extremo	El riesgo en este nivel no se acepta. Bajo ninguna circunstancia la entidad deberá mantener un riesgo con esa capacidad potencial de afectar el logro de los objetivos. Deben establecerse medidas de intervención inmediatas para disminuir su calificación	Nivel de Riesgo entre 15 y 25	Bimestral
	Riesgo Alto	El riesgo en este nivel no se acepta. Es necesario que la entidad desarrolle acciones prioritarias a corto plazo para su mitigación, debido al alto impacto que tendría su	Nivel de Riesgo entre 8 y 12	Bimestral

CONVENCIÓN	NIVEL DE RIESGO INHERENTE	CRITERIOS DE DECISIÓN DE ACEPTACIÓN DEL RIESGO	MÉTRICA	FRECUENCIA DE MONITOREO
		materialización sobre el logro de los objetivos		
	Riesgo Moderado	El riesgo en este nivel no se acepta. Es necesario desarrollar medidas de intervención sobre el riesgo con prioridad de segundo nivel para disminuir su calificación a una zona asumible	Nivel de Riesgo entre 4 y 6 Nivel de riesgo 3 para riesgos de corrupción	Semestral
	Riesgo Bajo	El riesgo en este nivel se acepta. El riesgo no presenta una gravedad significativa, por lo que no amerita la aplicación de acciones adicionales. El riesgo se debe gestionar mediante monitoreo periódico. Ningún riesgo de corrupción puede aceptarse	Nivel de Riesgo entre 1 y 3 para riesgos de gestión y seguridad de la información	Semestral

9.2 Nivel de Tolerancia del Riesgo

Es definido como la variación con respeto al nivel de aceptación del riesgo establecido por la entidad. Es la cantidad máxima de riesgo que la entidad está dispuesta a aceptar para logar su objetivo.

La SSF puede aceptar y mantener un riesgo de gestión, de corrupción o de seguridad de la información en una zona de calificación **MODERADO** después de la aplicación de controles únicamente sí como resultado de un análisis por parte de los responsables del proceso o de la alta dirección, se determina que no es posible establecer medidas adicionales a las ya aplicadas para reducir su nivel a **BAJO** o si la medida para su reducción nos es viable de acuerdo con las capacidades de los recursos de la entidad. En estos casos la decisión frente a la gestión del riesgo se puede establecer como **Mantener el riesgo bajo decisión informada**.

10. TIPOS DE RIESGOS EN LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR

La Guía de Administración del Riesgo y Diseño de Controles para Entidades Públicas versión 4 ha establecido para las entidades públicas tres tipos principales de riesgos: riesgos de gestión, riesgos de corrupción y riesgos de seguridad de la información.

Estos tipos de riesgos se diferencian en función de la manera en la cual deben ser gestionados por la entidad.

A continuación, se definen los tres principales tipos de riesgos:

- **RIESGOS DE GESTIÓN**: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

- **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.

- **RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como 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.

  Dentro de los riesgos de gestión se establecen subtipos de riesgos de acuerdo con su naturaleza que se presentan en la siguiente tabla.

Tabla 3 Subtipos de riesgos de gestión para la SSF

SUBTIPO DE RIESGO	DESCRIPCIÓN
RIESGOS ESTRATÉGICOS	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la SSF.
RIESGOS GERENCIALES	Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección

SUBTIPO DE RIESGO	DESCRIPCIÓN
RIESGOS OPERATIVOS	Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la SSF.
RIESGOS FINANCIEROS	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero.
RIESGOS DE CUMPLIMIENTO	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la SSF debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
RIESGO DE IMAGEN O REPUTACIONAL	Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de la SSF ante sus vigilados o partes interesadas
RIESGOS TECNOLÓGICOS	Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de la SSF.

Fuente Guía para la administración del riesgo y el diseño de controles en entidades públicas V4

11. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

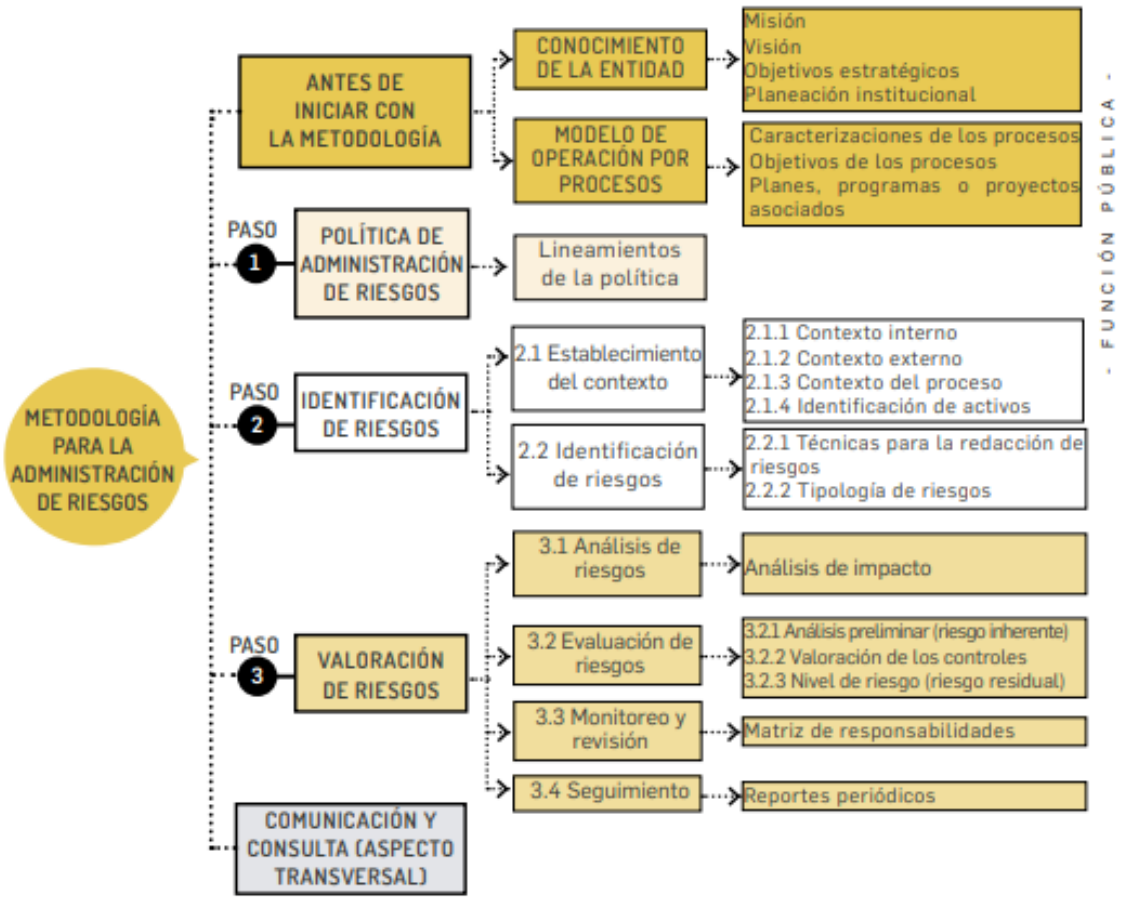
La metodología implementada por la SSF está diseñada para responder a las necesidades particulares de la entidad y se adapta a las características propias de su estructura orgánica, los procesos y la naturaleza de las actividades que desarrolla para cumplir su misión.

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.

Para la gestión del riesgo la entidad cuenta con una herramienta tecnológica que permite el registro de las diferentes etapas de la gestión, facilita la trazabilidad y se convierte en el documento oficial de la entidad pala la consulta, monitoreo y seguimiento a la gestión del riesgo. La herramienta es el aplicativo Isolucion, módulo de riesgos DAFP.

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 V4 para la gestión de los riesgos en entidades públicas

Figura 1. Esquema de gestión del riesgo



Tomado Guía para la administración del riesgo y el diseño de controles en entidades públicas V4.

Con base en lo anterior la entidad ha definido su ciclo básico de gestión del riesgo en 6 etapas:

1. Establecimiento del contexto.
2. Identificación del riesgo.
3. Análisis del riesgo.

4. Evaluación del riesgo.
5. Tratamiento del riesgo.
6. Monitoreo y Seguimiento a la gestión del riesgo.

A continuación, se explican cada una de las etapas para la gestión del riesgo en la SSF.

11.1 Análisis del Contexto

11.1.1 Metodología para el Análisis del Contexto

El contexto es el entorno en el cual la entidad planifica y busca alcanzar sus objetivos. La etapa del establecimiento del contexto consiste en analizar el entorno interno y externo para determinar qué factores del mismo pueden llegar a afectar el logro de los objetivos de la entidad y por ende dar origen a riesgos y oportunidades los cuales deben ser identificados y gestionados por la entidad.

Para realizar el análisis del contexto en la SSF es necesario definir dos dimensiones del contexto.

1. El análisis del contexto externo.
2. El análisis del contexto interno.

Para cada dimensión del contexto se definen los factores de mismo que serán considerados como punto de partida al momento de realizar la identificación de los riesgos y las oportunidades que pueden afectar el logro de los objetivos de la SSF.

La siguiente tabla muestra factores a analizar para las dos dimensiones del contexto de la SSF.

Tabla 4 Factores de contexto

DIMENSIÓN	FACTOR	DESCRIPCIÓN
CONTEXTO EXTERNO	**Políticos**	Cambios de gobierno, legislación, políticas públicas, regulación.
	Económicos y financieros	Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	Sociales y culturales	Demografía, responsabilidad social, orden público.
	Tecnológicos	Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.

DIMENSIÓN	FACTOR	DESCRIPCIÓN
	Ambientales	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	Legales y reglamentarios	Normatividad externa (leyes, decretos, ordenanzas y acuerdos).
CONTEXTO INTERNO	**Financieros**	Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	Personal	Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	Procesos	Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	Tecnología	Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	Estratégicos	Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	Comunicación interna	Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
	Activos de información	Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de los procesos.
CONTEXTO DEL PROCESO	**Diseño del proceso**	Claridad en la descripción del alcance y objetivo del proceso.
	Interacciones con otros procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	Transversalidad	Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	Procedimientos asociados	Pertinencia en los procedimientos que desarrollan los procesos.
	Responsables del proceso	Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos.

Fuente Guía para la administración del riesgo y el diseño de controles en entidades públicas V4

La entidad a través de los procesos realizará el análisis de los factores anteriormente descritos periódicamente o cada vez se presente un cambio relevante en el contexto para establecer cuáles de ellos podrían afectar el logro de los objetivos estratégicos, de los procesos o de los planes, programas y proyectos.

Para lo anterior se debe realizar una clasificación **DOFA** para cada uno de los factores de contexto y de cómo se presenta el mismo frente a la entidad o frente al proceso analizado.

La clasificación de los factores se realiza teniendo en cuenta los siguientes parámetros:

- **Debilidad:** Factor interno que es controlado por la entidad, pero por sus características puede generar un riesgo para la entidad.

