CÓDIGO: POCI

VERSIÓN: 02

FECHA: 25/08/2021

INDER Santander

GOBERNACION DE SANTANDER

INDERSANTANDER

Bucaramanga, Santander

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Cuadro Control de Cambios		
Versión	**Fecha**	**Descripción del Cambio**
01	11/07/2016	Emisión Inicial
02	25/08/2021	Se realizo la actualización de la política en cumplimiento de los lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, en versión 05 de diciembre de 2020 del Departamento Administrativo de la Función Pública-DAFP.

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVOS 5
   2.1 OBJETIVO GENERAL 5
   2.2 OBJETIVOS ESPECÍFICOS 5
3. ALCANCE 5
4. TERMINOS Y DEFINICIONES 6
5. POLITICA DE ADMINISTRACION DEL RIESGO 9
   5.1 LINEAMIENTOS PARA LA ADMINISTRACION DEL RIESGO 9
6. MARCO NORMATIVO 10
7. METODOLOGIA DE ADMINISTRACION DEL RIESGO 13
   7.1 IDENTIFICACIÓN DEL RIESGO 14
      7.1.1 IDENTIFICACIÓN DE RIESGOS DE PROCESOS 14
      7.1.2 QUE SE DEBE TENER EN CUENTA A LA HORA DE IDENTIFICAR LOS RIESGOS Y QUE NOS PERMITEN DETERMINAR: 14
      7.1.3 TIPOLOGÍA O CLASIFICACION DE LOS RIESGOS 15
      7.1.4 DESCRIPCIÓN DEL RIESGO 16
   7.2 NIVELES PARA IDENTIFICAR, ANALIZAR Y CALIFICAR EL RIESGO 17
      7.2.1 TABLA DE PROBABILIDAD 17
      7.2.2 TABLA DE IMPACTO 18
      7.2.3 EVALUACIÓN DE RIESGOS 19
   7.3 ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL 20
      7.3.1 TIPOS DE CONTROLES 21

7.4 RIESGO RESIDUAL 23

7.4.1 DESPLAZAMIENTO DEL RIESGO INHERENTE PARA CALCULAR EL RIESGO RESIDUAL 24

7.5 TRATAMIENTO DEL RIESGO 24

7.5.1 EL TRATAMIENTO O RESPUESTA DADA AL RIESGO, SE ENMARCA EN LAS SIGUIENTES CATEGORÍAS: 25

7.6 OPCIONES TRATAMIENTO DEL RIESGO DE LA ADMINISTRACIÓN 25

8. ACCIONES DE AVANCE Y SEGUIMIENTO A LOS RIESGOS 26

8.1. ENFOQUE BASADO EN PROCESOS 26

8.2. ACCIONES DE REPORTE 27

9. RESPONSABILIDAD Y COMPROMISOS FRENTE A LA POLITICA DE ADMINISTRACION DEL RIESGO 30

9.1. CURSOS DE ACCIÓN EN CASO DE DETECCIÓN DE LA MATERIALIZACIÓN DE LOS RIESGOS 34

10. PERIODICIDAD DEL SEGUIMIENTO 35

11. DIVULGACIÓN O PUBLICACIÓN DE LA POLÍTICA 36

1. INTRODUCCIÓN

El Decreto 1499 de 2017 establece los lineamientos para la implementación del Modelo Integrado de Planeación y Gestión, el cual es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas con el fin de generar resultados que atiendan los Planes de Desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad del servicio.

El INDERSANTANDER diseña y actualiza su Política de Administración del Riesgo de acuerdo a los parámetros del Modelo Integrado de Planeación y Gestión-MIPG en articulación con la Dimensión de Direccionamiento Estratégico, esta es aplicable a los trece (13) Procesos del Modelo Integrado de Planeación y Gestión teniendo como base lineamientos del Modelo Estándar de Control Interno-MECI, en lo que se refiere a las responsabilidades de las Línea Estratégica y Líneas de Defensa, las misma se actualiza en cumplimiento de los lineamientos de la **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas**, en versión 05 de diciembre de 2020 del Departamento Administrativo de la Función Pública-DAFP, la cual articula los Riesgos de Gestión, Riesgos de Corrupción y Riesgos de Seguridad Digital.

La Política de Administración del Riesgo del INDERSANTANDER resalta el grado de compromiso de la Entidad frente al cumplimiento de los Objetivos Estratégicos, direccionando a los procesos a asumir un pensamiento basado en riesgos, que permita anticiparse, disminuir y contrarrestar el impacto de eventos inesperados.

En la Política de Administración del Riesgo del INSTITUTO, se establece la metodología para la identificación, el análisis, la valoración, diseño de controles y el tratamiento de los riesgos que pudieran afectar el cumplimiento de su misión, así como la actuación preventiva, detectiva y correctiva para asumir, reducir y mitigar el riesgo e igualmente determina los planes de contingencia o acción, ante la materialización del riesgo.

Esta Política de Administración del Riesgo contiene los lineamientos establecidos por la alta dirección y fue socializada y aprobada en la sesión del Comité Institucional de Coordinación de Control Interno del 25 de Agosto de 2021.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer la metodología y lineamientos para la identificación, análisis, valoración, niveles de aceptación, probabilidad e impacto, niveles de responsabilidad, y tratamiento de los Riesgos de cada uno de los procesos, que conforman el MIPG del INDERSANTANDER, con el fin de definir e implementar la Política de Administración del Riesgo y los controles que permitan garantizar el cumplimiento de los objetivos institucionales del Instituto.

2.2 OBJETIVOS ESPECÍFICOS

1. Fomentar la cultura del mejoramiento continuo mediante las acciones preventivas y correctivas para la gestión del riesgo en todos los niveles del INDERSANTANDER.

