Supersolidaria
Superintendencia de la Economía Solidaria
"Super-Visión" para la transformación

Documento técnico
2020

# Política para la administración de Riesgos de la Supersolidaria

El emprendimiento es de todos
Minhacienda

**Superintendencia de la Economía Solidaria**

**-Supersolidaria-**

Ricardo Lozano Pardo
**Superintendente**

**Equipo directivo**

Martha Luz Camargo de la Hoz
**Secretaria General**

Martha Nury Beltrán Misas
**Delegada para la Supervisión del Ahorro y la Forma Asociativa Solidaria**

Gustavo Serrano Amaya
**Delegado para la Supervisión de la Actividad Financiera del Cooperativismo**

Ligia Galvis Amaya
**Jefe Oficina Asesora de Planeación y Sistemas**

Juan Carlos López Gómez
**Jefe Oficina Asesora Jurídica**

Mabel Astrid Neira Yepes
**Jefe Oficina de Control Interno**

**Equipo de trabajo**

Sonia Constanza Díaz Riveros
**Profesional Especializado - Grupo de Planeación**

Portada
**Grupo de Comunicaciones**

# Tabla de contenido

# 1. Introducción

La Superintendencia de la Economía Solidaria define su política para la administración del riesgo como parte fundamental en el cumplimiento de los objetivos institucionales y el quehacer misional, teniendo como referente el Modelo Integrado de Planeación y Gestión- MIPG, en sus dimensiones de direccionamiento estratégico y planeación, y Control Interno; algunos elementos de la norma técnica internacional ISO:31000:2018; lineamientos contenidos en la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública - DAFP y el Modelo de Seguridad y Privacidad de la información de la estrategia de Gobierno Digital; con el fin de emprender las medidas necesarias y establecer criterios orientadores para la identificación, análisis, valoración y tratamiento de los posibles eventos que se puedan presentar en el desarrollo de la gestión institucional, propendiendo el compromiso de la alta dirección y llevando la puesta en marcha del Sistema de Control Interno, como la clave para asegurar razonablemente que el Sistema de Gestión cumpla su propósito, lo que sin duda permite encausar el accionar de la entidad hacia el uso eficiente de los recursos y la prestación de trámites y servicios con calidad; donde cada servidor se constituya como parte integral de la gestión del riesgo, desarrollando una cultura organizacional fundamentada en la información, el control y la evaluación, para la toma de decisiones y la mejora continua.

## 2. Objetivo

Establecer elementos para la administración del riesgo que orienten el accionar de la entidad al fomento de una cultura de control, que permita la apropiación del Sistema de Control Interno y contribuya al cumplimiento de los objetivos institucionales de la Supersolidaria.

## 3. Alcance

La política de riesgos es aplicable a todos los procesos contenidos en el mapa de procesos de la entidad (estratégicos, operativos, misionales y de evaluación) que son desarrollados a través de las dependencias que componen la estructura organizacional de la Supersolidaria.

## 4. Glosario

**Aceptabilidad:** Resultado de la estimación del riesgo, en el cual, para cada riesgo identificado, éste puede considerarse aceptable o no de acuerdo a los criterios establecidos por la organización.

**Actividades Rutinarias:** Son aquellas que se realizan frecuentemente en las operaciones propias de la empresa.

**Actividades No Rutinarias:** Son aquellas que se realizan esporádicamente, indistintamente de que sean actividades propias de la empresa, contratadas o subcontratadas.

**Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital. (DAFP, 2018).

**Acción correctiva:** Se establecen para ayudar a la recuperación o reversión de la situación no deseada, además para establecer límites a las operaciones y efectuar un monitoreo constante.

**Acción detectiva:** Se diseñan para descubrir un evento, irregularidad o resultado no previsto, constituyen la segunda línea de defensa frente a los riesgos, al permitir accionar alarmas para alertar de hechos no deseados.

**Acción preventiva:** Constituyen a la primera línea de defensa al actuar sobre la causa de los riesgos. También llamados preliminares, se ejecutan antes de que se realice una actividad.

**Administración de riesgos:** Proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación. (INTOSAI, 2000).

**Amenaza:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización (DAFP, 2018).

**Análisis del riesgo:** Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

**Antrópico:** Producido o modificado por la actividad humana.

**Aspecto Ambiental:** Elemento de las actividades, productos o servicios de una organización que puede interactuar con el ambiente.

**Autocontrol:** El Autocontrol, como uno de los fundamentos del Modelo Estándar de Control Interno, busca que los servidores públicos tengamos la capacidad de detectar las desviaciones de nuestro quehacer diario y tomar por iniciativa propia, los correctivos necesarios para lograr el cumplimiento de nuestras metas individuales.

**Autoevaluación:** Mecanismo de verificación y evaluación, que le permite a la entidad medirse a sí misma, al proveer la información necesaria para establecer si ésta funciona efectivamente o si existen desviaciones en su operación, que afecten su propósito fundamental.

**Autogestión:** Capacidad institucional de realizar efectivamente su función administrativa.

**Autorregulación:** Capacidad de todo servidor público de controlar su trabajo, detectar sus desviaciones y efectuar correctivos.

**Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización del riesgo. (DAFP, 2018)

**Causa raíz:** Causa principal que puede originar la materialización de un riesgo.

**Causa Subyacente:** Se refiere a esa causa que subyace. El verbo subyacer, por su parte, se vincula a permanecer oculto o debajo de alguna cosa.

**Condición Especial:** Se indica bajo cual condición diferente a la operación normal se materializa el riesgo, ejemplo: proyecto, emergencia, contingencia. En caso de no ser una condición especial se escribe N/A.

**Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o proceso no autorizados. (DAFP, 2018)

**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. (DAFP, 2018).

**Control del Riesgo:** Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones). (DAFP, 2018)

**Control Correctivo:** Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad detectada u otra situación no deseable.

**Control Preventivo:** Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad potencial u otra situación potencial no deseable.

