ACUERDO 17 DE 2018
MANUAL DE POLÍTICAS DEL SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO DEL INFIDER

SARO

TABLA DE CONTENIDO

ACUERDO NÚMERO 17

(Junio 27 de 2018)

Por el cual se adopta el Manual de Políticas del Sistema de Administración de Riesgo Operacional, SARO, del Instituto de Fomento para el Desarrollo de Risaralda, Infider, y se dictan otras disposiciones

La Junta Directiva del Instituto de Fomento para el Desarrollo de Risaralda, Infider, en uso de sus atribuciones legales y en especial las conferidas por la Ordenanza número 023 del 7 de mayo de 2002, y

CONSIDERANDO:

- Que en el numeral 13 del artículo 11 de la Ordenanza 023 de mayo 7 de 2002 se define como función de la Junta Directiva del Instituto verificar el cumplimiento de las políticas señaladas a la Administración y el adecuado funcionamiento del Instituto.

- Que la entidad no cuenta con un manual de políticas de administración de riesgo operacional.

- Que la Superintendencia Financiera de Colombia, en adelante SFC, mediante la Circular Externa 034 del 2 de diciembre de 2013, imparte las instrucciones relativas al régimen especial de control y vigilancia aplicable a los institutos de fomento y desarrollo de las entidades territoriales que pretendan administrar excedentes de liquidez.

- Que conforme a lo estipulado en el Capítulo XXIII, Reglas relativas al Sistema de Administración de Riesgo Operativo, numeral 6.4.1 de la Circular 100 de 1995 - Básica Contable y Financiera de la SFC, la Junta Directiva debe definir y aprobar las políticas de la entidad en materia de administración del riesgo de liquidez.

- Que en la Parte II Título V Capítulo II numeral 2.1.4 de la Circular 029 de 2014- Básica Jurídica de la SFC, establece: *2.1.4 Manual de las actividades objeto de supervisión que pretenda desarrollar, en el cual se detalle la forma de operación de la entidad para adelantar la respectiva actividad, de acuerdo con lo previsto en el presente Capítulo. Así mismo, se deben detallar los roles y responsabilidades del (de las) área(s) encargada(s) de las actividades supervisadas, así como el manual de funciones de las personas responsables de las mismas.*

- Que en la Parte II Título V Capítulo II numeral 2.2.2.1.4 de la Circular 29 de 2014, Básica Jurídica de la SFC, se establece como función del consejo directivo u órgano quien haga

sus veces, aprobar las políticas para la ejecución de las actividades objeto de supervisión.

- Que la entidad considera pertinente acatar las instrucciones de la norma de la Superfinanciera Parte II, Título V, Capítulo II de la Circular 29 de 2014, Básica Jurídica de la SFC, los infis, con la finalidad de adaptarse a las nuevas condiciones y cultura de la gestión de riesgo en el sector.

- Que, en el desarrollo de su objeto social, el Infider se encuentra expuesto a riesgo operativo como consecuencia de una posible pérdida potencial ocasionada por eventos de fraude interno, fraude externo, fallas e interrupción de los sistemas, estructura física y procesos.

- Que el presente documento se viene trabajando desde vigencias anteriores y tiene como objeto la aprobación, adopción e implementación de las políticas del Sistema de Administración del Riesgo Operativo.

- Que la SFC es la entidad encargada de la supervisión y vigilancia de las actividades financieras en nuestro país, incluyendo la supervisión de algunas actividades adelantadas por los infis, y con el propósito de hacer más responsable el proceso, ha generado gran interés por el manejo de los diferentes riesgos presentados en el ejercicio de las funciones de los diferentes entes regulados.

- Que, por lo descrito anteriormente, y teniendo en cuenta la naturaleza del Instituto, el tamaño y la complejidad de las operaciones que se realizan, se hace necesario la adopción de las Políticas del Sistema de Administración del Riesgo Operativo.

ACUERDA:

ARTÍCULO 1°. ADOPCIÓN
Adoptar el Manual de Políticas del Sistema de Administración de Riesgo Operativo, SARO, del Instituto de Fomento para el Desarrollo de Risaralda, Infider.

ARTÍCULO 2°. OBJETIVO
Desarrollar e implementar en el Infider el Sistema de Administración de Riesgo Operacional, SARO, que contribuya al mejoramiento continuo de los procesos a través del afianzamiento de los controles permitiendo mitigar los riesgos inherentes y potenciales.

ARTÍCULO 3°. DEFINICIONES

Este documento requiere de definiciones específicas.

La definición generalmente aceptada de Riesgo Operativo (RO), tal y como se contempla en los documentos elaborados por el Comité de Basilea y que fue adoptada por la SFC en su normatividad respecto a este tipo de riesgo es la siguiente:

> *(...) Se entiende por Riesgo Operativo, la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos...*

Esta definición incluye el riesgo legal y riesgo reputacional (no lo contempla el Comité de Basilea) asociados a estos factores.

ARTÍCULO 4°. POLÍTICAS PARA LA ADMINISTRACIÓN DE RIESGO OPERATIVO Y LA CONTINUIDAD DEL NEGOCIO

El siguiente compendio de políticas considera los riesgos operativos propios de los procesos y actividades desarrolladas al interior del Infider, en donde se hace necesario el entendimiento, compromiso y disposición de todas las áreas y servidores públicos del Instituto, independiente de su nivel jerárquico, función o localización para su debido cumplimiento.