2. Gestionar de forma anticipada las vulnerabilidades o eventos que puedan afectar el logro de los objetivos institucionales desde el ámbito de la gestión, corrupción y seguridad digital.

3. Cumplir con los principios del Modelo Integrado de Planeación y Gestión, los atributos de calidad y el Modelo Estándar de Control Interno.

3. ALCANCE

La Política de Administración de Riesgo es aplicable a todos los procesos que conforman, el MIPG de INDERSANTANDER y a todas las actividades realizadas por los funcionarios y contratistas durante el ejercicio de sus funciones o ejecución de sus actividades, contemplando un adecuado tratamiento de Riesgos de Gestión, Corrupción y Seguridad Digital, identificando sus factores generadores hasta el establecimiento de controles de tratamiento para los mismos.

4. TERMINOS Y DEFINICIONES

Administración del Riesgo: Un 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 institucionales. (1)

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

Control: Medida que permite reducir o mitigar un riesgo.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impacta en los procesos, la entidad, los grupos de valor y demás partes Interesadas.

Amenazas: Causa potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o a una organización

Alta Dirección: personas que ocupa un cargo de elevada responsabilidad (mandato) en una organización o gobierno y participa en el ejercicio del poder (ya sea la suya o la de su superior o el empleador, público o privado legalmente), para INDERSANTANDER la alta dirección será el Director y los Comités CIGD y CICCI.

Establecimiento del contexto: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo[1].

CICCI: Comité Institucional de Coordinación de Control Interno

CIGD: Comité Institucional de Gestión y Desempeño

MIPG: Modelo Integrado de Planeación y Gestión

MECI: Modelo Estándar de Control Interno

---

[1] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN -ICONTEC. Norma Técnica Colombiana NTCISO31000. 2011. p. 20

Identificación del Riesgo: Proceso para encontrar, reconocer y describir el riesgo[2].

Líder o Responsable del proceso: Persona con la responsabilidad y autoridad para gestionar un riesgo.

Mapa de Riesgos: Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.

Análisis de 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 cuán frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

Política: Directriz emitida por la dirección sobre lo que hay que hacer para efectuar el control.

Plan de mejoramiento: Parte del plan de manejo que contiene las técnicas de la administración del riesgo orientadas a prevenir, evitar, reducir, dispersar, transferir o asumir riesgos.

Probabilidad: Probabilidad de ocurrencia del riesgo.

Impacto: Las consecuencias que pueden ocasionar a la organización la materialización del riesgo.

Riesgo: Efecto que causa sobre los objetivos de la entidad, debido a eventos potenciales.

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

---

[2] Ibid. p. 21

Auditoría Interna: Es un examen sistemático, objetivo e independiente de los procesos, actividades, operaciones y resultados de una Entidad Pública.

Autoevaluación del Control: Elemento de Control que basado en un conjunto de mecanismos de verificación y evaluación determina la calidad y efectividad de los controles internos a nivel de los procesos y de cada área organizacional responsable, permitiendo emprender las acciones de mejoramiento del control requeridas. Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún eficaces y apropiados.

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

Riesgo de Corrupción: La posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular[3].

Riesgos 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. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

TIC: Tecnologías de la Información y las Comunicaciones.

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

Factores de riesgo: Son las fuentes generadoras del riesgo.

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

---

[3] PRESIDENCIA DE LA REPÚBLICA/DEPARTAMENTO NACIONAL DE PLANEACIÓN/DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Estrategias para la construcción del plan anticorrupción y de atención al ciudadano. Bogotá. 2012. p.9

5. POLITICA DE ADMINISTRACION DEL RIESGO

El INDERSANTANDER, se compromete a construir el Mapa de Riesgos de Gestión, Corrupción y Seguridad Digital y adelantar el tratamiento mediante la implementación de una metodología de evaluación, monitoreo y seguimiento de forma periódica, identificando y administrando eventos potenciales que puedan afectar el adecuado funcionamiento de los procesos y el cumplimiento de metas en la entidad.

Las actividades relacionadas con la administración del Riesgo de Corrupción se revisarán cuatrimestralmente y para el caso de riesgos de Gestión y Seguridad Digital, semestralmente; la línea estratégica podrá determinar revisiones extraordinarias en aquellos casos en que se presenten cambios organizacionales o del entorno que puedan comprometer la gestión institucional.

El Área Administrativa y Financiera es la encargada de liderar la elaboración y consolidación de la Matriz de riesgos por procesos, el mapa de Riesgos de Corrupción y Seguridad Digital.

La Oficina de Control Interno deberá presentar Periódicamente un informe al Director y a los responsables de los Procesos respecto al estado de las Acciones establecidas para mitigación de los Riesgos identificados por Gestión, Corrupción y Seguridad Digital.

5.1 LINEAMIENTOS PARA LA ADMINISTRACION DEL RIESGO

Para la adecuada gestión del riesgo en el INSTITUTO, se presentan los siguientes lineamientos:

- Se establecerá la metodología que permita identificar, analizar, valorar y administrar los riesgos de gestión, corrupción y seguridad digital, que se puedan presentar en el desarrollo de las actividades que dan cumplimiento a la misión del INDERSANTANDER y su posterior tratamiento, manejo, monitoreo y seguimiento de los riesgos, para que no afecten los objetivos institucionales.

- Asegurar los recursos necesarios para ayudar a los responsables a gestionar y tratar los riesgos a su cargo.

- Los riesgos del INDERSANTANDER, se evalúan de acuerdo a los niveles de calificación de la probabilidad e impacto, definidos en la presente política.