**Corrupción:** Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

**Detectabilidad:** Determinación sobre los controles actuales del sistema, proceso y/o procedimiento que impidan que las causas se materialicen y que lo detecten antes de que alcance al cliente o usuario.

**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad. (DAFP, 2018)

**Efecto:** Desviación de lo esperado, ya sea positivo o negativo.

**Evaluación del riesgo:** Proceso usado para determinar las prioridades de gestión del riesgo mediante la comparación del nivel de riesgo contra normas predeterminadas, niveles de riesgo objeto u otros criterios.

**Evento:** Incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

**Frecuencia:** Medida de la tasa de ocurrencia de un evento, expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

**Gestión del Riesgo:** Es el conjunto de "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Contempla las etapas de política de administración del riesgo, construcción del mapa de riesgos, comunicación y consulta, monitoreo y revisión y seguimiento.

**Gestión del Riesgo de Corrupción:** Es el conjunto de "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo" de corrupción. (Presidencia de la República, 2015)

**Incertidumbre:** Deficiencia de la información relacionada con el conocimiento de un evento, su consecuencia o su probabilidad.

**Incidente:** Es el evento involuntario (casual y fortuito) que podría causar daños a las personas, equipos, servicios, productos o instalaciones.

**Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo. (DAFP, 2018)

**Impacto Ambiental:** Cualquier cambio en el ambiente, ya sea adverso o beneficioso, como resultado total o parcial de los aspectos ambientales de una organización.

**Integridad:** Propiedad de exactitud y completitud. (DAFP, 2018)

**Matriz de riesgos**: Es una herramienta que permite realizar la consolidación de las etapas de evaluación del riesgo, permitiendo conocer el panorama general del estado de los riesgos tanto inherentes como residuales de cada uno de los procesos.

**Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo. (DAFP, 2018)

**Método de detección:** Control por medio del cual se hace real la detectabilidad del riesgo.

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

**Oportunidad:** Puede surgir como resultado de una situación favorable para lograr un resultado previsto, por ejemplo, un conjunto de circunstancias que permita a la organización atraer clientes, desarrollar nuevos productos y servicios, reducir los residuos o mejorar la productividad. Una desviación positiva que surge de un riesgo puede proporcionar una oportunidad, pero no todos los efectos positivos del riesgo tienen como resultado oportunidades.

**Parte Interesada:** Persona o grupo, dentro o fuera del lugar de trabajo que tiene interés o está afectado por el desempeño de toda o de elementos de gestión de una organización.

**Peligro:** Fuente de daño potencial o situación con potencial para causar pérdida. Es una fuente o situación con potencial de daño en términos de lesión o enfermedad, daño a la propiedad, al ambiente de trabajo o una combinación de éstos.

**Pérdida:** Consecuencia negativa que trae consigo un evento.

**Plan de contingencia:** Plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones (proceso o procedimiento) de una compañía en caso de materializarse un riesgo. Se deben generar estas acciones de mejora de acuerdo al procedimiento.

**Plan de tratamiento del riesgo:** Plan que se define por medio de las acciones preventivas para implementar los nuevos controles, como producto del análisis y evaluación de cada uno de los riesgos. En caso de materializarse un riesgo se hace por medio de acción correctiva. Se deben generar estas acciones de mejora de acuerdo al procedimiento R- MECO-005 procedimiento para la identificación y tratamiento de acciones correctivas, preventivas y de mejora.

**Posibilidad:** Se emplea como una descripción cualitativa de la probabilidad o frecuencia.

**Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad. (DAFP, 2018)

**Probabilidad de detección:** Grado en el cual es probable que se haga efectiva la detectabilidad.

**Proceso de administración de riesgo:** Aplicación sistemáticas de políticas, procedimientos y prácticas de administración a las diferentes etapas de la Gestión del Riesgo.

**Riesgo:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias. (DAFP, 2018)

**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. (DAFP, 2018)

**Riesgo de Seguridad Digital:** 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. Incluyen aspectos relacionados con el ambiente físico, digital y las personas. (DAFP, 2018)

**Riesgo Inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. (DAFP, 2018)

**Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento. (DAFP, 2018)

**Tratamiento del riesgo:** Selección e implementación de las opciones apropiadas para ocuparse del riesgo.

**Tolerancia del riesgo:** Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable. (DAFP, 2018)

**Vulnerabilidad:** Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos. (DAFP, 2018).

## 5. Responsabilidades por línea de defensa

La Supersolidaria adopta el esquema de las líneas de defensa del Modelo Estándar de Control Interno – MECI, que consiste en asignar responsabilidades específicas y coordinar con eficiencia y eficacia la gestión del riesgo, de manera que no existan brechas en la cobertura de los controles ni duplicaciones innecesarias, permitiendo que al interior de la entidad se aseguren resultados satisfactorios.

A continuación, se definen las responsabilidades para la gestión del riesgo de acuerdo a cada línea de defensa:

## 4.1 Línea Estratégica

**Función:** Instancia decisoria dentro del Sistema de Control Interno que define el marco general para la gestión del riesgo y el control, y supervisa su cumplimiento.

**Responsables de las acciones en la línea estratégica:**

- Alta dirección
- Comité Institucional de Coordinación de Control Interno

**Responsabilidades frente al riesgo:**

1. Establecer y aprobar la política de administración del riesgo.
2. Definir y hacer seguimiento a los niveles de aceptación del riesgo.
3. Realizar seguimiento y análisis semestral a los riesgos institucionales.
4. Realizar monitoreo al cumplimiento de los estándares de conducta y la práctica de los principios y los valores del servicio público.
5. Retroalimentar al Comité Institucional de Gestión y Desempeño para la mejora de la gestión, a partir de los resultados de la evaluación o seguimiento al Sistema de Control Interno.
6. Evaluar el estado del Sistema de Control Interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del sistema a partir de la normatividad vigente.
7. Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
8. Revisión del adecuado despliegue de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.
9. Hacer seguimiento en el Comité Institucional de Coordinación 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.
10. 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.
11. Hacer seguimiento y pronunciarse por lo menos cada semestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a los criterios de aceptación establecidos y aprobados.
12. Revisar los informes presentados cada semestre 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.