- **Fortaleza**: Factor interno que es controlado por la entidad y que por sus características puede generar una oportunidad para la entidad o para sus procesos.

- **Amenaza**: Factor externo que es no está bajo el control de la entidad y que por sus características puede generar un riesgo para la entidad o para sus procesos. Para los riesgos de Seguridad de la información el concepto amenaza se asocia al concepto de Amenaza para los activos de la información.

- **Oportunidad:** Factor externo que no está bajo el control de la entidad y que por sus características puede generar una oportunidad para la entidad o para sus procesos.

  Nota: Para los riesgos de Seguridad de la información el concepto debilidad se asocia al concepto de vulnerabilidad de los activos de la información.

A partir del resultado del análisis del contexto interno se pueden identificar Fortalezas y Debilidades y del análisis del contexto externo se identifican Oportunidades y Amenazas. Las Debilidades y Amenazas son fuentes generadoras de riesgos frente a los objetivos y Las Oportunidades y Fortalezas con fuentes generadoras de oportunidades frente al logro de los objetivos.

11.1.2 Frecuencia y Responsabilidad Frente al Análisis del Contexto

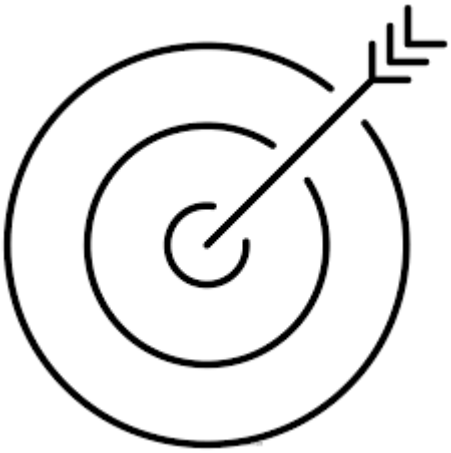
El análisis de contexto se debe realizar con frecuencia anual o en el momento en el que se presente un cambio o situación que pueda afectar el logro de los objetivos de la entidad.

Es responsabilidad de la Alta Dirección (línea estratégica) realizar el análisis de contexto de la entidad y dejar evidencia del mismo.

Es de responsabilidad del Dueño del Proceso (primera línea de defensa) en conjunto con su equipo de trabajo realizar el análisis de contexto de su proceso y dejar evidencia del mismo

11.2 Identificación del Riesgo

11.2.1 Identificación de los Riesgos de Gestión



La identificación de los riesgos de gestión 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.

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.

Al realizar la identificación de los riesgos se debe obtener la siguiente información:

- **RIESGO:** Evento que puede afectar el cumplimiento del objetivo estratégico o del proceso según sea el caso.

- **CAUSAS:** Se establecen los factores que pueden generar la materialización del riesgo. Es importante tener en cuenta que las causas deben ser gestionables a partir del establecimiento de actividades de controles.

- **CONSECUENCUAS:** Se determinan los posibles efectos por la materialización del riesgo. Es importante tener en cuenta que frente a estas consecuencias se determinará posteriormente el nivel de impacto.

Para realizar una mejor identificación de los riesgos, el ejercicio puede apoyarse en las siguientes herramientas técnicas y estadísticas que facilitan el análisis de la información disponible:

- **Lluvia de ideas**: Técnica usada para estimular y fomentar el flujo libre de la conversación entre un grupo de personas con conocimiento. Entre sus múltiples aplicaciones es útil para identificar los riesgos de un proceso o los criterios para las decisiones y/o las opciones de tratamiento. La lluvia de ideas implica tratar de garantizar la estimulación de la imaginación de las personas mediante los pensamientos y las declaraciones de los otros participantes.

- **Técnica Delphi**: Es una técnica para obtener un consenso confiable de la opinión de un grupo de personas expertas en un tema específico, aunque se asocia a la lluvia de ideas, una característica de esta técnica es que los expertos expresan sus opiniones individualmente y de manera anónima al tiempo que tiene acceso a los puntos de vista de otros expertos a medida que el proceso avanza.

- **Análisis de escenarios:** En este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse y con base en estas posibilidades, se determina qué puede llegar a suceder y las consecuencias de la afectación.

- **Entrevistas estructuradas o semiestructuradas**: Son útiles cuando es difícil hacer que las personas se reúnan para una sesión de lluvia de ideas o cuando el flujo libre de una discusión en un grupo no es el adecuado para las situaciones o las personas

implicadas. Estas se pueden aplicar en cualquier etapa la gestión del riesgo. Se crea un conjunto de preguntas pertinentes para guiar al entrevistador, siempre que sea posible las preguntas deberían ser abiertas, sencillas, tener un lenguaje adecuado para los entrevistados y abarcar solamente un aspecto. También se elaboran posibles preguntas de seguimiento para buscar aclaraciones. Se recomienda precaución para no "guiar" al entrevistado. Las respuestas se deberían tomar en consideración con algún grado de flexibilidad con el fin de brindar la oportunidad de explorar las áreas hacia las cuales el entrevistado puede querer dirigirse.

- **Técnica ¿qué pasa sí?:** La técnica es un estudio sistemático, basado en el trabajo de equipo, que utiliza un conjunto de palabras o frases de "indicación" que el facilitador utiliza frente a un taller para estimular a los participantes a que identifiquen los riesgos. El facilitador y el equipo utilizan frases normales del tipo "que pasaría si" en combinación con las indicaciones para investigar como un proceso, un servicio o una actividad se verán afectados por las desviaciones con respecto al comportamiento de las operaciones normales.

