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

Documento técnico
Versión 1-2021

Política para la administración de Riesgos de la Supersolidaria

El emprendimiento es de todos
Minhacienda

Superintendencia de la Economía Solidaria

-Supersolidaria-

Liliana Andrea Forero Gómez

Superintendente (E)

Equipo directivo

Manuel Jesús Berrio Scaff

Delegado para la Supervisión del Ahorro y la Forma Asociativa Solidaria y Secretario General (E)

Gustavo Serrano Amaya

Delegado para la Supervisión de la Actividad Financiera del Cooperativismo

Javier Enrique Ariza Rodríguez

Jefe Oficina Asesora de Planeación y Sistemas (E)

Rodolfo Yanguas Rengifo

Jefe Oficina Asesora Jurídica (E)

Mabel Astrid Neira Yepes

Jefe Oficina de Control Interno

Equipo de trabajo

Sonia Constanza Díaz Riveros

Profesional Especializado - Grupo de Planeación

Luis Edwin Osorio Corredor

Oficial de Seguridad designado por la Alta Dirección

Portada

Grupo de Comunicaciones

Tabla de contenido

Índice de tablas

Índice de gráficos

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 y el diseño de controles en entidades públicas versión 5 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 bajo un enfoque preventivo en la protección de los recursos públicos administrados y que 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) y proyectos que son desarrollados a través de las dependencias que componen la estructura organizacional de la Supersolidaria.

4. Términos y definiciones

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).

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.

Autenticación: Información procedente de un usuario que es quien dice ser. Se verifica y se debe garantizar que el origen de los datos es correcto.

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.

Ciberseguridad: Condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones en el ciberespacio.

Cifrado: Proceso de codificación de información sensible para poder evitar que esta llegue a personas no autorizadas.

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 de acceso a la red (Mac): Su principal objetivo es asegurar que todos los dispositivos que sean conectados a las redes corporativas, cumplan con las políticas de seguridad establecidas para evitar amenazas.3

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.

Delito Informático: Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

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.

Encriptación: Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

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.

Filtración de datos: Divulgaciones que no están autorizadas que tratan de adquirir información confidencial y que pueden dar lugar a robos o fugas.

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, permitiendo que al interior de la entidad se asegure el cumplimiento del quehacer misional. A continuación, se definen las responsabilidades para la gestión del riesgo de acuerdo a cada línea de defensa:

5.1 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 en representación del Superintendente
- Comité Institucional de Coordinación de Control Interno

Responsabilidades frente al riesgo:

1. Establecer y aprobar la política para la administración del riesgo.
2. Definir y hacer seguimiento a los niveles de aceptación del riesgo.
3. Realizar monitoreo y seguimiento 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 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 acción consolidado en el mapa de riesgos institucionales y de corrupción, 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.

5.2 Primera Línea de Defensa

Función: Se encarga de llevar a cabo la gestión del riesgo en cada uno de los procesos y proyectos, 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).
- Líderes de proyectos
- Responsables de activos de información
- Supervisores de contratos

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 del mapa de riesgos institucionales.
2. Identificar, analizar y valorar los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de proceso.
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 y detectar las deficiencias de los controles.
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. Mantener actualizadas las caracterizaciones de sus procesos.
8. Revisar que las actividades de control de los procesos se encuentren documentadas y actualizadas en los procedimientos.
9. 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.
10. 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.
11. Revisar las acciones de contingencia establecidas para los riesgos materializados, con el fin de tomar medidas oportunas y eficaces para evitar en lo posible la repetición del evento.
12. Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción con relación a la gestión de riesgos.
13. Reportar a la segunda línea de defensa el resultado de la gestión de riesgos del proceso, así como los riesgos materializados y las alertas tempranas de manera oportuna y bajo los tiempos de reporte establecidos.

5.3 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
- Profesional especializado riesgos

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 actualizar el mapa de riesgos institucionales y de corrupción de la entidad.
3. Consolidar los Mapas de Riesgos Institucionales y de corrupción y presentarlos para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno.

4. Presentar al Comité Institucional de Coordinación de Control Interno los informes de monitoreo a la gestión del riesgo.
5. Acompañar y orientar a los líderes de procesos y responsables en la identificación, análisis y valoración del riesgo.
6. 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.
7. Actualizar la matriz de responsabilidades por línea de defensa para cada vigencia.