13. Revisar las acciones que conforman el plan de tratamiento consolidado en el Mapa de Riesgos Institucionales, con el fin de que se tomen medidas oportunas y eficaces para evitar la materialización de riesgos o la repetición del evento.
14. Fomentar la generación de acciones para apoyar a la segunda línea de defensa frente a la promoción de espacios para capacitar a los líderes de proceso y sus equipos de trabajo sobre política y la metodología, así como las acciones de seguimiento del riesgo.

## 4.2 Primera Línea de Defensa

**Función:** Se encarga de llevar a cabo la gestión del riesgo en cada uno de los procesos, controla y mitiga los riesgos a través del autocontrol.

**Responsables de las acciones en la primera línea de defensa:**

- Líderes de proceso y sus equipos de trabajo (en general servidores públicos de todos los niveles de la entidad).

**Responsabilidades frente al riesgo:**

1. Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos generan nuevos riesgos o modifican los identificados en cada uno de los procesos, para la actualización de la Matriz de Evaluación de Riesgos.
2. Identificar, analizar y valorar los riesgos que pueden afectar el cumplimiento de los objetivos y actualizarlos cuando sea requerido.
3. Definir y aplicar los controles establecidos para mitigar los riesgos identificados, alinearlos con los objetivos institucionales y proponer mejoras a la gestión del riesgo en los procesos.
4. Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión de los procesos, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.
5. Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
6. Reportar los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.
7. Revisar que las actividades de control de los procesos se encuentren documentadas y actualizadas en los procedimientos.
8. Revisar el cumplimiento de los objetivos de los procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando.
9. Revisar los eventos de riesgos que se han materializado, 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.

10. Revisar los planes de contingencia establecidos para los riesgos materializados, con el fin de tomar medidas oportunas y eficaces para evitar en lo posible la repetición del evento.
11. Revisar y hacer seguimiento al cumplimiento de las actividades y planes de tratamiento con relación a la gestión de riesgos.
12. Reportar a la segunda línea de defensa el resultado de la gestión de riesgos del proceso, para su inclusión en la Matriz de Evaluación de Riesgos Institucionales y el Mapa de Riesgos Institucional, incluidos los riesgos de corrupción.

## 4.3 Segunda Línea de Defensa

**Función:** Su rol principal es orientar a la Primera línea de defensa en el proceso de gestión del riesgo y que los controles sean apropiados y funcionen correctamente; así mismo, consolidar y analizar información, enmarcado en la autogestión.

**Responsables de las acciones en la segunda línea de defensa:**

- Jefe Oficina Asesora de Planeación y Sistemas

**Responsabilidades frente al riesgo:**

1. Asesorar a la línea estratégica en el análisis del contexto interno y externo para el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
2. Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos pueden 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 la Matriz de Evaluación de Riesgos Institucionales.
3. Consolidar el Mapa de Riesgos Institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno.
4. Presentar al Comité Institucional de Coordinación de Control Interno el seguimiento a los controles establecidos para la mitigación del riesgo.
5. Acompañar y orientar a los líderes de procesos y responsables en la identificación, análisis y valoración del riesgo.
6. Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.
7. Supervisar a la primera línea de defensa en coordinación con los demás responsables de esta línea, para que identifique, evalué y gestione los riesgos y controles.
8. Evaluar que los riesgos sean consistentes con la política para la administración de riesgos de la entidad.

**Otros responsables de la segunda línea de defensa:**

- Coordinadores de procesos: Gestión de contratación, Gestión de recursos financieros, Gestión de servicios de TI.

**Responsabilidades frente al riesgo:**

1. Reportar a la Oficina Asesora de Planeación y Sistemas a través de ISOlución -módulo de riesgos y/o mecanismo dispuesto, el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar.
2. Supervisar que la primera línea de defensa identifique, evalué y gestione los riesgos en sus procesos, relacionados con contratación, gestión financiera y gestión de servicios de tecnologías de información.

## 4.4 Tercera Línea de Defensa

**Función:** Realizar evaluación (independiente) y seguimiento sobre la efectividad de la gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.

**Responsable de las acciones en la tercera línea de defensa:**

- Jefe Oficina de Control Interno

**Responsabilidades frente al riesgo:**

1. Dar orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación y Sistemas.
2. Monitoreo a la exposición de la entidad al riesgo y realizar recomendaciones con alcance preventivo.
3. Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.
4. Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.
5. Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos (gestión, corrupción y seguridad digital) de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control Interno.
6. Recomendar mejoras a la política de administración del riesgo.

7. Revisión de la definición y alineación de los objetivos de los procesos con los objetivos institucionales, sobre los cuales se identificaron los riesgos, y realizar las recomendaciones a que haya lugar.
8. Revisar que se hayan identificado los riesgos que afecten directamente el cumplimiento de los objetivos de los procesos y que se hayan incluido los riesgos de corrupción.
9. 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.
10. 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.
11. Para mitigar los riesgos de los procesos, revisar que se encuentren documentados y actualizados los procedimientos y planes de mejora establecidos 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.
12. Capacitación continua en temas relacionados con la gestión de riesgos, con el fin de fortalecer el rol de evaluador independiente.