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

A continuación, se presenta un ejemplo de identificación de un riesgo de gestión

EJEMPLO DE RIESGO DE GESTIÓN				
RIESGO	**DESCRIPCIÓN**	**TIPO**	**CAUSAS**	**CONSECUENCIAS**
Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	La combinación de factores como insuficiente capacitación del personal de contratos, cambios en la regulación contractual, inadecuadas políticas de operación y carencia de controles en el procedimiento de contratación pueden ocasionar inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad y, en consecuencia, afectar la continuidad de su operación.	Riesgo de Gestión / Operativo	Carencia de controles en el procedimiento de contratación Insuficiente capacitación del personal de contratos Desconocimiento de los cambios en la regulación contractual Inadecuadas políticas de operación	Parálisis en los Procesos Incumplimiento en la entrega de bienes y servicios a los grupos de valor Demandas y demás acciones jurídicas Detrimento de la imagen de la entidad ante sus grupos de valor Investigaciones disciplinarias

11.2.2 Identificación de los 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. A continuación, se presenta el esquema guía de validación de riesgos de corrupción.

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.

A continuación, se presenta un ejemplo de identificación de riesgos de corrupción

EJEMPLO DE RIESGO DE CORRUPCIÓN				
RIESGO	**DESCRIPCIÓN**	**TIPO**	**CAUSAS**	**CONSECUENCIAS**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin celebrar un contrato.	Situaciones como: debilidades en la etapa de la planeación del contrato, la excesiva discrecionalidad, las presiones indebidas, la carencia de controles, la falta de conocimiento y/o experiencia, sumados a la falta de integridad pueden generar un riesgo de corrupción en la contratación, como por ejemplo "exigencias de condiciones en los procesos de selección que solo cumple un determinado proponente".	Riesgo de Corrupción	Debilidades en la etapa de planeación, que faciliten la inclusión en los estudios previos, y/o en los pliegos de condiciones de requisitos orientados a favorecer a un proponente. Presiones indebidas. Carencia de controles en el procedimiento de contratación. Falta de conocimiento y/o experiencia del personal que maneja la contratación Excesiva discrecionalidad. Adendas que modifican las condiciones generales del proceso de contratación para favorecer a un proponente.	Pérdida de la imagen institucional. Demandas contra el Estado. Pérdida de confianza en lo público. Investigaciones penales, disciplinarias y fiscales. Detrimento patrimonial. Obras inconclusas. Mala calidad de las obras. Enriquecimiento ilícito de contratistas y/o servidores públicos.

11.2.3 Identificación de los Riesgos de Seguridad de la Información

11.2.3.1 Identificación y Valoración de Activos de Información

Para realizar la identificación de los riesgos de seguridad de la información es necesario primero realizar la identificación de los activos de seguridad digital entendiendo por estos los elementos que utiliza la entidad para funcionar en el entorno 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 establecer su criticidad y se establecen los controles adecuados para su protección.

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

a. Pérdida de la Confidencialidad
b. Pérdida de la Integridad
c. Pérdida 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.

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 informaciónl, siendo un ejercicio orientado por el responsable de seguridad de la información de la entidad pública y 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 5. 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

11.2.3.2 Identificación de Amenazas de Seguridad de la Información

Las amenazas, se definen como situaciones o fuentes que pueden generar daños a los activos y materializar los riesgos de Seguridad de la Información. Las amenazas se clasifican en:

I. **Deliberadas (D):** En donde existe la intención de generar daño, por ejemplo, piratería, falsificación de credenciales, hurto de información.

II. **Fortuitas (F):** Las cuales pueden presentarse por efecto de errores involuntarios.

III. **Ambientales (A):** Las cuales se pueden presentar como efecto eventos naturales o como efecto colateral de otro evento.

Tabla 6. Amenazas comunes en seguridad de la información

TIPO	AMENAZA	ORIGEN
DAÑO FÍSICO	Fuego	F, D, A
	Agua	F, D, A
EVENTOS NATURALES	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fallas en el sistema de suministro de agua	E

TIPO	AMENAZA	ORIGEN
PÉRDIDAS DE LOS SERVICIOS ESENCIALES	Fallas en el suministro de aire acondicionado	F, D, A
PERTURBACIÓN DEBIDA A LA RADIACIÓN	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
COMPROMISO DE LA INFORMACIÓN	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
FALLAS TÉCNICAS	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
ACCIONES NO AUTORIZADAS	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
COMPROMISO DE LAS FUNCIONES	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

11.2.3.2.1 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 7. 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

TIPO	VULNERABILIDADES
SOFTWARE	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	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 8. 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.	Riesgo de Seguridad de la Información	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 criterios 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.

11.3 Análisis 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.

11.3.1 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.

La probabilidad puede ser entendida también como la frecuencia con la que el riesgo se puede materializarse en términos de frecuencia y factibilidad.

- **Frecuencia:** se analizan el número de eventos en un periodo determinado, en cuyo caso se analizan los históricos de eventos asociados al riesgo.
- **Factibilidad:** se analiza la presencia de factores internos y externos que pueden propiciar el riesgo que no se ha materializado y que se pueda pronosticar su materialización.

Este ejercicio debe ser participativo e incluir el juicio experto de los colaboradores que más conocen el proceso en donde se está llevando a cabo este análisis. Una deficiente o subjetiva determinación de los niveles de probabilidad o de impacto deriva en una ineficaz gestión de los riesgos.