- Definir la exposición en materia de RO, estableciendo un perfil de riesgo para el Instituto, así como las acciones a desarrollar según el nivel de severidad definido.

- Realizar una adecuada identificación de riesgos operativos (potenciales y ocurridos) en todos los procedimientos y procesos que contempla el Modelo de Operación por Procesos del Infider.

- Todos los riesgos operativos identificados deben contar con una medición (cualitativa o cuantitativa) que permita determinar la probabilidad de impacto y ocurrencia de cada uno de ellos y pueda validarse la exposición al riesgo operativo que tiene el Infider.

- El seguimiento debe estar enfocado a monitorear el cumplimiento de las estrategias definidas para la mitigación de cada uno de los riesgos identificados y valorados, en los cuales deberán generarse reportes periódicos para conocimiento de la Gerencia y de la Junta Directiva o quien haga sus veces, del comportamiento general de estos riesgos y su tendencia en el tiempo.

- Establecer las actividades necesarias que permitan controlar y mitigar el riesgo operativo. Es así como en el conocimiento, actualización e implementación de las medidas de control respectivas, recae la responsabilidad de cada uno de los integrantes

de las diferentes áreas del Infider, siendo el insumo principal para establecer el mapa de riesgo residual y perfil de riesgo del Infider.

- Crear los mecanismos necesarios para divulgar información interna y externa que permitan generar confianza a los clientes, empleados y público en general, los cuales deben cumplir como propósito general informar sobre la gestión desarrollada en materia de riesgos al interior del Infider, buscando en todo momento la creación de una cultura de prevención de riesgos al interior del Instituto con una participación activa de todos los servidores públicos.

- Todos los servidores públicos del Infider deben cumplir con el programa de capacitaciones que en materia de riesgo operativo sean ofrecidas; así mismo, debe incluirse como componente permanente en el plan de inducción que sea ofrecido por el Instituto.

- El Infider adoptará un plan de continuidad del negocio enfocado en dar soporte a las actividades que sean sujetas de supervisión por parte de la SFC y que sean desarrolladas en el Instituto, el cual, deberá ser liderado por el área o persona encargada de sistemas y tecnología y debe considerar los controles de seguridad, disponibilidad de la información y pasos a seguir en materia de contingencia para cada una de estas actividades.

ARTÍCULO 5°. ESTRUCTURA ORGANIZACIONAL, ROLES Y RESPONSABILIDADES EN EL SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO Y PCCN

ARTÍCULO 5.1. JUNTA DIRECTIVA O QUIEN HAGA SUS VECES

Corresponde a la Junta Directiva del Instituto o quien haga sus veces adoptar las siguientes decisiones relativas a la administración del riesgo operativo de las diferentes actividades objeto de supervisión por la SFC mencionadas en la legislación vigente:

a. Establecer y aprobar las políticas relativas a la implementación de un sistema de administración de riesgo operativo en el Instituto.

b. Aprobar el presente Manual de Riesgo Operativo y sus actualizaciones.

c. Hacer seguimiento y pronunciarse sobre el perfil de riesgo operativo del instituto.

d. Establecer las medidas relativas al perfil de riesgo operativo, teniendo en cuenta el nivel de tolerancia al riesgo del Instituto.

e. Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente el representante legal en materia de riesgo operativo.

f. Pronunciarse sobre la evaluación periódica del SARO que realicen los órganos de control.

g. Autorizar, en el aforo del anteproyecto de presupuesto de cada vigencia fiscal, los recursos necesarios para implementar y mantener en funcionamiento el SARO de forma efectiva y eficiente.

h. Aprobar el Plan de Contingencia y Continuidad del Negocio definido en el presente Manual, así como sus respectivas modificaciones.

i. Pronunciarse respecto al resultado de las pruebas anuales realizadas al Plan de Contingencia y Continuidad del Negocio.

ARTÍCULO 5.2. GERENTE

Corresponde al gerente del Instituto la responsabilidad de velar por el cumplimiento de los manuales y demás disposiciones relacionadas con la administración del riesgo operativo. Sus funciones frente al SARO son las siguientes:

a. Someter a aprobación de la Junta Directiva o quien haga sus veces, el Manual de Riesgo Operativo y sus actualizaciones.

b. Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva o quien haga sus veces.

c. Recibir y evaluar los informes de seguimiento permanente de las etapas y elementos constitutivos del SARO.

d. Velar porque se implementen estrategias con el fin de establecer el cambio cultural que la administración de este riesgo implica para el Instituto.

e. Someter a aprobación de la Junta Directiva o quien haga sus veces, el Plan de Contingencia y Continuidad del Negocio y sus correspondientes actualizaciones.

f. Adoptar las medidas relativas al perfil de riesgo teniendo en cuenta el nivel de tolerancia al riesgo establecido en este Manual.

g. Adoptar el Plan de Contingencia y Continuidad del Negocio y disponer de los recursos necesarios para su oportuna ejecución.

h. Presentar informe, en caso de que se requiera, a la Junta Directiva o quien haga sus veces, sobre la evolución y aspectos relevantes del SARO, incluyendo, entre otros, las

acciones preventivas y correctivas implementadas o por implementar y el área responsable.

i. Informar a la Junta Directiva o quien haga sus veces el resultado anual de las pruebas realizadas al PCCN.
j. Disponer de los recursos necesarios para la oportuna administración del PCCN.