Otros responsables de la segunda línea de defensa:

- Coordinadores de los procesos: Gestión de contratación, Gestión de recursos financieros, Gestión de servicios de TI.
- Oficial de Seguridad designado por la Alta Dirección

Responsabilidades frente al riesgo:

1. Reportar a la Oficina Asesora de Planeación y Sistemas el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar.
2. Reportar alertas tempranas, materialización de riesgos y acciones contingentes adoptadas de riesgos asociados a sus procesos.
3. Supervisar que la primera línea de defensa identifique, evalué y gestione los riesgos en sus procesos, relacionados con contratación (matriz de riesgos de contratos), gestión financiera (riesgos de fraude) y gestión de servicios de tecnologías de información.

5.4 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, idoneidad y ejecución 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 para la 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 Min Tic, serán las siguientes:

- Definir el procedimiento para la identificación y valoración de activos de información.
- 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.
- Demás responsabilidades establecidas en la Política de seguridad de la información.

6. Proceso para la gestión del riesgo

El proceso para la gestión del riesgo permite tener un esquema general que comprende las actividades de establecimiento de contexto, evaluación del riesgo (identificación, análisis y valoración) definición de controles para el tratamiento y seguimiento.

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

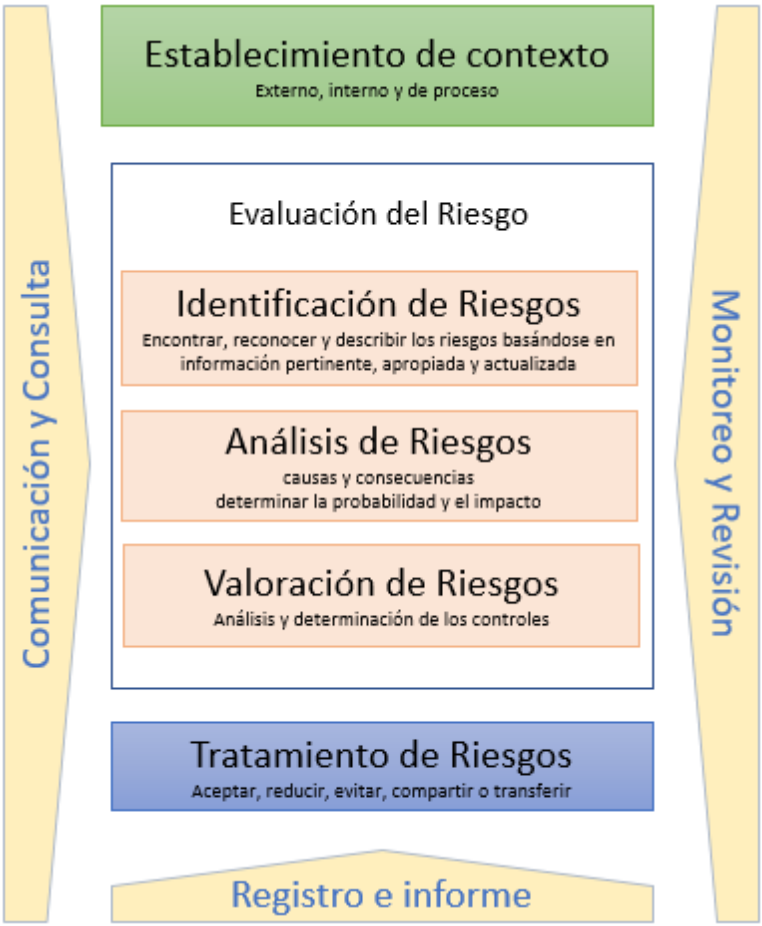

Gráfico 1. *Proceso de la gestión del riesgo. Basado en ISO 31000:2018*

Cada una de estas etapas se describen en la Metodología para la gestión de riesgos MT-PLES-001 versión 04.

7. Niveles y criterios para calificar la probabilidad

La probabilidad se entiende como la posibilidad de ocurrencia del riesgo y estará asociada al número de veces que el proceso o la actividad expuesta al riesgo, se ejecute durante un año.

En la siguiente tabla se determinan los niveles para la calificación de la probabilidad, determinados por la frecuencia de la actividad.

Medida Cualitativa	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Tabla 1. *Criterios para definir la probabilidad de ocurrencia. Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 DAFP.*

8. Niveles y criterios para calificar el impacto

Los niveles de medición del impacto están dados en función a la consecuencia económica 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.