### *Responsabilidades riesgos de seguridad digital*

Para el tratamiento de riesgos de seguridad digital, la entidad debe designar un responsable, el cual debe pertenecer a un área que haga parte de la alta dirección o línea estratégica y las responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad digital según MinTic, serán las siguientes:

- Definir el procedimiento para la Identificación y Valoración de Activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a las diferentes líneas de defensa en la gestión de riesgos de seguridad digital, el establecimiento de controles para mitigar los riesgos y el reporte.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

## 6. Proceso para la gestión del riesgo

El proceso para la gestión del riesgo permite tener un esquema general frente a los diferentes elementos que interactúan en el adecuado manejo de éstos, además consta de la definición del

enfoque organizacional para la valoración del riesgo y su posterior tratamiento, favoreciendo la gestión institucional.

A continuación, se presenta el proceso para la Gestión del Riesgo de la Supersolidaria:

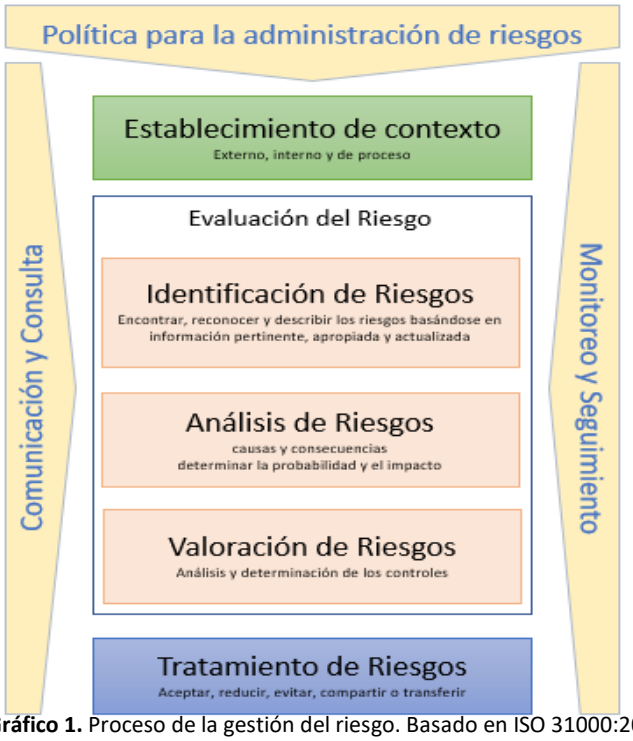


**Gráfico 1.** Proceso de la gestión del riesgo. Basado en ISO 31000:2018

La etapa de evaluación del riesgo (identificación, análisis y valoración), se desarrolla en la Metodología para la Evaluación de Riesgos D-MECO-003 versión 03.

## 7. Establecimiento de contexto

Para el establecimiento del contexto, se tendrán en cuenta los siguientes criterios:

### *Contexto externo*

- Factores sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos, ambientales, ya sean internacionales, nacionales, regionales o locales.
- Relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas.
- Complejidad de las redes y dependencias

### *Contexto interno*

- Visión, misión y valores
- Estructura de la organización, roles e informe de rendición de cuentas
- Objetivos institucionales y políticas internas
- Cultura organizacional
- Normas, directrices y modelos adoptados por la entidad
- Conocimiento clave de la entidad
- Mapa de procesos
- Datos, sistemas de información y flujos de información
- Relaciones con grupos de valor y de interés (percepciones y valores)
- Relaciones contractuales y compromisos

### *Contexto Proceso*

Para el análisis de contexto del proceso se debe contar con las caracterizaciones de cada uno de los procesos actualizadas y alineadas con el marco estratégico vigente de la entidad.

- Objetivo y alcance del proceso
- Procedimientos asociados
- Responsables del proceso
- Activos de seguridad digital del proceso

## 8. Niveles y criterios para calificar la probabilidad

En la siguiente tabla se determinan los niveles para la calificación de la probabilidad, determinados por la descripción de la medida cualitativa y la frecuencia (para la valoración de la probabilidad por criterios de factibilidad, consultar la Metodología para la evaluación de riesgos).

| Nivel | Medida Cualitativa | Frecuencia |
|---|---|---|
| 1 | Muy baja | Puede ocurrir solo en circunstancias excepcionales<br>Probabilidad anual entre el 0% y 3% |
| 2 | Baja | Podría ocurrir en algún momento<br>Probabilidad anual entre el 3% y 10% |
| 3 | Media | Probablemente ocurrirá en algunas circunstancias<br>Probabilidad anual entre el 10% y 30% |
| 4 | Alta | Probablemente ocurrirá en repetidas circunstancias<br>Probabilidad anual entre el 30% y 50% |
| 5 | Muy alta | Se espera que ocurra en la mayoría de las circunstancias<br>Probabilidad anual superior al 50% |

**Tabla 1.** Criterios para calificar la probabilidad

## 9. Niveles y criterios para calificar el impacto

Los niveles de medición del impacto están dados en función a la consecuencia económica, legal y reputacional que la entidad puede sufrir en caso de materialización de un evento de riesgo.