Nota: La determinación de la Probabilidad aplica de la misma manera para los 3 tipos de Riesgos, de gestión, corrupción y de seguridad de la información**.**

Los criterios para calificar el nivel de probabilidad de cada riesgo se muestran en la siguiente tabla

Tabla 9. Criterios para Calificar Nivel de Probabilidad del Riesgo Inherente

NIVEL	CRITERIO	DESCRIPCIÓN	MÉTRICA
1	RARA VEZ	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos (5) cinco años
2	IMPROBABLE	El evento puede ocurrir en algún momento	Al menos (1) una vez en los últimos (5) cinco años
3	POSIBLE	Se espera que el evento ocurra en algún momento	Al menos (1) una vez en los últimos (2) dos años
4	PROBABLE	Es posible que el evento ocurra en varias oportunidades	Al menos (1) una vez en el último año
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias.	Mas de una vez en el año

11.3.2 Determinación del Nivel de Impacto

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 relacionados para cada riesgo en la etapa de identificación para que con base en ellas se establezca el nivel de afectación que representa la materialización del riesgo para la Entidad.

En la calificación del impacto no se consideran las medidas de mitigación existentes como por ejemplo planes de contingencia o pólizas de seguros, ya que lo que se establece en esta etapa es el riesgo inherente (Sin aplicación de controles)

Los efectos de la materialización de un riesgo se puede presentar en diferentes áreas de impacto de la entidad y afectarlas de manera diferente. Por lo anterior y para facilitar este ejercicio se presenta en la siguiente lista de posibles áreas de impacto.

Tabla 10. Impactos o Consecuencias comunes

NO	IMPACTO O CONSECUENCIA (En Caso de que el riesgo se materialice podría…)
1	Generar reprocesos
2	Afectar las salidas de los procesos
3	Afectar el cumplimiento de objetivos y metas institucionales
4	Impactar el cumplimiento de los objetivos de los procesos
5	Afectar la imagen de la entidad
6	Afectar el presupuesto de la entidad
7	Afectar la prestación de los servicios
8	Generar incumplimiento legal o regulatorio
9	Generar incumplimiento contractual
10	Dar origen a PQRS
11	Afectar el nivel de satisfacción del cliente
12	Incrementar la significancia de los impactos ambientales
13	Generar afectación a la seguridad y salud de los trabajadores
14	Generar perdida o daño en la información crítica de la entidad
15	Generar interrupción de la operación o de la prestación de los servicios de la entidad

Para determinar el nivel de impacto del riesgo se realiza la calificación de acuerdo con los criterios establecidos en la siguiente tabla:

Tabla 11. Criterios para determinar el Nivel de Impacto de los Riesgos de Gestión y Corrupción

NIVEL	CRITERIO	DESCRIPCIÓN	MÉTRICA
1	INSIGNIFICANTE	El impacto generado por la materialización del riesgo no afecta el logro de los objetivos institucionales, pero puede afectar levemente el logro de los objetivos de los procesos, programas o proyectos que desarrolla la entidad	Afectación menor al 5% de un objetivo de proceso, programa o proyecto
2	MENOR	El impacto generado por la materialización del riesgo no afecta el logro de los objetivos institucionales, pero puede afectar de manera moderada el logro de los objetivos de los procesos, programas o proyectos que desarrolla la entidad	Afectación menor al 10% de un objetivo de proceso, programa o proyecto proceso, programa o proyecto

NIVEL	CRITERIO	DESCRIPCIÓN	MÉTRICA
3	MODERADO	El impacto generado por la materialización del riesgo puede afectar levemente el logro de los objetivos institucionales o puede afectar de manera significativa el logro de los objetivos de los procesos, programas o proyectos que desarrolla la entidad	Afectación menor al 2% de un objetivo institucional, Afectación menor al 20% de un objetivo de proceso, programa o proyecto
4	MAYOR	El impacto generado por la materialización del riesgo puede afectar de manera significativa el logro de los objetivos institucionales o puede afectar de manera muy significativa el logro de los objetivos de los procesos, programas o proyectos que desarrolla la entidad	Afectación menor al 10% de un objetivo institucional, Afectación menor al 50% de un objetivo de proceso, programa o proyecto
5	CATASTRÓFICO	El impacto generado por la materialización del riesgo puede afectar de manera mayor o total el logro de los objetivos institucionales o puede impedir el logro de los objetivos de los procesos, programas o proyectos que desarrolla la entidad	Afectación mayor al 10% de un objetivo institucional, Afectación mayor al 50% de un objetivo de proceso, programa o proyecto

Tabla 14. Criterios para determinar el Nivel de Impacto de los Riesgos de Seguridad de la Información

NIVEL	CRITERIO	CRITERIOS DE IMPACTO (Seguridad de la Información)	
		IMPACTO CUANTITATIVO	IMPACTO CUALITATIVO
1	INSIGNIFICANTE	Pérdida económica de entre el 0.1 y 0.4 % del presupuesto anual del proceso. Disminución en la prestación del servicio TI entre un 0.1% y 4.9%	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
2	MENOR	Pérdida económica de entre el 0.5 y 0.9 % del presupuesto anual del proceso. Disminución en la prestación del servicio entre un 5% y 9.9%	-No afecta la seguridad de la información del proceso. -Se puede recuperar la información con la misma calidad en un tiempo moderado. -Se presentan reprocesos menores en las actividades del proceso.
3	MODERADO	Pérdida económica de entre el 1 y 10% del presupuesto anual. Disminución en la prestación del servicio entre un 10% y 20%	-Hay una afectación moderada de la seguridad de la información de la entidad. -Afecta medianamente la imagen corporativa de la entidad ante sus partes interesadas.