Medida Cualitativa	Cuantitativo	Cualitativo	Peso
Leve	Afectación menor a 10 SMLMV.	•No hay interrupción de las operaciones de la entidad. •No se generan sanciones administrativas. •El riesgo afecta la imagen de algún área de la organización.	20%
Menor	Entre 10 y 50 SMLMV	•Interrupción de las operaciones de la entidad de 1 a 23 horas. •Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. •El riesgo afecta la imagen de la entidad internamente, de conocimiento general a nivel interno, nivel directivo y/o de proveedores.	40%
Moderado	Entre 50 y 100 SMLMV	•Interrupción de las operaciones de la entidad de 24 a 47 horas. •Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. •Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. •Reproceso de actividades y aumento de carga operativa. •Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. •Investigaciones penales, fiscales o disciplinarias.	60%
Mayor	Entre 100 y 500 SMLMV	•Interrupción de las operaciones de la entidad de 48 a 119 horas. •Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. •Sanción por parte del ente de control u otro ente regulador. •Incumplimiento en las metas y objetivos institucionales. •El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	80%
Catastrófico	Mayor a 500 SMLMV	•Interrupción de las operaciones de la entidad mayor a 120 horas. •Intervención por parte de un ente de control u otro ente regulador. •Pérdida de información crítica para la entidad que no se puede recuperar. •Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. •El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.	100%

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

Medición de impacto de riesgos de corrupción

La medición de impacto de los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración:

Descriptor	Descripción	Nivel	Respuestas afirmativas
Moderado	*Afectación parcial al proceso y a la dependencia. *Genera medianas consecuencias para la entidad.	5	1-5
Mayor	*Impacto negativo de la entidad. *Genera altas consecuencias para la entidad.	10	6-11
Catastrófico	*Consecuencias desastrosas para el sector. *Genera consecuencias desastrosas para la entidad.	20	12-19

Tabla 3. *Criterios para calificar el impacto de riesgos de corrupción.*

Cada riesgo de corrupción identificado, debe valorar el impacto de acuerdo a las preguntas establecidas en el formato FT-PLES -090.

Medición de impacto de riesgos de Seguridad Digital

En cuanto a los riesgos de seguridad digital, la medición se dará bajo los siguientes criterios:

Categoría	Descripción Cuantitativa	Descripción Cualitativa	Nivel
LEVE	Afectación en un valor igual o mayor al 1% de los grupos de valor de la Supersolidaria.	Interrupción de las operaciones de la entidad hasta por 8 horas (1 jornada laboral) y no conlleva afectación significativa para la Supersolidaria.	20%
	Afectación de un valor menor al 1% del presupuesto del presupuesto de la Entidad.	Afectación de la disponibilidad por hasta 1 hora de la jornada laboral.	
	No hay afectación medioambiental.	Afecta la confidencialidad de la información de uso interno de la persona que ejecuta el proceso.	
MENOR	Afectación en un valor igual o mayor al 1% y menor al 10% de los grupos de valor de la Supersolidaria.	Interrupción de las operaciones de la entidad por (1) día y no conlleva afectación significativa para la Supersolidaria.	40%
	Afectación en un valor igual o mayor al 1% e inferior al 10% del presupuesto de la Entidad.	Afectación de la disponibilidad por más de una hora y hasta 1 semana.	
	Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.	Afecta la confidencialidad de la información pública y clasificada del área que lidera un proceso.	
MODERADO	Afectación en un valor igual o mayor al 10% y menor al 20% de los grupos de valor de la Supersolidaria.	Afectación moderada de la integridad de la información que afecte hasta (2) sistemas de información con impacto significativo de índole legal o económica, retraso de funciones o genera pérdida de imagen severa de la Supersolidaria.	60%
	Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto de seguridad de información de la entidad.	Afectación la disponibilidad hasta tres (3) Sistemas de información o (1) semana.	
	Afectación leve del medio ambiente requiere de 3,1 a 1 año de recuperación.	Afecta la confidencialidad de la información pública y clasificada de un sistema de información.	
MAYOR	Afectación en un valor igual o mayor al 20% e inferior al 50% de los grupos de valor de la Supersolidaria.	Afectación grave de la integridad de la información, impacto significativo de índole legal o económica, retraso de funciones o genera pérdida de imagen severa de la Supersolidaria.	80%
	Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto de la Entidad.	Afectación de una (1) semana, hasta dos (2) semanas en la Disponibilidad de la Información	
	Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	Afecta la información clasificada y reservada de un sistema de información.	
CATASTRÓFICO	Afectación en un valor igual o superior al 50 % de los grupos de valor de la Supersolidaria.	Afectación muy grave de la integridad de la información, así como a un impacto negativo de índole legal o económico, retraso de funciones o genera pérdida de imagen severa de la Supersolidaria, además no puede repararse.	100%
	Afectación en un valor igual o superior al 50 % del presupuesto de la Entidad.	Afectación de más de (2) semanas en la disponibilidad de la información	
	Afectación muy grave del medio ambiente que requiere mas de 3 años de recuperación.	Afectación de la confidencialidad información clasificada y reservada de las organizaciones solidarias o personas con las que interactúa en la Supersolidaria.	