Para la calificación del impacto de cada uno de los riesgos identificados, se deben revisar de manera detallada cada uno de los criterios cuantitativos y cualitativos presentados en la siguiente tabla.

| RIESGO | NIVEL | VALOR DEL IMPACTO | IMPACTO (CONSECUENCIAS) CUANTITATIVO | IMPACTO (CONSECUENCIAS) CUALITATIVO |
|---|---|---|---|---|
| RIESGOS DE GESTIÓN | Catastrófico | 5 | Impacto que afecte la ejecución presupuestal en un valor de pérdida de cobertura en la prestación de los servicios de la entidad ≥50%.<br><br>Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%.<br><br>Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad. | Interrupción de las operaciones de la entidad por más de cinco (5) días.<br><br>Intervención por parte de un ente de control u otro ente regulador.<br><br>Pérdida de información crítica para la entidad que no se puede recuperar.<br><br>Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.<br><br>Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados. |
| | Mayor | 4 | Impacto que afecte la ejecución presupuestal en un valor ≥20%.<br><br>Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%.<br><br>Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%.<br><br>Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad. | Interrupción de las operaciones de la entidad por más de dos (2) días.<br><br>Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.<br><br>Sanción por parte del ente de control u otro ente regulador.<br><br>Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.<br><br>Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos. |

| RIESGO | NIVEL | VALOR DEL IMPACTO | IMPACTO (CONSECUENCIAS) CUANTITATIVO | IMPACTO (CONSECUENCIAS) CUALITATIVO |
|---|---|---|---|---|
| | Moderado | 3 | Impacto que afecte la ejecución presupuestal en un valor ≥5%.<br><br>Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%.<br><br>Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%.<br><br>Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad. | Interrupción de las operaciones de la entidad por un (1) día.<br><br>Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.<br><br>Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios.<br><br>Reproceso de actividades y aumento de carga operativa.<br><br>Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.<br><br>Investigaciones penales, fiscales o disciplinarias |
| | Menor | 2 | Impacto que afecte la ejecución presupuestal en un valor ≥1%.<br><br>Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%.<br><br>Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%.<br><br>Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad. | Interrupción de las operaciones de la entidad por algunas horas.<br><br>Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias.<br><br>Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos. |
| | Insuficiente | 1 | Impacto que afecte la ejecución presupuestal en un valor ≥0,5%.<br><br>Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%.<br><br>Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%.<br><br>Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad. | No hay interrupción de las operaciones de la entidad.<br><br>No se generan sanciones económicas o administrativas.<br><br>No se afecta la imagen institucional de forma significativa. |

| RIESGO | NIVEL | VALOR DEL IMPACTO | IMPACTO (CONSECUENCIAS) CUANTITATIVO | IMPACTO (CONSECUENCIAS) CUALITATIVO |
|---|---|---|---|---|
| RIESGOS DE SEGURIDAD DIGITAL | Catastrófico | 5 | Afectación ≥65% hasta 92% de la población.<br><br>Afectación ≥65% hasta 92% del presupuesto anual de la entidad.<br><br>Afectación muy grave del medio ambiente que requiere de ≥5 años de recuperación. | Afectación muy grave de la integridad de la información debido al interés particular de los servidores públicos y terceros.<br><br>Afectación muy grave de la disponibilidad de la información debido al interés particular de los servidores públicos y terceros.<br><br>Afectación muy grave de la confidencialidad de la información debido al interés particular de los servidores públicos y terceros. |
| | Mayor | 4 | Afectación ≥39% hasta 65% de la población.<br><br>Afectación≥39% hasta 65% del presupuesto anual de la entidad.<br><br>Afectación importante del medio ambiente que requiere de ≥6 meses de recuperación. | Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros.<br><br>Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.<br><br>Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. |
| | Moderado | 3 | Afectación ≥15% hasta 39% de la población.<br><br>Afectación ≥15% hasta 39% del presupuesto anual de la entidad.<br><br>Afectación leve del medio ambiente requiere de ≥1 a 4 semanas de recuperación. | Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros.<br><br>Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros.<br><br>Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros. |
| | Menor | 2 | Afectación ≥5% hasta 15% de la población.<br><br>Afectación ≥5% hasta 15%del presupuesto anual de la entidad.<br><br>Afectación leve del medio ambiente requiere de ≥2 días de recuperación. | Afectación leve de la integridad.<br><br>Afectación leve de la disponibilidad.<br><br>Afectación leve de la confidencialidad. |
| | Insuficiente | 1 | Afectación ≥0% hasta 5% de la población.<br><br>Afectación ≥0% hasta 5% del presupuesto anual de la entidad.<br><br>No hay afectación medioambiental. | Sin afectación de la integridad.<br><br>Sin afectación de la disponibilidad.<br><br>Sin afectación de la confidencialidad. |

| RIESGO | NIVEL | VALOR DEL IMPACTO | IMPACTO (CONSECUENCIAS) CUANTITATIVO | IMPACTO (CONSECUENCIAS) CUALITATIVO |
|---|---|---|---|---|
| RIESGOS DE CORRUPCIÓN | Catastrófico | 5 | Genera consecuencias desastrosas para la entidad | |
| | Mayor | 4 | Genera altas consecuencias sobre la entidad. | |
| | Moderado | 3 | Genera medianas consecuencias sobre la entidad | |

**Tabla 2.** Criterios para calificar el impacto

## 10. Zona de riesgo

La Supersolidaria tendrá cuatro (4) zonas de riesgo:


**Gráfico 2.** Zona de Riesgo

Estos niveles de se tendrán en cuenta para todos los riesgos a excepción de los **riesgos de corrupción**, cuya zona solo será **moderada, alta y extrema**.

A continuación, se ubica cada zona de riesgo en el mapa de calor:

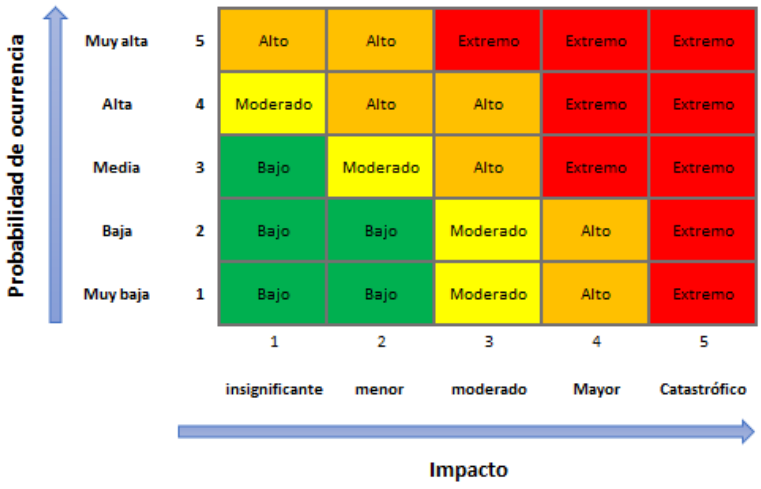


**Gráfico 3.** Mapa de calor

## 11. Niveles de aceptación del riesgo

De acuerdo con los niveles de riesgo establecidos, se definen los criterios de nivel de aceptación, periodicidad del seguimiento y las acciones a realizar en caso de materialización, como se presenta a continuación.