ARTÍCULO 5.3. OFICINA DE CONTROL INTERNO

El propósito de la Oficina de Control Interno respecto de la administración del riesgo es el de proveer una evaluación objetiva a la entidad a través del proceso de auditoría interna sobre la efectividad de las políticas y acciones en la materia, de cara a asegurar que los riesgos institucionales están siendo administrados apropiadamente y que el Sistema de Control Interno está siendo operado efectivamente, sus funciones respectivas son las siguientes:

a. Brindar elementos para la evaluación sobre procesos de administración del riesgo

b. Determinar si la evaluación de los riesgos es correcta

c. Evaluar los procesos de administración del riesgo

d. Evaluar reportes de riesgos institucionales

e. Revisar el manejo de los riesgos institucionales

ARTÍCULO 5.4. ÁREA DE SISTEMAS

Corresponde al área o persona encargada de Sistemas y Tecnología todo lo concerniente con la identificación de los riesgos operativos, relacionados con el componente tecnológico y el liderazgo de la implementación y desarrollo del PCCN del Infider:

a. Liderar la recuperación tecnológica, basado en la estrategia de continuidad del negocio definida.

b. Identificar y valorar los posibles riesgos tecnológicos que puedan afectar la continuidad de la operación normal del Instituto.

c. Mantener comunicación constante con los demás actores del PCCN durante el estado de contingencia, informando el estado de recuperación de la misma a la cadena de mando establecida para su atención.

d. Asegurar la seguridad y continuidad de la información, así como oportunidad de la misma.

e. Implementar las acciones correspondientes a la recuperación y puesta a punto de la información en los tiempos establecidos dentro del PCCN.

f. Informar oportunamente a la administración de los eventos que por su nivel de severidad afecten la continuidad del negocio y requieran de tratamiento especial.

g. Efectuar continuo monitoreo a las acciones y tratamientos implementados como medidas de aseguramiento de los procesos críticos del Instituto.

h. Valorar y determinar el nivel de vulnerabilidad y posibles eventos vandálicos informáticos que pueda verse involucrado el Instituto.

i. Medir permanentemente la efectividad de los controles implementados y solicitar los ajustes y modificaciones en caso de que se requiera.

j. Asegurar la capacitación y entrenamiento del personal de Sistemas.

k. Asegurar que las personas involucradas en todas las etapas del PCCN tengan una correcta y adecuada capacitación en este tema.

l. Coordinar, apoyar y hacer seguimiento a la gestión de PCCN de cada área.

m. Efectuar y valorar el resultado de las pruebas efectuadas.

ARTÍCULO 5.5. DIRECCIÓN TÉCNICA EN ADMINISTRACIÓN DE RIESGO
Sus funciones frente al SARO son las siguientes:

a. Definir los instrumentos, metodologías y procedimientos tendientes a que el Infider administre y mida efectivamente sus riesgos operativos, acorde con los lineamientos y mejores prácticas que considere convenientes.

b. Desarrollar mecanismos, procesos y procedimientos para el reporte y consolidación histórica de los eventos de riesgo ocurridos durante el desarrollo de las actividades normales del Instituto.

c. Establecer la metodología para recoger la información de riesgos cualitativos en cada una de las áreas.

d. Entrenar a los líderes de procedimientos en la práctica de administración y gestión de riesgos.

e. Evaluar la efectividad de los controles identificados en cada uno de los procesos y su impacto en la mitigación de riesgos.

f. Establecer y monitorear el comportamiento de los riesgos identificados, informando y reportando a la Gerencia por lo menos dos veces al año.

g. Realizar seguimiento a los planes de acción identificados para los riesgos que no son aceptados en el Infider.

h. Efectuar la calificación general de riesgos del Infider y su impacto dentro de la estrategia organizacional.

i. Liderar programas de capacitación en materia de RO a todos los funcionarios del Instituto por lo menos una vez al año.

j. Integrar la estrategia del SARO con el PCCN.

k. Definir los instrumentos, metodologías y procedimientos tendientes a gestionar efectivamente el PCCN.

l. Acompañar el desarrollo de las diferentes etapas del PCCN.

ARTÍCULO 5.6. LÍDERES DE PROCESOS Y PROCEDIMIENTOS

Sus funciones frente al SARO son las siguientes:

a. Identificar y valorar riesgos, controles y planes de acción en cada uno de sus procesos y procedimientos.

b. Propender por mantener una aversión al riesgo en todas sus actuaciones.

c. Conservar una posición prudente en la administración de los recursos públicos, los cuales deben ser asegurados y expuestos al menor riesgo posible.

d. Impulsar y promover la cultura del RO para el personal a su cargo como un hábito en todos los procesos y actividades que se ejecuten.

e. Participar en el control y mitigación de los riesgos a los cuales se encuentran expuestos sus procesos.

f. Conservar en un nivel óptimo de actualización las matrices de riesgos operativos de los procedimientos a su cargo.

g. Establecer y conocer el nivel de exposición de riesgo operativo en que se encuentra los procedimientos a su cargo.

h. Articular la estrategia institucional con la gestión y administración de riesgos operativos.

i. Solicitar oportunamente al área encargada de la documentación de los procedimientos, las actualizaciones debidas, cuando se identifiquen desviaciones de los mismos.

j. Colaborar con el levantamiento de información de cada una de sus áreas identificando los procesos prioritarios para el desarrollo de los planes de contingencia y continuidad del negocio.

k. Propender por el control y mitigación de los riesgos presentes en sus procesos.

l. Responsables por la información suministrada para el establecimiento de cada uno de los mapas de riesgo en los procesos a su cargo; así mismo, establecer controles e implementar estrategias según las definidas en el presente Manual.

m. Ejecutar de manera oportuna los planes de acción que se establezcan para la mitigación de riesgos operativos en su área.