- Los riesgos identificados en el INDERSANTANDER, deberán ser monitoreados cuatrimestralmente en referencia a los riesgos de Corrupción y semestralmente para los riesgos de Gestión y Seguridad Digital, para asegurar que sus controles sean eficaces y eficientes, y así obtener información oportuna, para mejorar la evaluación y gestión de los riesgos.
- La tolerancia es el nivel de riesgo que el INDERSANTANDER, está dispuesto a soportar, que corresponde a los riesgos que se encuentren en zona residual baja y los que se encuentren en otra zona se trataran de acuerdo al numeral 7.2.3 de la presente política.
- Los niveles de responsabilidad sobre periodicidad de seguimiento y evaluación de los riesgos estarán plasmados en el numeral 7.2, 7.2.3 ,10 y 11 de esta política.
- Comunicar internamente los resultados de la gestión del riesgo desarrollada institucionalmente.
- Los mecanismos de comunicación utilizados para dar a conocer la presente Política de Administración del Riesgo en todos los niveles de la entidad, están plasmados en el numeral 11.

6. MARCO NORMATIVO

NORMATIVIDAD	ARTICULO	CONTENIDO
LEY 87 DE 1993	ART. 2	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). Artículos 2 OBJETIVOS DEL CONTROL INTERNO: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

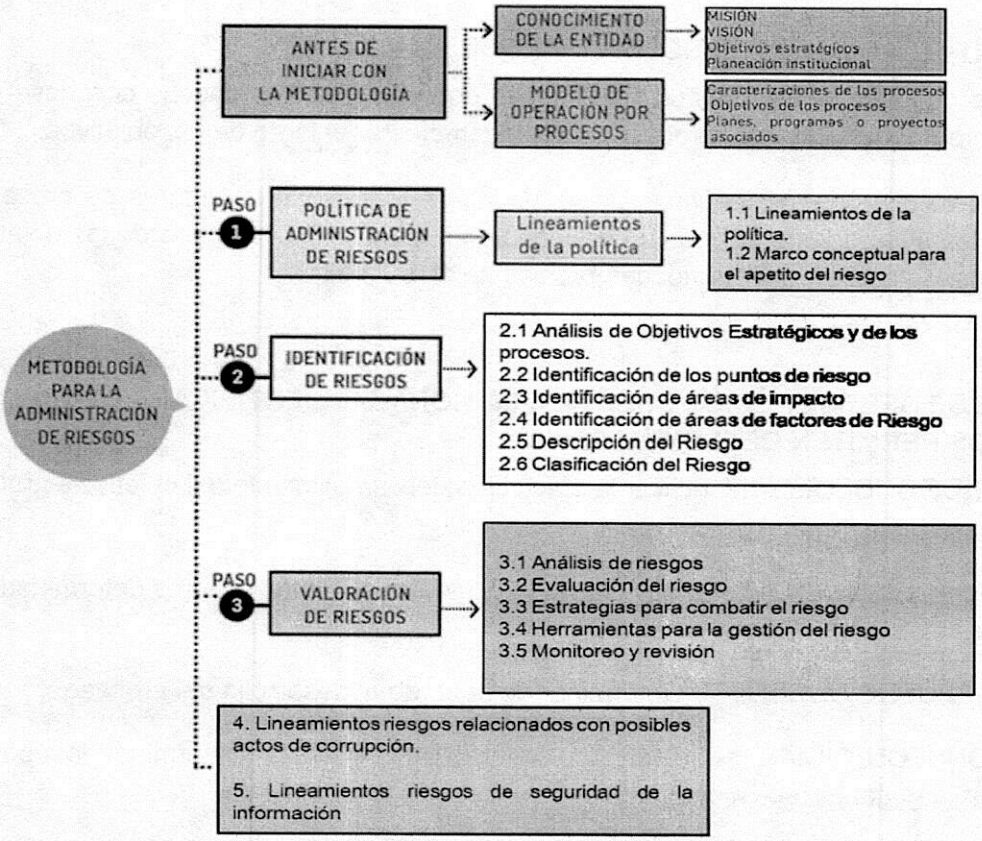
NTC GTC137	Numeral 3.7.1.6	Vocabulario gestión del Riesgo
LEY 489 DE 1998	CAPITULO VI.	Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Referente al Sistema Nacional de Control Interno.
DIRECTIVA PRESIDENCIAL 09 DE 199		Lineamientos para la implementación de la política de lucha contra la corrupción.
la Ley 1474 de 2011	Art .8	Por el cual se dictan normas sobre el Sistema Nacional de control Interno de la Entidades y Organismos de la Administración Publica del Orden Nacional y territorial y se dictan otras disposiciones. (Modificado parcialmente por el Decreto 2593 del 2000 y por el Art .8 de la Ley 1474 de 2011).
LEY 1474 DE 2011 ESTATUTO ANTICORRUPCIÓN	ART. 73	Plan Anticorrupción y de Atención al Ciudadano: Señala la obligatoriedad para cada entidad del orden nacional, departamental y municipal de elaborar anualmente una estrategia de lucha contra la corrupción y las medidas para mitigar estos riesgos. Al Programa Presidencial de Modernización, Eficiencia, Transparencia, le corresponde diseñar la metodología para elaborar el Mapa de Riesgos de Corrupción.
DECRETO 4637 DE 2011 SUPRIME Y CREA UNA SECRETARÍA EN EL DAPRE	ART. 2	Crea la Secretaría de Transparencia en el Departamento Administrativo de la Presidencia de la República.
	ART. 4	Suprime el Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la corrupción.
DECRETO 1469 DE 2014. MODIFICACIÓN DE LA	ART. 15	Funciones de la Secretaría de Transparencia: 13) Señalar la metodología para diseñar y hacer seguimiento a las estrategias de lucha contra la corrupción y atención al ciudadano que deber tan elaborar anualmente las entidades del orden nacional y territorial.