| Tipo de riesgo | Zona de riesgo | Nivel de aceptación del riesgo | Periocidad del seguimiento | Acciones a realizar en caso de materialización |
|---|---|---|---|---|
| Riesgos de Gestión | Bajo | Se ACEPTARÁ el riesgo. | Se administra por medio de las actividades propias del proceso y las áreas harán autocontrol mensual a su desempeño. | Establecer acciones correctivas al interior del proceso y verificar la calificación del riesgo residual y ubicación del riesgo para su inclusión en el mapa de riesgos. |
| | Moderado | Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. | se hace seguimiento TRIMESTRAL | • Proceder de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso).<br><br>• Realizar nuevamente la evaluación del riesgo, analizando la causa principal y determinar acciones correctivas, replantear los riesgos del proceso y actualizar el plan de mejora del proceso.<br><br>• Actualizar la Matriz y el Mapa de Riesgos.<br><br>• Informar al Proceso de Planificación Estratégica sobre el hallazgo y las acciones tomadas.<br><br>• Informar a la dirección, acciones definidas para la mitigación del riesgo materializado. |
| | Alto | Se establecen acciones de control preventivas que permitan EVITAR la materialización del riesgo.<br>Se debe incluir el riesgo en el Mapa de Riesgo Institucional. | Se monitorea TRIMESTRAL | |
| | Extremo | Se establecen acciones de Control Preventivas que permitan MITIGAR la materialización del riesgo.<br>Se debe incluir el riesgo tanto en el Mapa de Riesgo Institucional. | Se monitorea TRIMESTRAL | |
| Riesgos de Corrupción | Todos los niveles | Ningún riesgo de corrupción podrá ser aceptado.<br><br>Se establecen acciones para EVITAR o MITIGAR. | Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos. | El líder del proceso debe:<br>• Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado.<br>• Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento.<br>• Efectuar el análisis de causas y determinar acciones preventivas y de mejora.<br>• Actualizar el mapa de riesgos<br><br>El jefe de la Oficina de Control interno:<br><br>• Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar.<br>• Realizar la denuncia ante la instancia de control correspondiente de acuerdo al procedimiento establecido en el proceso de control interno disciplinario.<br>• Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. |
| Riesgos de Seguridad de la información | Bajo | Se ACEPTARÁ el riesgo. | Se administra por medio de las actividades propias del proceso y las áreas harán autocontrol mensual a su desempeño. | Es necesario realizar acciones de mejoramiento ejecutando actividades, tales como:<br><br>• Hacer una descripción detallada de lo ocurrido y del impacto generado en el proceso.<br><br>• Revisar las causas, riesgos y controles. Se debe tener en cuenta que en el análisis del riesgo varia la probabilidad.<br><br>• Tomar acciones para evitar el que se repita la materialización del riesgo detectado y actualizar el Mapa de riesgos y sus acciones de seguimiento contempladas.<br><br>• Realizar un monitoreo permanente. Los procesos deben Informar a la Oficina Asesora de Planeación la materialización de sus riesgos, quien a su vez comunicará al Comité Institucional de Coordinación de Control Interno. |
| | Moderado | Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. | se hace seguimiento TRIMESTRAL | |
| | Alta | Se establecen acciones de control preventivas que permitan EVITAR la materialización del riesgo.<br>Se debe incluir el riesgo en el Mapa de Riesgo Institucional. | Se monitorea TRIMESTRAL | |
| | Extrema | Se establecen acciones de Control Preventivas que permitan MITIGAR la materialización del riesgo.<br>Se debe incluir el riesgo tanto en el Mapa de Riesgo Institucional. | Se monitorea TRIMESTRAL | |

**Tabla 3.** Niveles de aceptación del riesgo

## 12. Tratamiento de riesgos

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo, para lo cual, la Supersolidaria se enmarca dentro de las siguientes categorías de acuerdo a la zona de riesgo:

| ZONA DE RIESGO | Categorías | | | |
|---|---|---|---|---|
| | Aceptar | Evitar | Reducir | Compartir o transferir |
| Extremo | | x | x | x |
| Alto | | x | x | x |
| Moderado | | x | x | |
| Bajo | x | | | |

**Gráfico 3.** Matriz tratamiento de riesgos

### *Categorías para el tratamiento de riesgos*

A continuación, se presenta cada una de las categorías para tratar el riesgo y las respectivas acciones a realizar.