ARTÍCULO 5.7. TODOS LOS SERVIDORES PÚBLICOS Y CONTRATISTAS DEL INSTITUTO
Sus funciones frente al SARO son las siguientes:

a. Reportar oportunamente los eventos de Riesgo Operativo que ocurran en el transcurso diario de sus actividades, según lo indicado en el respectivo procedimiento que defina el Instituto para tal fin.

b. Conservar la plena conciencia de que los recursos públicos deben ser asegurados y expuestos al riesgo en la menor medida posible.

c. Adoptar una cultura de autocontrol y mitigación de Riesgo Operativo en todas las actividades diarias.

d. Participar, presentar y aprobar las capacitaciones que se brinden en materia de Riesgo Operativo en el Instituto.

e. Informar oportunamente al área o persona encargada de planeación, cuando se identifique la necesidad de efectuar ajustes a procedimientos y contribuir a la actualización del mismo.

ARTÍCULO 5.8. COMITÉ TÉCNICO DE RIESGO OPERATIVO

El Comité Técnico de Riesgo Operativo es el órgano colegiado encargado de la evaluación y análisis del riesgo operacional, así como de la recomendación de propuestas o modificaciones a las políticas de riesgo operacional, para su presentación y posterior aprobación por la Junta Directiva o quien haga sus veces. Sus funciones son las siguientes:

a. Evaluar los informes sobre la evolución del perfil de riesgo de la entidad y los controles adoptados de acuerdo con los tratamientos establecidos.
b. Analizar los informes de las Dirección Técnica en Administración de Riesgo.

c. Proponer a la Junta Directiva o quien haga sus veces ajustes a los límites de exposición y/o niveles de tolerancia al riesgo operacional establecidos.

d. Evaluar los resultados de las pruebas de vulnerabilidad al sistema de información del Instituto y proponer correctivos a la Junta Directiva o quien haga sus veces.

e. Valorar las acciones de mejoramiento del Sistema de Control Interno del Instituto y proponer ajustes al mismo.

f. Evaluar y proponer para aprobación de la Junta Directiva o quien haga sus veces:

- Las políticas y monitoreo de los diferentes riesgos a que está expuesta la entidad, así como de la administración de la infraestructura informática y equipo humano técnico dedicado a la gestión de riesgos.

- Las metodologías para identificar, medir, monitorear y controlar los diferentes tipos de riesgos inherentes al negocio y propios de Infider.

- Los ajustes en políticas, metodologías y límites de exposición al riesgo como consecuencia de cambios en la normatividad o necesidades internas de la entidad.

ARTÍCULO 5.8.1. INTEGRANTES

El Comité Técnico de Riesgo Operativo estará conformado por los siguientes funcionarios:

- Gerente
- Director administrativo y financiero
- Jefe Oficina Asesora Jurídica

- Uno de los profesionales del Área Comercial designado por el gerente

Invitado:

- Jefe Oficina de Control Interno

Secretaría:

- Director técnico en administración de riesgos, quien se encargará de:

  - Convocar a las reuniones
  - Elaborar las actas
  - Custodiar las actas y demás documentos derivados de las sesiones

ARTÍCULO 5.8.2. SESIONES DEL COMITÉ
La periodicidad de las sesiones del Comité Técnico de Riesgo Operativo será trimestral, o antes, si lo ameritan las circunstancias.

ARTÍCULO 6°. LINEAMIENTOS DE ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 6.1. LÍMITES DE EXPOSICIÓN DE RIESGO OPERATIVO
El siguiente mapa de calor determina el nivel de severidad que debe otorgarse a los riesgos operativos identificados y se convierte en el perfil de riesgo de la entidad, al cual, según su nivel de severidad (combinación de probabilidad e impacto), se le determina una estrategia definida posteriormente:

PROBABILIDAD	IMPACTO				
	No significativo (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

Donde las estrategias se definen según su severidad, en los siguientes niveles:

SEVERIDAD	ESTRATEGIA
BAJA (B)	Asumir el riesgo y conservar un monitoreo permanente sobre los mismos; pueden implementarse controles sencillos asegurando que no aumenten de nivel de severidad.
MODERADA (M)	Asumir, mitigar el riesgo, mediante la aplicación de actividades básicas y/o controles sencillos que permita disminuir el nivel de severidad del riesgo.
ALTA (A)	Plan de acción para mitigar, evitar, compartir o transferir el riesgo. Implementar una serie de acciones concernientes a la mitigación del mismo, dejando claro tiempos y formas; exige valoración permanente de los mitigantes.
EXTREMA (E)	Acción inmediata para mitigar, evitar, compartir o transferir el riesgo. Informar a la Gerencia la existencia del riesgo y los planes de acción para el tratamiento del mismo. Coordinación con el responsable del proceso de las valoraciones de las actividades pertinentes.