ESTRUCTURA DEL DAPRE		
DECRETO 1081 DE 2015 ÚNICO DEL SECTOR DE LA PRESIDENCIA DE LA REPUBLICA	ART. 2.1.4.1 y siguientes	Señala como metodología para elaborar la estrategia de lucha contra la corrupción la contenida en el documento "Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano"
LEY 1712 DE 2014. LEY DE TRANSPARENCIA Y DE ACCESO A LA INFORMACIÓN PÚBLICA	ART. 9	Literal g) Deber de publicar en los sistemas de información del Estado o herramientas que lo sustituyan el Plan Anticorrupción y de Atención al Ciudadano.
GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS	Versión 05 de Diciembre de 2020	El Departamento Administrativo de la Función Pública, como entidad técnica, estratégica y transversal del Gobierno nacional, pone a disposición de las entidades la metodología para la administración del riesgo. En esta versión 5 se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo. Es importante resaltar que se mantiene la estructura general bajo tres pasos principales, los cuales fundamentan la estructura metodológica que desde las primeras versiones de la guía se ha venido desarrollado.
ISO 31001:2018 GESTION DEL RIESGO - DIRECTRICES		Este documento está dirigido a las personas que crean y protegen el valor en las organizaciones gestionando riesgos, tomando decisiones, estableciendo y logrando objetivos y mejorando el desempeño.

7. METODOLOGIA DE ADMINISTRACION DEL RIESGO

Para administrar los riesgos del INDERSANTANDER, se adoptará la metodología vigente propuesta por el Departamento Administrativo de la Función Pública; en virtud de esta se desarrolla el siguiente esquema que nos brinda la información más relevante en el proceso de la identificación de riesgos al que está expuesta la entidad.

Figura 1



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Fuente: Adaptada Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, en versión 05 de diciembre de 2020, página 20.

7.1 IDENTIFICACIÓN DEL RIESGO

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control del INSTITUTO, teniendo en cuenta el contexto estratégico en el que opera la Entidad, la caracterización de los trece (13) procesos que conforman el Modelo Integrado de Planeación y Gestión - MIPG, que contempla su objetivo y alcance, y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos. Para ello se contemplan los siguientes factores:

7.1.1 IDENTIFICACIÓN DE RIESGOS DE PROCESOS

La Entidad adelanta la identificación del riesgo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos.

El principal objetivo de la identificación del riesgo es lograr que los líderes de procesos, conozcan los eventos que podrían tener impacto en el logro de cada uno de los objetivos estratégicos, de procesos y actividades propias del INSTITUTO.

7.1.2 QUE SE DEBE TENER EN CUENTA A LA HORA DE IDENTIFICAR LOS RIESGOS Y QUE NOS PERMITEN DETERMINAR:

¿QUÉ PUEDE SUCEDER? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.

¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factores determinados en el contexto.

¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo al desarrollo del proceso.

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar los posibles efectos por la materialización del riesgo.

Con el fin de facilitar la identificación de riesgos de procesos, se presenta a continuación el espacio que se maneja en el formato **"Mapa de Riesgos"** para el desarrollo de este paso:

7.1.3 TIPOLOGÍA O CLASIFICACION DE LOS RIESGOS

Con el fin de formular políticas de operación y en el proceso de identificación del riesgo, se debe hacer una clasificación, para darles el tratamiento indicado a los riesgos que se gestionan en el INDERSANTANDER, lo cuales se encuentran clasificados en:

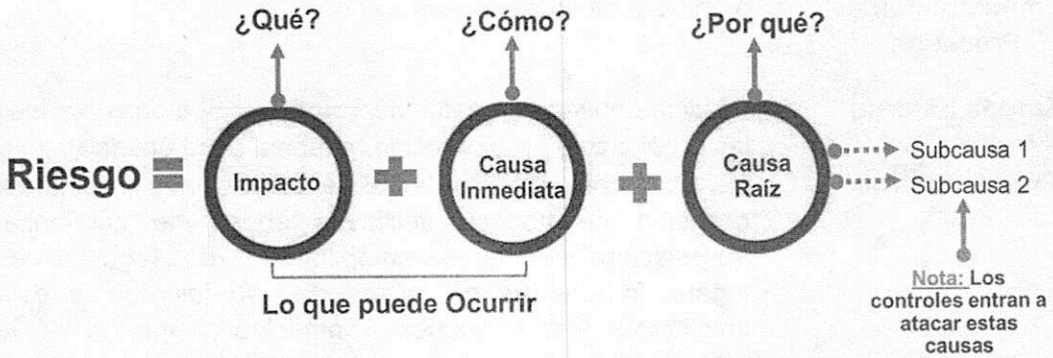
CLASES DE RIESGOS	
RIESGO	**DEFINICIÓN**
Ejecución y Administración de Procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude Externo	Pérdida derivada de actos de fraude por personas ajenas a las organización (no participa personal de la entidad).
Fraude Interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad, en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas Tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones Laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación
Usuarios, Productos y Prácticas Organizacionales	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños Activos Físicos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos.

7.1.4 DESCRIPCIÓN DEL RIESGO

La descripción del riesgo debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento, tanto para el líder del proceso en el INDERSANTANDER, como para personas ajenas al proceso.

Se propone una estructura que facilita su redacción y claridad se inicia con la frase **POSIBILIDAD DE** y se analizan los siguientes aspectos:

Figura 2



Fuente: Adaptada Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, en versión 05 de diciembre de 2020, página 32.

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

Impacto: Son las consecuencias que puede ocasionar a la Entidad la materialización del riesgo.

Causa Inmediata: Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o sub-causas que pueden ser analizadas.