| Categorías | Descripción | Acción |
|---|---|---|
| Aceptar | El riesgo se acepta cuando la frecuencia es baja y el impacto es insuficiente, es decir, no se pone en peligro la estabilidad de la entidad.<br><br>(Ningún riesgo de corrupción podrá ser aceptado). | Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario establecer controles y este puede ser aceptado, esto aplicaría para riesgos inherentes en la zona de calificación de riesgo bajo y se administra por medio de las actividades propias del proceso asociado.<br><br>La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo. |
| Evitar | Es siempre la primera alternativa a considerar. Se logra cuando al interior de los procesos se genera cambios sustanciales de mejoramiento, rediseño o eliminación, resultado de unos controles y acciones emprendidas, orientadas a la eliminación de la causa del riesgo o la actividad fuente del riesgo. | Se establecen acciones preventivas para evitar que se materialicen las causas identificadas.<br><br>para evitar la actividad o acción que da origen al riesgo:<br>– Retirar la(s) actividad(es) que lo origina(n)<br>– Cambiar las condiciones relacionadas (Ej: cambiar de lugar una instalación |
| Reducir | Al 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. | Si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles, se consigue mediante la optimización de los procedimientos y la implementación de controles por medio de acciones preventivas, para protegerse en caso de que se presente cambiando en la medida de las posibilidades la probabilidad o impacto del mismo.<br><br>Los controles deben proporcionar uno o más tipos de protección:<br>• Corrección de cualquier anormalidad.<br>•Eliminación de posibles errores y vulnerabilidades o fuentes de errores y vulnerabilidades, pero sin eliminar el riesgo, sólo reduciéndolo.<br>•Prevención de ataques sobre las vulnerabilidades.<br>• Minimizar el impacto: Controles que reducen o limitan los daños.<br>•Disuasión: Para hacer cambiar de intención o idea.<br>•Detección de errores o anomalías.<br>•Recuperación: Para regresar a la situación normal; monitoreo de señales de advertencia de vulnerabilidades, amenazas y riesgos, para prevenir.<br>• Conciencia: actividades de capacitación para orientar sobre la seguridad de la información, de modo que todos los usuarios sepan aplicar los conocimientos relacionados en su rutina personal y profesional. |
| Compartir o transferir | Hace referencia a buscar respaldo y compartir con un tercero parte del riesgo; esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro, o de un grupo a otro. Así mismo, el riesgo puede ser minimizado, compartiéndolo con otro grupo o dependencia.<br><br>Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.<br><br>Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. | Método para compartir algunos riesgos<br>• Puede implicar la creación de riesgos nuevos y tratamientos adicionales.<br>• Tomar pólizas de seguros (todo riesgo, entre otros).<br>• Contratación de servicios de terceros (outsourcing para procesos. Ej: celaduría, vigilancia, custodia de valores, entre otros) Es importante tener en cuenta que este tipo de acción conlleva a que se generen otros riesgos.<br>• Compartir el riesgo con acuerdos contractuales con proveedores. |

**Tabla 4.** Categorías para el tratamiento de riesgos

## 13. Monitoreo y Seguimiento

El propósito de las actividades de monitoreo y seguimiento es valorar la efectividad del control interno de la entidad, la eficiencia, eficacia y efectividad de los procesos y los resultados de la gestión del riesgo, con el propósito de detectar desviaciones y generar recomendaciones para orientar las acciones de mejora en la Supersolidaria.

Dentro de las responsabilidades establecidas por cada línea de defensa, se describen las responsabilidades en la gestión del riesgo, incluidas las actividades de monitoreo y seguimiento, sin embargo, en este capítulo, se describen de manera detallada algunas de las acciones a realizar, como se describe a continuación:

### *Monitoreo*

El líder de proceso realizará evaluaciones continuas o de autoevaluación a su proceso, realizando monitoreo a la medición de los resultados generados, teniendo en cuenta los indicadores de gestión, cuyo propósito será tomar las decisiones relacionadas con la corrección o mejoramiento del desempeño; también controla el desarrollo de las acciones para mitigar los riesgos, verificando la ejecución de las actividades en el tiempo programado, las cuales son fundamentales para prevenir o para reducir el riesgo.

El monitoreo debe:

a) Garantizar que los controles son eficaces y eficientes en el diseño y en la operación.
b) Obtener información adicional para mejorar la valoración del Riesgo.
c) Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.
d) Detectar cambios en el contexto externo e interno que puedan exigir revisión de los tratamientos del Riesgo y establecer un orden de prioridades de acciones para el tratamiento del Riesgo.
e) Identificar nuevos riesgos que pueden surgir.

Dentro del monitoreo a realizar se consolidará el mapa de riesgos institucionales, el cual contendrá el plan de tratamiento de riesgos, cuyo propósito es consolidar todas las acciones a adoptar para la prevención o mitigación de los riesgos, relacionando de manera específica cada una, el responsable de su ejecución, la periodicidad, la fecha de inicio y fecha fin; de manera tal que los involucrados comprendan las disposiciones.

El seguimiento de avance será reportado por las áreas a la Oficina Asesora de Planeación y Sistemas de manera trimestral dentro de los cinco (5) primeros días hábiles del siguiente mes, para la consolidación del mapa de riesgos y análisis; y su posterior presentación al Comité Institucional de Coordinación de Control Interno.

## *Seguimiento*

Para el seguimiento se llevarán a cabo evaluaciones independientes de forma periódica, por parte de la oficina de control interno a través de la auditoría interna de gestión. Estas evaluaciones permiten determinar si se han definido, puesto en marcha y aplicado los controles establecidos por la entidad de manera efectiva.

Las evaluaciones, independientes a los componentes varían en alcance y frecuencia, dependiendo de la importancia del riesgo, de la respuesta al riesgo y de los resultados de las evaluaciones continuas o autoevaluación. La auditoría se constituye en "una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de la entidad; que ayuda a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno", siendo la auditoría una herramienta de realimentación del SCI y de MIPG que analiza las debilidades y fortalezas del control y de la gestión, así como el desvío de los avances de las metas y objetivos trazados, lo cual influye en los resultados y operaciones propuestas en la entidad.

La actividad de auditoría interna debe realimentar a la entidad en el mantenimiento de controles efectivos, mediante la evaluación de la eficacia y eficiencia de los mismos promoviendo la mejora continua. Así mismo, para formarse una opinión sobre la adecuación y eficacia de los procesos de gestión de riesgos y control, la oficina de control interno debe basarse en las evidencias obtenidas en el ejercicio de auditoría.