Tabla 4*. Criterios para calificar el impacto de riesgos de seguridad digital.*

9. Zona de riesgo

La Supersolidaria tendrá cuatro (4) zonas de riesgo (Baja, moderada, alta y extrema), las cuales 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:

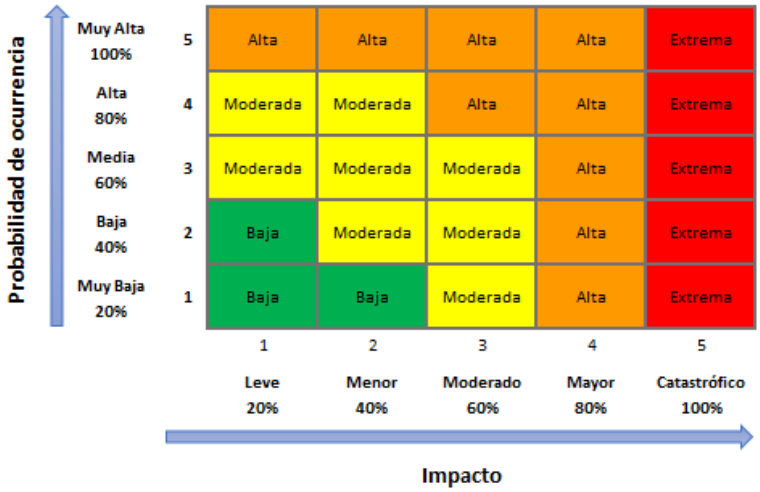

Gráfico 2. *Mapa de calor.*

10. Niveles de aceptación del riesgo

De acuerdo con los niveles de riesgo residual, se definen los criterios de nivel de aceptación, así como la estrategia de tratamiento, como se presenta a continuación.

Tipo de riesgo	Zona de riesgo residual	Estrategia de tratamiento
Riesgos de gestión y seguridad digital	**Baja**	Se ACEPTA el riesgo y se administra por medio de actividades propias del proceso o proyecto asociado.
	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo.
	Alta y extrema	Se establecen acciones de control preventivas que permitan EVITAR la materialización del riesgo.

Riesgos de Corrupción	**Baja**	Ningún riesgo de corrupción podrá ser aceptado.
	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo.
	Alta y extrema	Se adoptan medidas para: REDUCIR la probabilidad de ocurrencia, el impacto o ambos factores de riesgo. La estrategia conlleva a la implementación de controles preventivos. EVITAR Se abandonan o modifican actividades que dan lugar al riesgo. COMPARTIR con un tercero el tratamiento de una parte del riesgo para reducir la probabilidad de ocurrencia, el impacto o ambos factores.

Tabla 5. *Niveles de aceptación del riesgo.*

11. 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
Extremo		x	x	x
Alto		x	x	x
Moderado			x	
Bajo	x			

Gráfico 3. *Tratamiento de riesgos.*

Cada una de estas categorías cuenta con una estrategia, de acuerdo a lo establecido en la Tabla 5. Niveles de aceptación del riesgo.

12. Monitoreo y Seguimiento

El propósito de las actividades de monitoreo y seguimiento al reporte, es valorar la efectividad de los controles 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, a continuación, se describen las responsabilidades frente al monitoreo, seguimiento y reporte.