7.2 NIVELES PARA IDENTIFICAR, ANALIZAR Y CALIFICAR EL RIESGO

Los líderes y sus equipos de trabajo luego de identificar los riesgos de procesos, Corrupción y Seguridad Digital, deben establecer el nivel de riesgo, la determinación de su probabilidad de ocurrencia y el impacto de sus consecuencias. El análisis de la creación puede adoptarse por medio de datos históricos existentes, o bien, a partir del conocimiento y experiencia de los funcionarios y contratistas que participan en el análisis. Las etapas que deben seguirse como parte de la evaluación y calificación de Riesgos corresponden a:

Determinación de la Probabilidad; se entiende la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o factibilidad, así:

7.2.1 TABLA DE PROBABILIDAD

El nivel de probabilidad, estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando en el INDERSANTANDER, es decir el número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la siguiente tabla se establecen los criterios para definir el nivel de probabilidad:

Para su determinación se utiliza la siguiente tabla de probabilidad:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 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%

Fuente: Adaptada Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, en versión 05 de diciembre de 2020, página 39.

7.2.2 TABLA DE IMPACTO

El impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

Para la definición de la tabla de criterios se definen impactos **ECONÓMICOS** y **REPUTACIONALES** como variables principales, ya que se encontrara situaciones tales relacionadas con : afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, temas todos que se agrupan en impacto económico y reputacional.

Cuando se presenten ambos impactos para un riesgo, tanto **ECONÓMICO** como **REPUTACIONAL**, los cuales tienen diferentes niveles, se debe tomar el más alto.

A continuación, se presenta los diferentes criterios para definir el nivel de impacto:

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Adaptada Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, en versión 05 de diciembre de 2020, página 40.

7.2.3 EVALUACIÓN DE RIESGOS

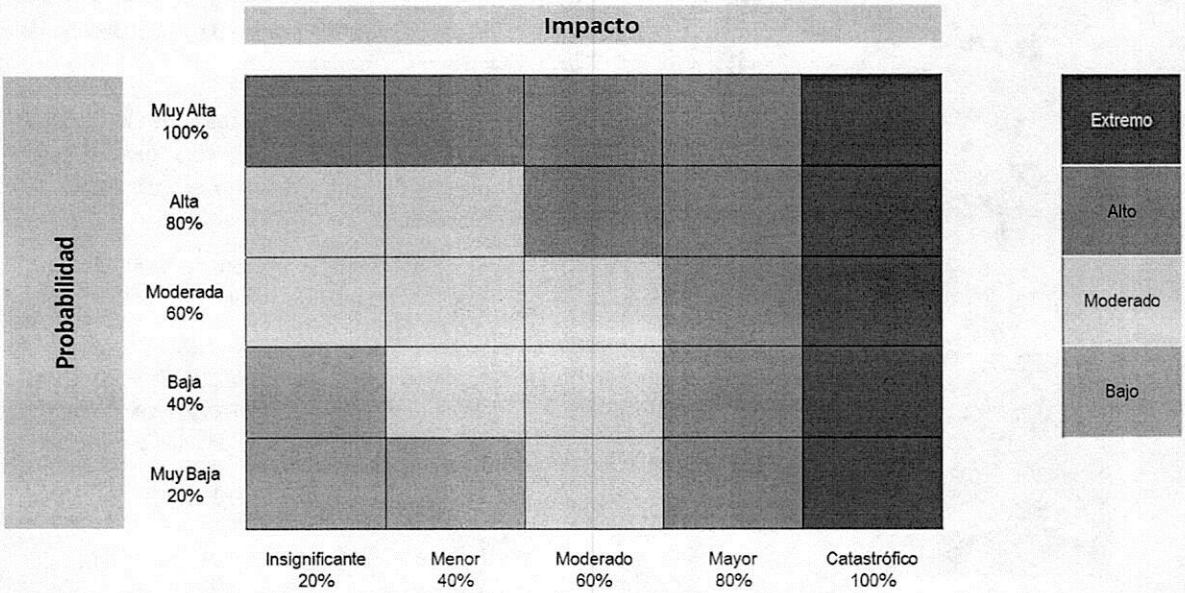
A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Calificación = Impacto x Probabilidad

En general, en el análisis del riesgo se determina la gravedad del riesgo en la entidad, esto se realiza al terminar la identificación, calificación y evaluación del riesgo. Se recomienda

utilizar la matriz de priorización que permite determinar cuáles riesgos requieren de un tratamiento inmediato:

Análisis preliminar (riesgo inherente): Se trata de determinar los niveles de severidad, a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.



Fuente: Adaptada Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, en versión 05 de diciembre de 2020, página 42.

7.3 ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL

Para una adecuada redacción del control se propone la siguiente estructura:

De acuerdo a la metodología es indispensable ejecutar los siguientes pasos enunciados a continuación, en aras de contar con adecuada planeación y formulación de los controles:

1. **Responsable de ejecutar el control:** Identifica el cargo del servidor que ejecuta el control, en caso se ser controles automáticos se identificará el sistema que realiza la actividad.
2. **Acción:** Se determina mediante verbos en los cuales se identifica la acción a realizar como parte del control.

3. Complemento: Corresponde a los detalles que permiten identificar claramente el objeto del control (plan de acción, responsable, fecha de implementación, fecha de seguimiento, seguimiento y estado).