NIVEL	CRITERIO	CRITERIOS DE IMPACTO (Seguridad de la Información)	
		IMPACTO CUANTITATIVO	IMPACTO CUALITATIVO
			-Se presentan reprocesos moderados en las actividades. -La información se puede recuperar, pero no con la misma calidad.
4	MAYOR	Pérdida económica de entre el 11 y 20% del presupuesto anual. Disminución en la prestación del servicio entre un 21% y 29.9%	-Se genera una afectación importante en la seguridad de la información de la entidad. -Afecta altamente la imagen corporativa de la entidad. -Se generan mayores reprocesos en las actividades. -Es difícil de recuperar la información.
5	CATASTROFICO	Pérdida económica superior al 20% del presupuesto anual. Disminución en la prestación del servicio hasta en un 50%	-Se presenta una afectación crítica a la seguridad de la información. -Se afecta negativamente y en gran proporción la imagen corporativa de la entidad ante terceros. -No es posible realizar la recuperación de la información. -Puede afectar las decisiones estratégicas de la entidad y la continuidad del negocio.

11.3.3 Determinación del Nivel de Riesgo Inherente

El nivel de riesgo inherente resulta de multiplicar el nivel de probabilidad por el nivel de impacto para cada uno de los riesgos.

Los resultados de la calificación el nivel de riesgo inherente del riesgo debe ser registrados en las matrices de riesgos de gestión, de corrupción y de seguridad de la información de la entidad según sea el caso.

El resultado permite 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. A este ejercicio se le conoce como **evaluación del riesgo** que es la siguiente etapa en la gestión del riesgo

11.3.4 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.

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 digital y el mapa de zonas de calor para los riesgos de corrupción.

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

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

		IMPACTO				
		Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5
PROBABILIDAD	Rara vez 1	1	2	3	4	5
	Improbable 2	2	4	6	8	10
	Posible 3	3	6	9	12	15
	Probable 4	4	8	12	16	20
	Casi seguro 5	5	10	15	20	25

Mapa de Zonas de Calor para los Riesgos de Corrupción.

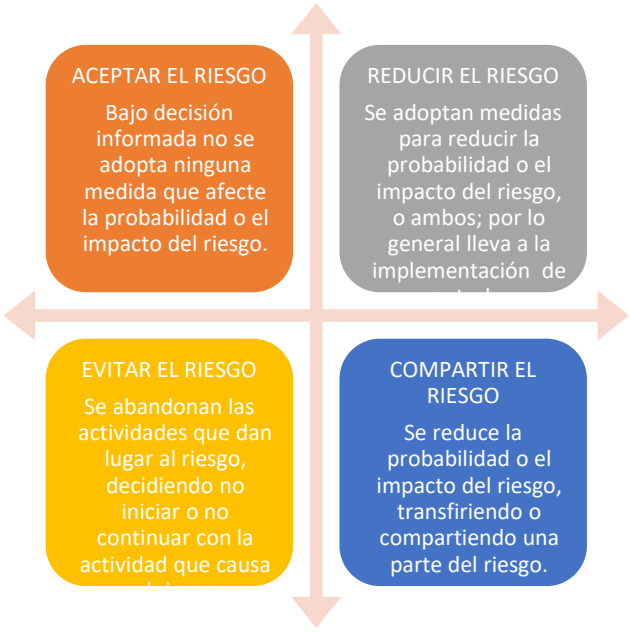
ZONAS DE CALOR RIESGOS DE CORRUPCIÓN

			IMPACTO		
			Moderado 3	Mayor 4	Catastrófico 5
PROBABILIDAD	Rara vez	1	3	4	5
	Improbable	2	6	8	10
	Posible	3	9	12	15
	Probable	4	12	16	20
	Casi seguro	5	15	20	25

Frente a estos criterios de aceptación del riesgo de la entidad, todo riesgo que resultado de su análisis se ubique en una zona diferente a la verde, requiere de la implementación de controles o medidas de intervención para su mitigación, de acuerdo a las prioridades establecidas en la **tabla 2. Niveles de Riesgo y Criterios de Decisión.**

Una vez se ubican los riesgos en los mapas de zonas de calor se inicia la etapa de tratamiento de los riesgos para aquellos que lo requieran.

11.3.5 Tratamiento del Riesgo



Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. Los tratamientos pueden ser de diferentes tipos de acuerdo con su finalidad.

Las otras opciones de tratamiento en la SSF son:

1. **Aceptar el Riesgo**: Bajo decisión informada y avalada por el comité institucional de control interno la entidad decide no intervenir el riesgo, esta decisión puede tomarse debido a que el costo de intervenir el riesgo es más alto que los impactos que los impactos estimados en caso de materializarse.
2. **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**.** Debido a la naturaleza de la Superintendencia del Subsidio Familiar, esta es la opción más utilizada para mitigar los riesgos.
3. **Evitar el riesgo:** Con el aval del comité institucional de coordinación de control interno la entidad decide abandonar la actividad fuente generadora del riesgo.
   Compartir el riesgo: Bajo esta opción se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Puede darse a través del establecimiento de pólizas o subcontratación.

11.3.5.1 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.

Los controles preventivos deben abordar directamente las causas del riesgo por lo que no deben existir causas que no tengan asociados al menos un control preventivo.

Es responsabilidad de la primera línea de defensa diseñar e implementar controles efectivos para mitigar los riesgos.