La coordinación de las auditorías (cualquiera que sea su ámbito) está en cabeza del jefe de control interno, con el apoyo del líder del sistema de gestión; para ello, la oficina de control interno elabora un plan de auditoría anualmente y selecciona los proyectos, procesos y actividades a ser auditados basados en un enfoque de riesgos documentado, alineados con los objetivos y prioridades de la entidad, y desarrolla adecuados procedimientos para obtener suficiente evidencia para evaluar el diseño y la eficacia de los procesos de control en los diferentes procesos y actividades de la entidad. Este plan debe ser flexible de manera que puedan efectuarse ajustes durante el año, como consecuencia de cambios en las estrategias de la dirección, condiciones externas, áreas de mayor riesgo o modificación a los objetivos de la entidad.

Este seguimiento genera un Informe, el cual es presentado en el Comité Institucional de Coordinación de Control Interno. En el caso que la Oficina de Control Interno realice recomendaciones, éstas se desarrollan a través acciones de mejora en el proceso y su registro quedará en el módulo de mejora de ISOlución.

### *Riesgos de corrupción*

El seguimiento al mapa de riesgos de corrupción se hará a través de la matriz de seguimiento al Mapa de riesgos de corrupción (formato ISOlución), donde la primera línea de defensa hará registro del avance de cumplimiento de las acciones establecidas mensualmente y la segunda línea de defensa cada cuatrimestre.

El jefe de la Oficina de Control Interno, debe adelantar seguimiento al Mapa de Riesgos de Corrupción de manera independiente a través del formato dispuesto por el DAFP (anexo 6 guía para la administración de riesgos DAFP) y adicionalmente, adelantará las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

## 14. Comunicación y Consulta

El propósito de la comunicación y la consulta consiste en asistir a las partes interesadas a comprender el riesgo, las bases con que se toman decisiones y las razones por las que son necesarias acciones específicas, buscando promover la toma de conciencia y la autogestión, facilitando un intercambio de información basado en hechos, oportuno, pertinente y comprensible, teniendo en cuenta la confidencialidad, disponibilidad e integridad de la información.

Para la comunicación en función del fortalecimiento de los temas que giran en torno a la administración de riesgos, se utilizarán herramientas de formación virtual que permitan a su vez, evaluar el grado de interiorización de la política y metodología de riesgos de la Supersolidaria y generar mayor interacción frente a la resolución de inquietudes y/o conocer el estado de avance.

Para la consulta a la ciudadanía, se aplicarán encuestas de percepción.

**La comunicación de la información y el reporte debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos**, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la **mejora en la prestación de servicios**.

Es preciso **promover la participación** de los funcionarios con mayor experticia, con el fin de **aportar su conocimiento** en la identificación, análisis y valoración del riesgo.

Es importante tener en cuenta que se debe **conservar evidencia de la comunicación** de la información y reporte de la gestión del riesgo en **todas sus etapas**, por tanto, se debe hacer especial énfasis en la difusión, socialización, capacitación y/o entrenamiento de todos y cada de los pasos que componen la metodología de la administración del riesgo, asegurando que permee a la totalidad de la entidad.

## 14.1 Comunicación interna

La comunicación interna en la entidad para la gestión de riesgos se dará desde las líneas de defensa.

### *Línea Estratégica*

Corresponde al Comité Institucional de Coordinación de Control Interno y a la alta dirección establecer esta Política a través de acto administrativo, y asegurarse de comunicarla a todos los servidores de la Supersolidaria, de tal manera que conozcan su rol y nivel de responsabilidad dentro de la gestión de riesgos; esta comunicación se realizará con el apoyo del grupo de comunicaciones y la Oficina Asesora de Planeación y Sistemas, donde a través de los canales de comunicación dispuestos por la entidad, se realice la socialización de la Política y la sensibilización frente a la importancia de la gestión de riesgos en el cumplimiento de las metas y objetivos institucionales.

Además, cada vez que se reúna el Comité Institucional de Coordinación de Control Interno debe generarse un acta, la cual será responsabilidad de la Oficina de Control Interno, quien ejerce la secretaria técnica de dicho Comité, de acuerdo a lo establecido en la Resolución 2017130005055 del 19 de septiembre de 2017.

### *Primera Línea de Defensa*

Corresponde a la primera línea de defensa promover la comunicación de los riesgos al interior de sus áreas y comunicar a los colaboradores de los procesos para conocer los avances en la gestión de riesgos en sus procesos y los controles establecidos para la mitigación de los riesgos identificados, posteriormente aportar la evidencia de dicha comunicación.

*Segunda Línea de Defensa*

Corresponde a la Oficina Asesora de Planeación y Sistemas, apoyar en la difusión de esta política y realizar acompañamiento en la apropiación de la metodología para la gestión de riesgos.

*Tercera Línea de Defensa*

Corresponde a la Oficina de Control Interno comunicar a través de los informes de auditoría y seguimiento, el estado de la gestión de riesgos institucionales; establecer comunicación constante con la segunda línea de defensa.

## 14.2 Comunicación externa

La comunicación externa con los grupos de interés y valor de la Supersolidaria se dará a través de los canales de comunicación oficiales dispuestos de la entidad y en concordancia con los criterios establecidos en la Política de Comunicaciones, propendiendo la participación y el efectivo intercambio de información.

Dentro de los reportes externos para cumplir con los requisitos legales y reglamentarios, deberán ser reportados a las autoridades o instancias, en las herramientas o canales que el gobierno disponga.

En caso de presentarse una crisis o materialización de un riesgo donde se requiera la coordinación interinstitucional o con la comunidad, la institución hará uso de los medios físicos y tecnológicos con que cuente, para elaborar y desarrollar los planes de contingencia requeridos, dispondrá de los mecanismos para consolidar la información y comunicará oportunamente las acciones a realizar.