7.3.1 TIPOS DE CONTROLES

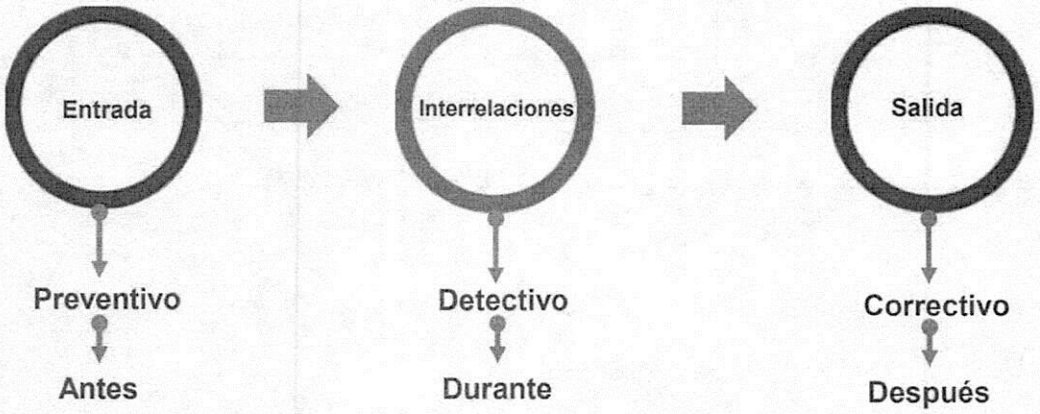
Acorde con lo anterior tenemos las siguientes tipologías de controles:

Control Preventivo: Acción y/o mecanismo ejecutado antes que se realice la actividad originadora del riesgo, se busca establecer condiciones que aseguren el resultado final esperado. En general estos controles actúan sobre las causas del riesgo.

Control Detectivo: Acción y/o mecanismo ejecutado que permite detectar el riesgo durante la ejecución del proceso y puede disminuir la materialización de dicho riesgo.
Estos controles detectan el riesgo, pero genera reprocesos.

Control Correctivo: Acción que se ejecutan después de que se materializa el riesgo y en la mayoría de ocasiones permiten reducir el impacto de dicho riesgo.

A través de la cadena de valor de los procesos puedo establecer cuando se activa el control y por lo tanto establecer su tipología con mayor precisión:



Así mismo, de acuerdo a la forma como se ejecutan tenemos:

Control Manual: Controles que son ejecutados por una persona, tiene implícito el error humano

Control Automático: Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta los lineamientos establecidos en la guía de administración del riesgo, es fundamental señalar que los atributos permiten un impacto del tratamiento y ponderación, mediante los controles de un máximo del 50% de acuerdo a la formulación del Departamento Administrativo de la Función Pública y sus características relacionadas con la eficiencia y la formalización.

En la tabla que se muestra a continuación puede observar el propósito, desviación, descripción y peso asociados, a cada uno así:

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la	25%

Características			Descripción	Peso
			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

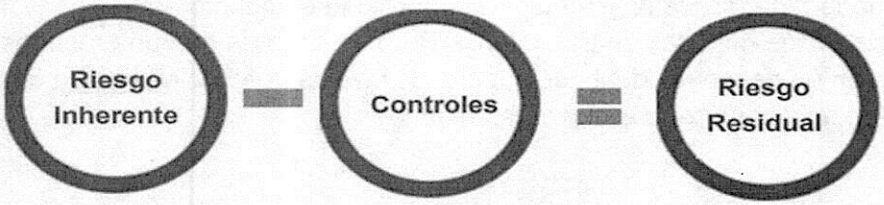
Fuente: Adaptada Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, en versión 05 de diciembre de 2020, página 45 y 46.

7.4 RIESGO RESIDUAL

El riesgo residual es aquél que permanece después de que la primera Línea de Defensa desarrolle sus respuestas a los riesgos. El riesgo residual refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la alta dirección para mitigar el riesgo inherente.

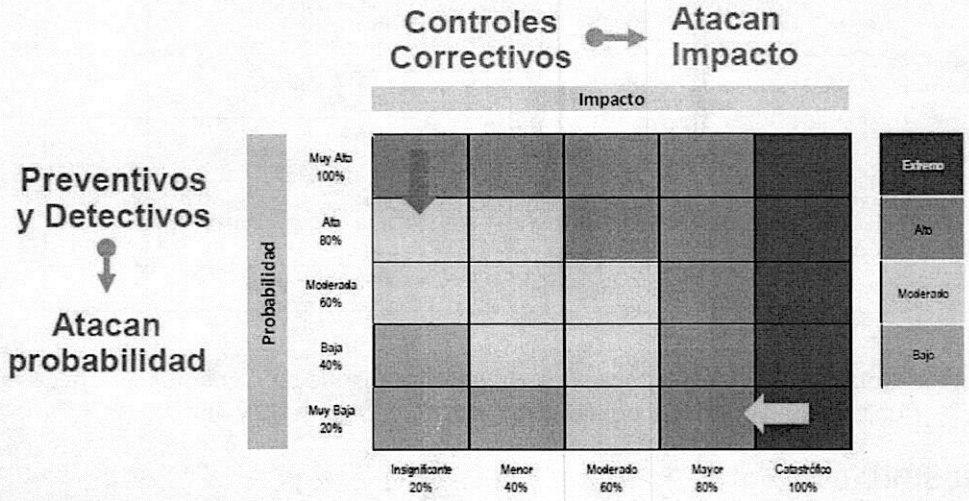
Riesgo Residual

El resultado de aplicar la efectividad de los controles al riesgo inherente, nos determina el riesgo residual.



7.4.1 DESPLAZAMIENTO DEL RIESGO INHERENTE PARA CALCULAR EL RIESGO RESIDUAL

Una vez realizado el análisis y evaluación de los controles para la mitigación de riesgos, procedemos a la elaboración del mapa de riesgos residual, para ello debemos identificar si los controles reducen la probabilidad o el impacto, para así reducir porcentualmente cada variable.



La metodología establece que los controles mitigan el riesgo de forma acumulativa. Opera una política de reducción máxima del 50% para los controles.

7.5 TRATAMIENTO DEL RIESGO

Es la respuesta establecida por la Primer Línea de Defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de Corrupción.

Los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo, derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento.

7.5.1 EL TRATAMIENTO O RESPUESTA DADA AL RIESGO, SE ENMARCA EN LAS SIGUIENTES CATEGORÍAS:

Aceptar el Riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).

Compartir el Riesgo: Se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo. Los dos principales métodos de compartir o transferir parte del riesgo.