Es responsabilidad de la segunda línea de defensa evaluar los controles en su diseño

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

Identificación de Controles Existentes

Posterior a la evaluación del riesgo inherente, es necesario identificar y evaluar los controles que actualmente aplica la SSF para mitigar los riesgos.

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 de una materialización de un riesgo, estos controles mitigan los posibles impactos de las materializaciones y por ende disminuyen el nivel de impacto de los mismos.

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 no pretenden evitar que un riesgo se materialice, pero permiten mitigar los efectos derivados de la materialización.

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.

Evaluación del Diseño de Controles.

Los controles son actividades que al ejecutarse adecuadamente disminuyen por sí solas la probabilidad de que el riesgo se materialice o mitigan su impacto. Por lo anterior la entidad ha definido unos criterios que todo control debe cumplir con el objetivo de lograr efectividad al momento de su aplicación.

Los criterios 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 15. Criterios para la evaluación de controles en el diseño

CRITERIO DE EVALUACIÓN	PREGUNTAS PARA LA EVALUACIÓN DE CONTROLES	POSIBLES RESUESTAS	CALLIFICACIÓN
Responsable	**¿Existe un responsable del control?:** Hace referencia a si existe un responsable de la ejecución del control con la autoridad, competencias y conocimientos necesarios.	**Asignado** **No Asignado**	**15** **0**
Autoridad sobre el Control	**¿El Responsable tiene la autoridad y la adecuada segregación de funciones en la ejecución del control?:** Hace referencia a si el responsable de la ejecución del control cuenta con la autoridad, competencias y conocimientos necesarios para aplicar el control o para hacer que se aplique.	**Adecuado** **No adecuado**	**10** **0**
Frecuencia	**¿La frecuencia del control es adecuada?:** Hace referencia a si el control tiene una periodicidad específica para su ejecución (diario, mensual, trimestral, etc.) que ayude a prevenir o detectar el riesgo de manera oportuna.	**Oportuna** **Inoportuna** **No definida**	**15** **10** **0**
Propósito	**¿Se tiene establecido el propósito del control?:** Hace referencia a si el control tiene un propósito que indique para que se realiza el mismo asegurándose de que ese propósito esté respondiendo a las causas que generan el riesgo	**Previene materialización o mitiga impacto** **No está definido de qué manera previene o mitiga el riesgo**	**15** **0**
Metodología	**¿Se ha definido y documentado la metodología para realizar la actividad de control?**: Hace referencia a si se ha establecido y estandarizado el control a través de información documentada la manera en la que se realiza el control	**Estandarizado** **No Estandarizada** **No definida**	**15** **10** **0**

CRITERIO DE EVALUACIÓN	PREGUNTAS PARA LA EVALUACIÓN DE CONTROLES	POSIBLES RESUESTAS	CALLIFICACIÓN
Desviaciones	**¿Se registran y gestionan las observaciones y desviaciones encontradas?:** Hace referencia a si se ha determinado que se debe hacer en caso de encontrar una posible materialización del riesgo	**Existen criterios formales de registro y manejo de posibles materializaciones** **Existen criterios no unificados para registro y manejo de posibles materializaciones** **No existen criterios registro y manejo de posibles materializaciones**	**15** **10** **0**
Evidencia	**¿Se cuenta con las evidencias de la ejecución control?**: Hace referencia a si se tiene definida la evidencia que debe quedar de la ejecución del control y si esta evidencia permite que la información sea revisada por un tercero	**Completa** **Parcial** **No se ha definido**	**15** **10** **0**

Un control fuerte en el diseño tendrá un puntaje de 100 como resultado de la validación.

Evaluación de la Ejecución de los Controles

Una vez que se evalúa el diseño de los controles, estos deben ejecutarse de manera consistente con este diseño, 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 por auditoría interna o por los seguimientos realizados por la Oficina de Control Interno.

Taba 16. Criterios para la evaluación de controles en el diseño

CRITERIO DE EVALUACIÓN	PREGUNTAS PARA LA EVALUACIÓN DE CONTROLES	POSIBLES RESUESTAS	CALLIFICACIÓN
Responsable	**¿Existe un responsable del control?:** Se debe evidenciar la ejecución del control por parte del responsable establecido para el mismo.	**Evidencia completa** **Evidencia parcial** **No se evidencia**	**15** **10** **0**
Autoridad sobre el Control	**¿El Responsable tiene la autoridad y la adecuada segregación de funciones en la ejecución del control?:** Hace referencia a si se evidencia un responsable de la ejecución del control con la autoridad, competencias y conocimientos necesarios.	**Evidencia completa** **Evidencia parcial** **No se evidencia**	**10** **05** **0**
Frecuencia	**¿La frecuencia del control es adecuada?:** Hace referencia a si cuenta con evidencia de la aplicación del control de acuerdo con la periodicidad establecida para su ejecución (diario, mensual, trimestral, etc.	**Evidencia completa** **Evidencia parcial** **No se evidencia**	**15** **10** **0**
Propósito	**¿Se tiene establecido el propósito del control?:** Hace referencia a si se cuenta con la evidencia suficiente sobre si el control cumple con su propósito	**Evidencia completa** **Evidencia parcial** **No se evidencia**	**15** **10** **0**
Metodología	**¿Se ha definido y documentado la metodología para realizar la actividad de control?**: Hace referencia a si existe evidencia de aplicación del control de acuerdo con lo establecido en la información documentada	**Evidencia completa** **Evidencia parcial** **No se evidencia**	**15** **10** **0**
Desviaciones	**¿Se registran y gestionan las observaciones y desviaciones encontradas?:** Hace referencia a si se cuenta con evidencia del oportuno registro de materialización y de la aplicación de los procedimientos establecidos para estos casos	**Evidencia completa** **Evidencia parcial** **No se evidencia**	**15** **10** **0**
Evidencia	**¿Se cuenta con las evidencias de la ejecución control?**: Hace referencia	**Evidencia completa**	**15**