ARTÍCULO 6.2. IDENTIFICACIÓN DEL RIESGO OPERATIVO

Los líderes de cada proceso y procedimiento identificados en el MOP (Modelo de Operación por Procesos) institucional, tienen la responsabilidad de identificar y analizar el Riesgo Operativo en todas las actividades que conforman el procedimiento.

La identificación de estos riesgos operativos contempla tanto riesgos potenciales como ocurridos; para ello se debe contar con herramientas y metodologías que permitan realizar dicha identificación.

ARTÍCULO 6.2.1. FUENTES DE RIESGOS

Infider establece como fuentes de riesgo todo individuo, grupo humano, entidad o elemento físico o fenómeno del entorno, de los cuales se pueden derivar eventos que podrían afectar las áreas de impacto del Instituto, cuya ocurrencia se debe evitar para incrementar la posibilidad del logro de los objetivos.

Se definen como fuentes de riesgos genéricas:

- Relaciones comerciales y legales
- Circunstancias económicas y de mercado organizacional
- Comportamiento humano
- Eventos naturales
- Circunstancias políticas
- Tecnología y asuntos técnicos
- Actividades de gestión y control
- Actividades individuales

ARTÍCULO 6.2.2. ÁREAS DE IMPACTO

Infider establece como área de impacto, todo recurso bien u oportunidad al cual el instituto le ha o debe asignar un valor y su afectación podrá comprometer el incumplimiento de sus obligaciones y objetivos, por tal motivo debe ser protegida.

Se definen como áreas de impacto genéricas:

- Activos y recursos básicos
- Ingresos y derechos
- Costos
- Gente y comunidad
- Desempeño
- Programación de actividades
- Medio ambiente
- Intangibles
- Comportamiento organizacional

ARTÍCULO 6.3. MEDICIÓN DE LOS RIESGOS

La medición de los riesgos será realizada contemplando la frecuencia y el impacto de los mismos, obteniendo así la medición individual. Lo anterior, permitirá realizar una consolidación de todos los riesgos identificados en el Infider para poder establecer el mapa de riesgo inherente del Instituto.

Infider en su desarrollo metodológico establecerá las categorías y niveles con que se efectuará la medición de los componentes de frecuencia e impacto, estos a su vez deberán ser revisados periódicamente con el propósito de realizar los ajustes respectivos a sus criterios de medición. La estructura de información para desarrollar el presente componente se presentará en forma matricial; de esta manera la metodología adoptada tendrá una condición de medición semicuantitativa.

La base de datos de eventos de pérdida servirá como criterio técnico de ajuste de los componentes de medición y sus métricas podrán ser, adicionalmente soportadas, por datos o eventos del entorno.

Las tablas de medición procurarán ser conservadas por lo menos un año, solo en los eventos que se consideren por su nivel de impacto en el modelo podrán ser modificadas, previa sustentación técnica soportada.

La medición de riesgos identificados se efectuará en tres momentos, tales como: riesgo inherente, riesgo con controles y riesgo con tratamientos.

ARTÍCULO 6.4. SEGUIMIENTO

El seguimiento debe estar enfocado a monitorear el cumplimiento de las estrategias definidas para la mitigación de cada uno de los riesgos identificados y valorados, en los cuales deberán generarse reportes periódicos para conocimiento de la Gerencia y la Junta Directiva o quien haga sus veces, del comportamiento general de estos riesgos y su tendencia en el tiempo.

El seguimiento al estado de los riesgos en los diversos estados (inherente, con controles y tratamiento) deberá efectuarse periódicamente por el responsable del proceso y sus valoraciones deberán quedar registradas en el respectivo sistema de información.

ARTÍCULO 6.5. CONTROL

Deben establecerse los procesos y procedimientos necesarios que permitan controlar y mitigar el Riesgo Operativo. Es así como el conocimiento, actualización e implementación de las medidas de control respectivas recae la responsabilidad de cada uno de los integrantes de las diferentes áreas del Infider, siendo el insumo principal para establecer el mapa de riesgo residual y perfil de riesgo del Infider.

Para efectuar el análisis de controles debe realizarse una calificación del nivel de mitigación a partir de sus características:

- Forma de ejecución
- Tipo
- Estado actual
- Ejecución
- Evidencia

Así mismo, deben calificarse la oportunidad, efectividad y eficiencia de los mismos.