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.

Evitar el Riesgo: Se estudia a profundidad el cese de las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo o estableciendo controles eficaces que no permitan la materialización del mismo.

7.6 OPCIONES TRATAMIENTO DEL RIESGO DE LA ADMINISTRACIÓN

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
Riesgos de Gestión (*Estratégicos, gerenciales, operativos, financieros, tecnológicos, de cumplimiento y de Imagen)*	Baja	Se ***ACEPTA*** el riesgo y se administra por medio de las actividades propias del proceso, igual debe existir un seguimiento continuo del riesgo.
	Moderada	Se establecen acciones de control preventivas que permitan ***REDUCIR***, la probabilidad e impacto de ocurrencia de este riesgo.
Riesgos de Seguridad Digital	Alta y Extrema	Se puede optar por un Plan de Acción, Acción Preventiva o cambio de controles para reducir, evitar y compartir la ocurrencia y consecuencia del riesgo.

Riesgos de Corrupción	Baja	Ningún riesgo de corrupción podrá ser aceptado.
	Moderada	Ningún riesgo de corrupción podrá ser aceptado, implementar controles para reducir, evitar y compartir.
	Alta y Extrema	Ningún riesgo de corrupción podrá ser aceptado implementar controles para reducir, evitar y compartir.

8. ACCIONES DE AVANCE Y SEGUIMIENTO A LOS RIESGOS

8.1. ENFOQUE BASADO EN PROCESOS

El avance y seguimiento a los riesgos de la Entidad, se efectúa a través del enfoque basado por procesos.

8.2. ACCIONES DE REPORTE

Tipo de Riesgo	Responsable	Acción
Riesgos de Gestión, Corrupción y Seguridad Digital	LIDERES DE LOS PROCESOS	Revisar y reportar al Área Administrativa y Financiera (CPS de MIPG), el estado de operación y avance de los controles y plan de acción del mapa de riesgo, junto con los soportes que evidencian el respectivo avance, evitando incumplimientos de los procesos y los eventos en los que se han materializado los riesgos en la entidad. Para tal fin, se debe reportar mediante el diligenciamiento del formato FOCI13 Seguimiento al mapa de riesgo. El cual se encuentra anexo. **Reporte avance riegos de corrupción:** • Los primeros 3 días hábiles del mes de Mayo, Septiembre y Enero del siguiente año. **Reporte avance de riesgos de gestión:** • Los primeros 3 días hábiles del mes Julio y Enero del siguiente año.
	TICS	1. Asesorar a la primera línea en la identificación y valoración de los riesgos de seguridad digital que puedan afectar los objetivos de sus procesos a cargo. 2. Asesorar a la primera línea en la definición y aplicación de controles que buscan mitigar los riesgos de seguridad digital identificados.

		3. Apoyar al Área Administrativa y Financiera (CPS de MIPG), en el monitoreo de los riesgos de seguridad digital identificados y los controles establecidos por la primera línea. 4. Apoyar al Área Administrativa y Financiera (CPS de MIPG), en la evaluación conjuntamente con la primera línea de defensa, de los riesgos identificados en los mapas de riesgo. **Reporte avance riegos de corrupción:** • Los primeros 3 días hábiles del mes de Mayo, Septiembre y Enero del siguiente año. **Reporte avance de riesgos de gestión:** • Los primeros 3 días hábiles del mes Julio y Enero del siguiente año.
	ÁREA ADMINISTRATIVA Y FINANCIERA (CPS MIPG)	Adelantar el monitoreo a los controles implementados en la primera línea de defensa y evaluar su cumplimiento, así como asesorar en caso de materialización de los riesgos la ejecución de los planes de acción. Consolidar el informe de gestión y avance de las acciones de los mapas de riesgos por proceso y reportar de forma consolidada al jefe de la oficina de control interno reportando el formato FOCI13 Seguimiento al mapa de riesgo, así **Reporte avance riegos de corrupción:**

		• Los primeros 5 días hábiles del mes de Mayo, Septiembre y Enero del siguiente año. **Reporte avance de riesgos de gestión:** • Los primeros 5 días hábiles del mes Julio y Enero del siguiente año.
	CONTROL INTERNO	Realizar el seguimiento a las acciones de control establecidas por los procesos para la mitigación de riesgos y los planes de acción, verificando que se realicen de manera oportuna cerrando las causas del problema, con el fin de evitar en lo posible la repetición de hallazgos o materialización de riesgos. Revisar que se hayan identificado riesgos significativos que afectan el cumplimiento de los objetivos de los procesos incluyendo los de corrupción, permitiendo adecuar el diseño y ejecución de controles y que la calificación del impacto o probabilidad del riesgo sea coherente con los resultados de las auditorías realizadas. Realizar recomendaciones y seguimiento para el fortalecimiento de los controles y en caso de que se requiera sugerir la actualización de los mapas de riesgo. **Reporte avance riegos de corrupción:** • Los primeros 10 días hábiles del mes de Mayo, Septiembre y Enero del siguiente año.

		Reporte avance de riesgos de gestión: • Los primeros 10 días hábiles del mes Julio y Enero del siguiente año.

9. RESPONSABILIDAD Y COMPROMISOS FRENTE A LA POLITICA DE ADMINISTRACION DEL RIESGO

LINEAS DE DEFENSA	RESPONSABLES	RESPONSABILIDAD FRENTE AL RIESGO
Estratégica	Director y Comité Institucional de Coordinación de Control Interno	**1.** Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. **2.** Analizar los cambios en el entorno (Contexto Interno y Externo), que puedan tener un impacto significativo en la operación de la entidad. **3.** Realimentar al CIGD, CICI sobre los ajustes que se deban hacer en la entidad sobre la Gestión del Riesgo (Cuatrimestral, antes de adelantarse el comité de coordinación de control interno). **4.** Revisar los informes de riesgos presentados por el Jefe de la Oficina de Control Interno.