Línea de Defensa	Seguimiento y Monitoreo	Reporte	Periodicidad
Línea estratégica	Realiza seguimiento y monitoreo a la gestión del riesgo en las reuniones que se programen del Comité Institucional de Coordinación de Control Interno - CICCI, a través de los informes presentados por la segunda y tercera línea de defensa. En caso de ser necesario toma las decisiones a las que haya lugar.	Actas de Comité.	De acuerdo a lo dispuesto en el acto administrativo de creación del CICCI
Primera Línea de Defensa	Los líderes de proceso y sus equipos de trabajo realizan monitoreo y seguimiento a la gestión de riesgos de sus procesos y proyectos de manera permanente e informan las situaciones detectadas o materializaciones a la segunda línea de defensa a través de los formatos dispuestos.	Reporte de seguimiento, alertas tempranas y riesgos materializados a través de los formatos FT-PLES-019 Seguimiento mapa de riegos de corrupción y FT-PLES-022 Seguimiento mapa de riesgos institucionales. Este reporte debe realizarse a más tardar los primeros tres (3) días hábiles del mes siguiente.	Mensual
Segunda Línea de Defensa	Realiza monitoreo a partir del seguimiento que reporta la primera línea de defensa.	Informes de monitoreo presentados a la línea estratégica.	Trimestral (mapa de riegos institucionales) Cuatrimestral (mapa de riesgos de corrupción)

Tercera Línea de Defensa	Realiza seguimiento y evaluación a través de auditoría interna y el seguimiento reportado por la primera línea de defensa en los formatos dispuestos y los informes de monitoreo de la segunda línea de defensa.	Informes de ley y resultados del plan anual de auditoría a la línea estratégica de acuerdo a lo establecido en la norma.	De acuerdo al cronograma establecido en el Plan Anual de Auditorías (mapa de riesgos institucionales). Cuatrimestralmente (mapa de riesgos de corrupción).

Tabla 6. *Responsabilidades frente al monitoreo, seguimiento y reporte.*

Dentro del ejercicio de monitoreo, seguimiento y reporte, se deben tener en cuenta los siguientes aspectos:

Monitoreo

a. Garantizar que los controles son eficaces y eficientes en el diseño y en la ejecución.
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 del tratamiento del riesgo y establecer un orden de prioridades de acciones para el tratamiento del Riesgo.
e. Identificar nuevos riesgos que pueden surgir dentro del desarrollo de las actividades de los procesos y/o proyectos.
f. Tener en cuenta el procedimiento PR-PLES-017 Monitoreo a la gestión de riesgos

Seguimiento

a. El seguimiento de avance junto con las evidencias serán reportados por el líder de proceso y/o delegado de riesgos en cada proceso, en los formatos dispuestos por la Oficina Asesora de Planeación y Sistemas de manera mensual, dentro de los tres (3) primeros días hábiles del siguiente mes y conforme a cronograma establecido, para la revisión, análisis de la información y consolidación del informe de riesgos por parte de la segunda línea de defensa, y su posterior presentación a la línea estratégica (Alta Dirección y Comité Institucional de Coordinación de Control Interno).
b. 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.
c. 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 en la gestión de riesgos, control y gobierno”, siendo la auditoría una

herramienta de retroalimentación del Sistema de Control Interno - CI y del Modelo Integrado de Planeación y Gestión - 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.

d. La actividad de auditoría interna debe retroalimentar 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, la Oficina de Control Interno debe basarse en las evidencias obtenidas en el ejercicio de auditoría.
e. La coordinación de las auditorías (cualquiera que sea su ámbito) está en cabeza del jefe de control interno; 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 las actividades 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 e internas, áreas de mayor riesgo o modificación a los objetivos de la entidad.
f. El 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 de oportunidades de mejora en el proceso o establecimiento de planes de mejoramiento.

Reporte

a. Para el reporte de seguimiento mensual que debe realizar la primera línea de defensa, es importante aportar las evidencias en cada una de las carpetas dispuestas, ya que la relación de URL no permite muchas veces tener acceso a la información por parte de las líneas de defensa que realizan el monitoreo y seguimiento a la gestión de riesgos.
b. Los pantallazos de calendario no son válidos como evidencia, ya que no permiten evidenciar si se llevó o no a cabo la sesión, así como validar los acuerdos o temas abordados. En caso de no ser posible la grabación de memorias, se recomienda diligenciar acta de reunión en el formato dispuesto por el SIG de la SES.
c. Los reportes deben llevarse a cabo dentro de los tiempos establecidos, ya que el no cumplimiento, afecta la presentación de informes de ley en las fechas que se deben publicar.
d. De manera previa a realizar el reporte, se deben tener en cuenta las observaciones realizadas por la segunda línea de defensa en los informes de monitoreo, en aras de mejorar el reporte de seguimiento y el grado de cumplimiento de los criterios de eficacia establecidos para medir la efectividad en la ejecución de los controles.
e. Si no es posible suministrar la evidencia por el grado de criticidad establecido en el inventario de activos de información del proceso, se debe mencionar esta particularidad en el reporte.
f. Los permisos para edición a los mapas de proceso, sólo se darán a servidores que estén designados en la matriz de responsabilidades por línea de defensa.