ARTÍCULO 7°. METODOLOGÍA DE IMPLEMENTACIÓN DE SARO EN EL INSTITUTO

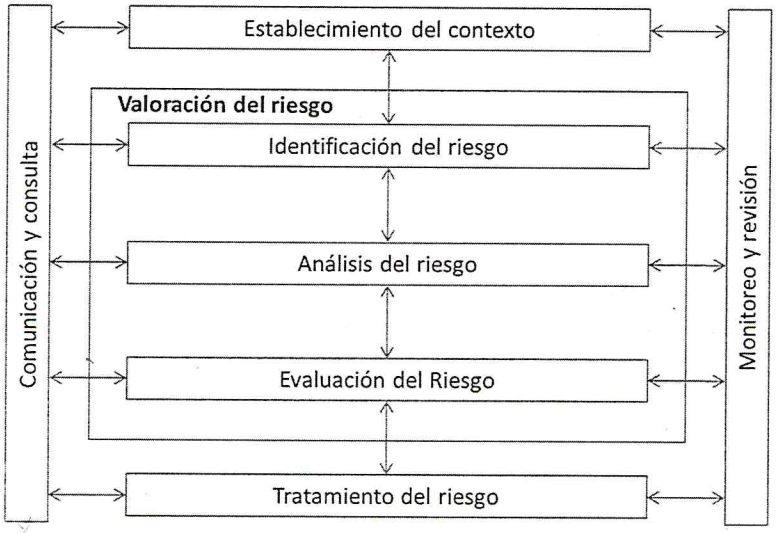
Para cumplir las políticas establecidas en el presente documento, el Infider adopta e implementa mejores prácticas propuestas en estándares internacionales como lo son el Comité de Basilea 2, la NTC 5254, la ISO 31000 así como las directrices impartidas en materia de riesgo operativo por el Departamento Administrativo de la Función Pública.

La Dirección Técnica en Administración de Riesgos es la dependencia encargada de diseñar, implementar y realizar seguimiento a la implementación de este Sistema de Administración de Riesgo en el Infider.

Una implementación exitosa del SARO debe estar sustentada en la consolidación de una cultura de *Mitigar Riesgos* que permita aumentar la conciencia sobre la importancia de la

gestión de todos los riesgos operativos identificados y sucedidos, acompañada siempre y en todo momento por estrategias comunicacionales que deben ser trabajadas en conjunto con el área o persona encargada de comunicaciones.

La gestión del Riesgo Operativo es una parte integral del proceso de gestión administrativa; la metodología implementada recoge los siguientes aspectos que permiten una gestión continua de este tipo de riesgo:



ARTÍCULO 7.1. COMUNICACIÓN Y CONSULTA

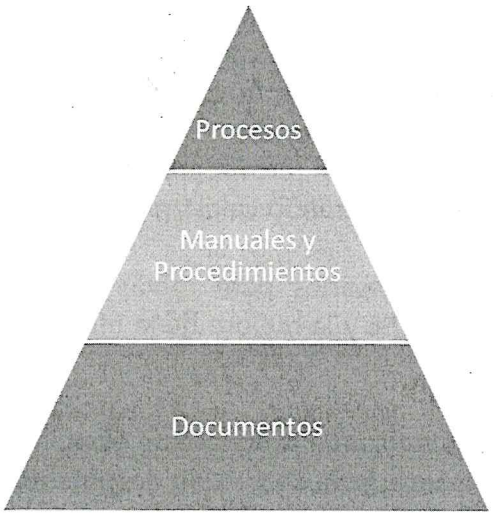
La comunicación y consulta con las partes interesadas, tanto internas como externas, deberá tener vigencia durante el ciclo del desarrollo del SARO, procurando que los planes para la comunicación y la consulta se efectúen tempranamente, abordando aspectos relacionados con el propio riesgo, las causas, las consecuencias y las medidas que se toman para tratarlo. Es conveniente que tengan lugar la comunicación y las consultas externas e internas eficaces para garantizar que aquellos responsables de la implementación del proceso para la gestión de riesgo y las partes involucradas comprendan las bases sobre las cuales se toman las decisiones y las razones por las cuales se requieren acciones particulares.

ARTÍCULO 7.2. ESTABLECIMIENTO DEL CONTEXTO

El Infider, en la construcción y elaboración del Plan Estratégico Institucional vigente analizará su visión, misión y foco estratégico, para posteriormente trazar, de acuerdo con sus perspectivas (financiera, clientes, procesos y aprendizaje) los objetivos estratégicos a los cuales debe apuntar cada una de las áreas y servidores públicos del Instituto.

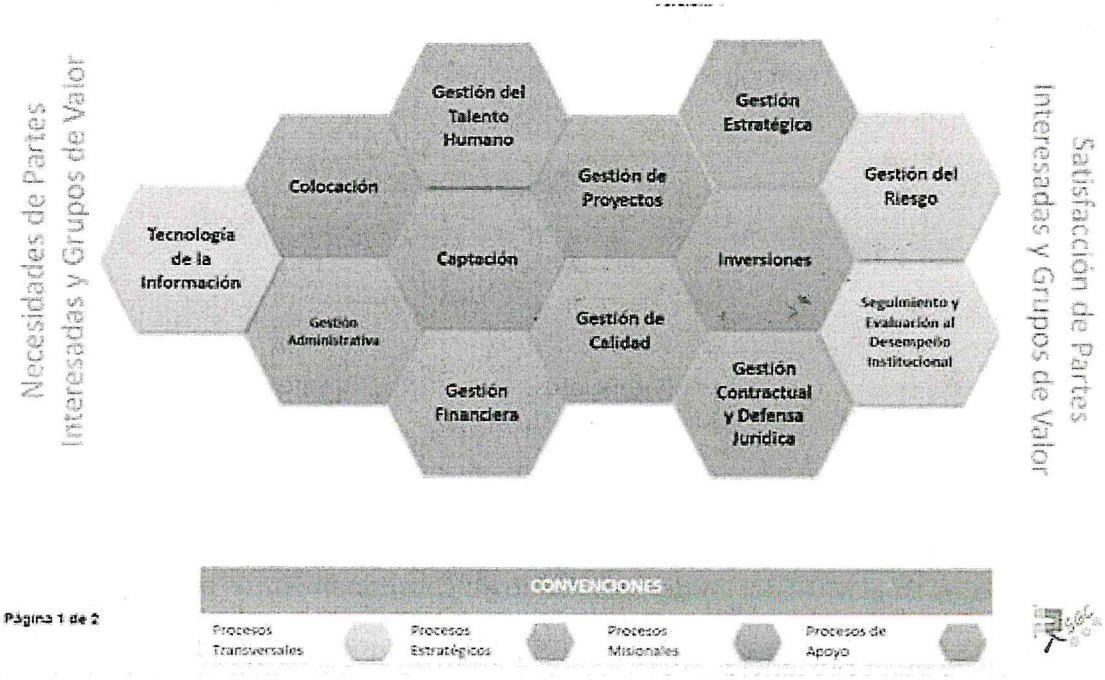
Por lo anterior, el establecimiento del contexto permitirá articular los objetivos, definir en la gestión del riesgo los parámetros externos e internos que se consideren y establecer el alcance y los criterios para el desarrollo del proceso.