		5. Revisar los planes de acción establecidos para cada uno de los riesgos, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la materialización de los mismo. **6.** Aprobar la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.
Primera Línea	Líderes de los procesos	1. Identificar y valorar los riesgos que puedan afectar los objetivos de su proceso a cargo, y hacer una actualización continua de los mismos. 2. Definir, aplicar y realizar mejoramiento continuo, a los controles para mitigar los riesgos identificados, alineados con las metas y objetivos de la entidad. 3. Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar la deficiencia de los controles y determinar las acciones de mejora que haya lugar. 4. Informar de forma cuatrimestral y semestral al Área Administrativa y Financiera (CPS de MIPG), como Segunda Línea de defensa, sobre los avances de las acciones de control de los riegos de su proceso, teniendo en

		cuenta lo establecido en el numeral 8.2 del presente documento.
Segunda Línea	Área Administrativa y Financiera (CPS MIPG)	1. Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. 2. Presentar al jefe de control interno el monitoreo a la eficacia de los controles. 3. Asesorar y Supervisar que la primera línea identifique, evalué y gestione los riesgos y controles, para que se efectúen acciones de mejora. 4. Identificar cambios en los niveles de aceptación del riesgo en la entidad, especialmente de los riesgos ubicados en zona baja y presentarlo para aprobación del Comité Institucional de Coordinación de Control Interno (CICCI) 5. Monitorear de forma cuatrimestral, los riesgos de corrupción y semestralmente los de gestión y seguridad digital, identificados y los controles establecidos, por la primera línea de defensa. 6. Evaluar conjuntamente con la primera línea de defensa, que los riesgos sean consistentes, con la presente política. 7. Presentar ante el Comité Institucional de Gestión y Desempeño-MIPG, las

		acciones de mejora propuestas por los líderes de los procesos. 8. Asesorar, orientar y capacitar a los líderes de los procesos, en identificación, análisis y valoración del riesgo y definición de controles. 9. Garantizar capacitación a los líderes de procesos en la metodología de implementación de gestión del riesgo.
Tercera Línea de Defensa	Jefe de Control Interno	1. Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y los controles, con énfasis en el diseño e idoneidad de los controles establecidos por los procesos. 2. Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. 3. Llevar a cabo el seguimiento de los riesgos consolidados y reportar los resultados al Comité Institucional de Coordinación de Control Interno (CICCI). 4. Recomendar mejoras a la política de administración del riesgo.

9.1. CURSOS DE ACCIÓN EN CASO DE DETECCIÓN DE LA MATERIALIZACIÓN DE LOS RIESGOS

Riesgos de Gestión, Corrupción y seguridad digital	Líder de Proceso	Informar a la línea estratégica el hecho encontrado. Realizar la respectiva denuncia ante la instancia de control pertinente. Identificar las acciones correctivas necesarias y documentarlas en un plan de mejoramiento Actualizar mapa de riesgos.
	Área Administrativa y Financiera (CPS MIPG)	Informar al líder del proceso, quien analizará la situación y definirá las acciones a quien haya lugar. Dar lineamientos para que se implementen las acciones correspondientes, con el líder del proceso para la revisión y ajuste del mapa de riesgos. Informar a la alta gerencia de la materialización del riesgo.

	Oficina de Control Interno	Informar al líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar. Realizar la respectiva denuncia ante la instancia de control pertinente. Informar a la segunda línea de defensa con el fin de dar inicio a las acciones correspondientes, con el líder del proceso para la revisión y ajuste del mapa de riesgos. Aprobar el plan de mejoramiento interno suscrito y realizar el seguimiento del mismo.

10. PERIODICIDAD DEL SEGUIMIENTO

Con el fin de lograr un esquema articulado de comunicación entre las líneas de defensa para el seguimiento a riesgos se establecen los siguientes periodos para realizarlo de acuerdo a las responsabilidades y competencias en el Sistema de Control Interno, así:

Riesgos de Corrupción:

El seguimiento se realiza cuatrimestralmente por Control Interno a todos los procesos tres (3) veces al año, de acuerdo a la información presentada por las líneas de defensa, en las siguientes fechas:

Primer seguimiento: Con corte al **30 de abril**. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo.

Segundo seguimiento: Con corte al **31 de agosto**. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre.

Tercer seguimiento: Con corte al **31 de diciembre**. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero.

Riesgos de Gestión y Seguridad Digital:

Semestral: Línea Estratégica, Primera y Segunda adelantara seguimiento semestral y la Tercera Línea de Defensa de acuerdo a la priorización en el Plan Anual de Auditorias

Primer seguimiento: La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de Agosto.

Segundo seguimiento: La publicación deberá surtirse dentro de los diez (10) primeros días hábiles de Diciembre.

El seguimiento adelantado por la oficina de Control Interno, se deberá publicar en la página web de la entidad o en lugar de fácil acceso al ciudadano.

11. DIVULGACIÓN O PUBLICACIÓN DE LA POLÍTICA

La Política de Administración de Riesgos deberá ser divulgada oficialmente a todos los funcionarios y contratistas del INDERSANTANDER. De igual manera deberá ser incorporada y explicada en los procesos de inducción y reinducción efectuados por la entidad al momento de la vinculación de los funcionarios y contratistas.

La publicación de la política será efectuada en el link de MIPG ubicado en la página web oficial de INDERSANTANDER y en la herramienta institucional Dropbox.

PEDRO BELÉN CARRILLO CÁRDENAS
Director

Elaboró: Erika Lizeth Ariza Pinto-CPS MIPG.
Revisó: María Amparo Castellanos Amado – P.U. Administrativa y Financiera.
Aprobó: Comité Institucional de Coordinación de Control Interno.