CRITERIO DE EVALUACIÓN	PREGUNTAS PARA LA EVALUACIÓN DE CONTROLES	POSIBLES RESUESTAS	CALLIFICACIÓN
	a si se cuenta con la evidencia establecida para la ejecución del control deja evidencia de su ejecución y si esta evidencia permite que la información sea revisada por un tercero	**Evidencia parcial** **No se evidencia**	**10** **0**

Un control fuerte en la ejecución tendrá un puntaje entre 90 y 100 como resultado de la validación.
:
Los criterios para la calificación de los controles son los siguientes:

Tabla 17. Criterios para la evaluación de la solidez de los controles en el diseño

Criterio de Evaluación de la solidez del Control en el Diseño	Calificación
Fuerte	Entre 90 -100
Moderado	Entre 70 - 89
Débil	Entre 0 - 69

Como resultado de la evaluación de la solidez de los controles se presenta un desplazamiento de los riesgos en el mapa de calor de una zona de riesgo inherente a una zona riesgos residual. El desplazamiento se realiza de acuerdo con lo establecido en la siguiente tabla.

Tabla 18. Desplazamiento del Riesgo en el Mapa de Calor

Resultado de la calificación	Calificación	Desplazamiento en el mapa de calor
Control Preventivo Fuerte	Entre 90 -100	Desplazamiento en eje de probabilidad 2 cuadrantes hacia arriba
Control Preventivo Moderado	Entre 70- 89	Desplazamiento en eje de probabilidad 1 cuadrante hacia arriba
Control Preventivo Débil	Entre 0 - 69	No hay desplazamiento
Control Detectivo Fuerte	Entre 90 -100	Desplazamiento en eje de impacto 2 cuadrantes hacia la izquierda
Control Detectivo Moderado	Entre 70- 89	Desplazamiento en eje de impacto 1 cuadrante hacia la izquierda
Control Detectivo Débil	Entre 0 - 69	No hay desplazamiento
Control Correctivo Fuerte	Entre 90 -100	Desplazamiento en eje de impacto 2 cuadrantes hacia la izquierda
Control Correctivo Moderado	Entre 70- 89	Desplazamiento en eje de impacto 1 cuadrante hacia la izquierda
Control Correctivo Débil	Entre 0 - 69	No hay desplazamiento

El registro de la evaluación de los controles quedará consignado en los mapas de riesgos de gestión, de corrupción y de seguridad de la información.

Después de la validación de la solidez de controles los riesgos se obtiene el nivel de riesgos residual y sobre este nuevamente se evaluará el riesgo para **determinar si es necesario establecer nuevas medidas de intervención del riesgo o si el riesgo en su nivel residual puede asumirse.**

El nivel de riesgo residual se validará nuevamente por la tercera línea de defensa a través de la evaluación del control en su aplicación.

El mapa de riesgos resultante después de la evaluación de los controles, es el mapa de riesgos residual.

11.3.6 Monitoreo y Revisión

La Entidad debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad. El modelo integrado de plantación y gestión (MIPG) en la dimensión 7 “Control interno” desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control.

11.3.6.1.1 Responsabilidades Frente al Monitoreo y Revisión por Líneas de Defensa

Para la realización de las actividades de monitoreo y seguimiento a la efectividad de la gestión del riesgo, se establecen las siguientes responsabilidades de acuerdo con las líneas de defensa:

Línea estratégica:

- Revisar los cambios en el “Direccionamiento estratégico” y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
- Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.
- Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por la Oficina de Control Interno o Auditoría Interna.
- Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas.
- Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

Primera Línea de Defensa

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso.
- Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- Revisar y reportar a la Oficina Asesora de Planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.
- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

Segunda Línea de Defensa

- Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.
- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos.

- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.
- Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

Tercera Línea de Defensa

- Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
  Para mitigar los riesgos de los procesos se encuentren documentados y actualizados en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

11.3.6.1.2 Frecuencia para la Revisión y Monitoreo para los Riesgos de Gestión y de Seguridad de la Información

El seguimiento a la gestión de los riesgos se debe realizar de acuerdo con las responsabilidades establecidas para tal fin por el esquema de líneas de defensa La frecuencia para realizar los ejercicios de seguimiento a los riesgos de gestión y seguridad de la información se establece en la siguiente tabla.

Tabla 19. Frecuencia para el seguimiento a los riesgos de gestión y de seguridad de la información

NIVEL DE RIESGO INHERENTE	FRECUENCIA DE SEGUIMIENTO
Extremo	Trimestral
Alto	Trimestral
Moderado	Trimestral
Bajo	Semestral

11.3.6.1.3 Monitoreo a los Riesgos de Corrupción

Los responsables de los procesos, en conjunto con sus equipos (primera línea de defensa), deben monitorear y revisar periódicamente la gestión de riesgos de corrupción. Le corresponde, igualmente, a la Oficina Asesora de Planeación adelantar el seguimiento, para este propósito se debe elaborar un informe con frecuencia cuatrimestral.

Se debe dejar evidencia de los ejercicios de seguimiento y revisión a la gestión del riesgo mediante informes de gestión elaborados de acuerdo con lo establecido en las responsabilidades propias de cada línea de defensa.