Ahora bien, para cumplir los objetivos estratégicos descritos, el Infider realiza su gestión operativa a través de un Modelo de Operación por Procesos (MOP), categorizándolos de la siguiente manera:



- Procesos caracterizados que apuntan al cumplimiento de los Objetivos Estratégicos (Misionales, Estratégicos, Apoyo y Evaluación.
- Procedimientos operativos identificados en cada una de las áreas involucradas en los procesos.
- Plantillas y formatos generados para el cumplimiento, control, etc. De los procedimientos.

Lo anterior, se resume en el siguiente diagrama del MOP:



Página 1 de 2

ARTÍCULO 7.3. PROCESOS

- **Procesos misionales:** son aquellos procesos mediante los cuales se genera valor agregado a los productos y servicios a los que apunta el objeto social del Infider; estos van dirigidos a satisfacer las necesidades y expectativas de sus clientes.

- **Procesos estratégicos:** son los procesos mediante los cuales, quienes toman decisiones en la organización, obtienen, procesan y analizan información procedente de fuentes internas o externas con el fin de evaluar y hacer seguimiento a la situación actual del Infider, así como su nivel de competitividad, con el propósito de anticipar y decidir sobre el direccionamiento de la organización hacia el futuro.

- **Procesos de apoyo:** son los procesos que respaldan, proveen de diferentes recursos a los misionales, estratégicos y de evaluación, generando valor agregado al Infider.

- **Procesos de evaluación:** son procesos necesarios para medir y recopilar datos destinados a realizar el análisis del desempeño y la mejora de la eficacia y eficiencia, siendo parte integral del MOP.

La información documentada puede ser consultada en el software de gestión documental, el cual será alimentado por el área o persona encargada de gestión documental.

ARTÍCULO 7.4. IDENTIFICACIÓN DE RIESGOS

Partiendo de los procedimientos identificados en el MOP, se procederá por cada uno de sus líderes a realizar la identificación de cada uno de los riesgos operativos potenciales y los que ocurran en el transcurso de las operaciones:

Riesgos potenciales: estos riesgos son identificados utilizando como herramienta principal el *juicio de expertos* que tiene cada uno de los líderes de los procesos y procedimientos existentes en el MOP del Infider, partiendo de cuestionamientos sencillos como lo son:

- ¿Qué puede suceder?

- ¿Cómo puede suceder y por qué?

Esta identificación debe estar orientada y acompañada por la Dirección Técnica en Administración de Riesgos del Infider y debe quedar diligenciada en la Matriz de Riesgo Operacional, garantizando la posterior administración y seguimiento a los controles, tratamientos e indicadores de los riesgos identificados.

Para la identificación de los riesgos, debe registrarse en la Matriz de Riesgo Operacional que contenga como mínimo:

- ***Causas:*** son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.

- ***Riesgo:*** hace referencia al riesgo operativo identificado por el líder del procedimiento, debe registrarse el nombre del riesgo.

- ***Descripción:*** hace referencia a la descripción detallada del riesgo identificado.

- ***Factor:*** fuente generadora de riesgo de acuerdo a las definidas en el presente Manual, estas pueden ser:

  - Recurso humano
  - Procesos
  - Tecnología
  - Infraestructura
  - Situaciones externas
  - Corrupción
  - Situaciones políticas
  - Sistema de Gestión Seguridad y Salud en el Trabajo, SG-SST
  - LA/FT

- ***Categoría:*** para poder administrar los eventos de riesgo, estos deben ser agrupados en diferentes categorías definidas en el presente Manual:

  - Fraude externo
  - Fraude interno
  - Relaciones laborales
  - Clientes
  - Fallas tecnológicas
  - Ejecución de procesos

- Daños en activos físicos

- ***Consecuencias potenciales:*** describir brevemente cuál es el impacto que puede tener la materialización de este riesgo; puede ser económico o cualitativo.