Riesgos de corrupción

El seguimiento al mapa de riesgos de corrupción se hará a través del formato FT-PLES-019 Seguimiento mapa de riegos de corrupción, donde la primera línea de defensa hará registro del avance de cumplimiento de las acciones establecidas mensualmente, y la segunda y tercera línea de defensa cada cuatrimestre.

El Jefe de la Oficina de Control Interno, adelanta evaluación y seguimiento independiente al Mapa de Riesgos de Corrupción 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.

13. 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 participación de 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 trámites y 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 para la gestión del riesgo, asegurando que permee a la totalidad de la entidad.

Los mapas de riesgos de la Supersolidaria estarán a dispuestos para consulta por parte de nuestros grupos de valor e interés a través de la página web de la entidad http://www.supersolidaria.gov.co/es/modelo-de-control-interno y a través del software ISOLUCIÓN (Mapa de procesos/ planificación estratégica). Los ajustes que se realicen a los mapas de riesgos, deben contar con aprobación por parte del Comité Institucional de Coordinación de Control Interno, previa actualización en canales de comunicación.

Trazabilidad del riesgo

Cada riesgo lleva un código único de identificación compuesto por la sigla del proceso y un número, comenzando el primer riesgo con el #1 y en adelante en forma consecutiva a medida que se vaya incluyendo los riesgos identificados a la matriz de riesgos. En caso de eliminación de un riesgo no se asignará el código del riesgo eliminado a un nuevo riesgo, sino que se codificará de acuerdo al consecutivo que se lleve. Los códigos eliminados del mapa de riesgos vigente, quedarán registrados en la base histórica de eventos.

13.1 Comunicación interna

La comunicación interna en la entidad para la gestión de riesgos se dará a partir del esquema de 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 sus actualizaciones, así como 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 al interior de sus áreas y dar a conocer a sus colaboradores a través de los Comités Primarios, (de acuerdo al procedimiento PR-PLES-014), los avances en la gestión de riesgos en sus procesos, los controles establecidos para su mitigación y socializar las observaciones de los resultados de auditoría e informes de monitoreo; 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, realizar acompañamiento en la apropiación de la metodología para la gestión de riesgos y comunicar al Comité Institucional de Coordinación de Control Interno los resultados de monitoreo a la gestión de riesgos.

Tercera Línea de Defensa

Corresponde a la Oficina de Control Interno comunicar al Comité Institucional de Coordinación de Control Interno los resultados del seguimiento a través de los informes de auditoría y ley, frente al estado de la gestión de riesgos institucionales y retroalimentar al Comité Institucional de Gestión y Desempeño. Es importante establecer comunicación constante con la segunda línea de defensa para la articulación de la gestión de riesgos.

13.2 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.

Control de Cambios		
Versión	**Fecha**	**Observación**
0	4/junio/2020	Se aprueba documento técnico en su versión inicial y se actualizan disposiciones a través de Resolución 2020121006745 y se deroga la Resolución 2017100007035 del 29 de diciembre de 2017.
1	29/septiembre/2021	Actualización de la Política para la Administración de Riesgos de la Supersolidaria, de acuerdo a lineamientos dados por el Departamento Administrativo de la Función Pública - DAFP en la guía para la administración de riesgos y el diseño de controles en entidades públicas (versión 5) de diciembre de 2020, en la que se ajustaron los siguientes criterios: • Ajuste a objetivo y alcance. • Actualización de términos y definiciones. • Actualización de los niveles y criterios para calificar la probabilidad y el impacto. • Actualización de las zonas de riesgo - ubicación en mapa de calor. • Actualización de criterios para el tratamiento de riesgos. • Actualización de criterios para el monitoreo, seguimiento y reporte. • Actualización niveles de aceptación del riesgo. • Se incluyó información para la consulta de los mapas de riesgo por parte de los grupos de valor e interés. • Se incluyó trazabilidad del riesgo.