- ***Riesgos ocurridos*:** para poder tener un mejor control del comportamiento de los eventos de riesgo que se materializan en la operatividad diaria del Infider se debe contar con un registro de estos para poder generar un histórico de los mismos y poder ajustar los mapas de riesgo previamente identificados en su frecuencia e impacto de acuerdo con la ocurrencia de los mismos.

El registro de eventos de riesgo operativo tiene los siguientes objetivos:

- Desarrollar estrategias de mitigación ante la materialización de los mismos
- Generar conciencia en los costos resultantes de situaciones de riesgo que impactan negativamente los resultados del Infider
- Contar con una base de datos que permitirá cuantificar la exposición al riesgo operativo y focalizar esfuerzos tanto operativos como financieros
- Realizar análisis de los factores de riesgo asociados a los eventos reportados, lo cual puede dar indicios de necesidad de mejoras en áreas y/o procesos del Infider

Deben registrarse todos los eventos ocurridos, así generen o no pérdida.

La base de datos debe contener como mínimo lo siguiente:

- ID del evento
- Nombre el evento
- Fecha de descubrimiento
- Fecha de inicio
- Fecha de finalización (no obligatorio)
- Fecha de contabilización (no obligatorio)
- Tipo de impacto (cualitativo, cuantitativo)
- Cuantía estimada del impacto
- Cuantía total recuperada (no obligatorio)
- Cuantía recuperada por seguros (no obligatorio)
- Factor de riesgo
- Categoría de riesgo
- Procedimiento afectado
- Tipo de pérdida
- Descripción del evento
- Área

La base de datos debe ser administrada por la Dirección Técnica en Administración de Riesgos. Estos riesgos deberán ser revisados por lo menos una vez al año.

ARTÍCULO 7.5. ANÁLISIS DEL RIESGO

Para iniciar la etapa de análisis de riesgos se debe ordenar, clasificar y documentar la información de los procesos de la entidad, para lo cual se debe tener en cuenta tanto la percepción del líder de cada proceso o procedimiento, como la información resultante de la matriz de riesgo operacional.

Por una parte, se realiza una revisión de la identificación de riesgos operativos, buscando mitigar el riesgo antes de su materialización. Es fundamental entender que el análisis tiene su sustento en las posibles consecuencias que pueda traer para el Infider la materialización de los mismos, bien sea por la frecuencia de ocurrencia o el impacto.

Adicionalmente, cuando se registre la ocurrencia de un evento de RO, se debe realizar un análisis y calificación del mismo; actividad donde se busca integrar aquellos riesgos que no hayan sido identificados previamente por los líderes de los procesos y a partir del cual se tiene como objetivo promover el desarrollo de estrategias que permitan la mitigación de los riesgos operativos.

Teniendo en cuenta que la Gestión de Riesgo Operativo es un proceso que agrega valor al Infider, es fundamental entender que el registro de eventos no es el objetivo final, sino que es una herramienta que contribuye con la mitigación de riesgos. En este sentido, la mitigación de riesgos se alinea a los objetivos estratégicos de *Administrar eficientemente la estructura de gastos* y *Aumentar la capacidad de gestión institucional,* mencionados anteriormente en el presente Manual. Esto puede verse a través de la reducción de costos, e incluso a través del mejoramiento de procesos que permiten potencializar ventajas competitivas de diferenciación de cara a los clientes del Infider.

Para lograr esto, los líderes de cada proceso deben realizar la calificación de cada riesgo en cada una de las escalas de probabilidad (frecuencia de ocurrencia) e impacto (consecuencia en caso de materialización), las cuales estarán registradas en el respectivo procedimiento de desarrollo metodológico del SARO.

- **Probabilidad (frecuencia de ocurrencia):**

La valoración de la probabilidad de la ocurrencia del riesgo se establecerá mediante los criterios construidos en la matriz de riesgo operacional y se expondrá en el procedimiento respectivo.

Se establecerán las escalas de valoración bajo cinco niveles, los cuales buscarán cubrir las

posibles asignaciones de medición de este componente.

Las fijaciones de las tablas de valoración permanecerán por periodos máximos de un año, permitiendo la estabilización de los criterios de medición.

Tabla de valoración de la ocurrencia o probabilidad:

ID	Escala	Probabilidad de ocurrencia
1	Raro	2 o menos veces al año
2	Improbable	Entre 3 y 4 veces al año
3	Posible	Entre 5 y 10 veces al año
4	Probable	Entre 11 y 24 veces al año
5	Casi Seguro	Más de 24 veces al año

- **Impacto (consecuencia en caso de materialización):**

El impacto puede ser cualitativo o cuantitativo, según el riesgo identificado o el evento ocurrido; para esto, el Infider define en el respectivo procedimiento en la matriz de valoración con los criterios a evaluar; esta clasificación debe plasmarse en el mapa de riesgos inherente, el cual debe establecerse según lo orienta la política de límites (niveles de severidad) y la estrategia definida por parte de la entidad para la mitigación del mismo; además, se debe observar la realización de las siguientes actividades:

- Registrar en la Matriz de Riesgo Operacional el resultado de la calificación de la consecuencia, de acuerdo con la tabla respectiva.
- Realizar la calificación del mismo para los eventos de riesgo ocurridos, por parte de la Dirección Técnica en Administración de Riesgos, para evaluar su impacto y que quede registrado en la Matriz de Riesgo Operacional con una calificación más acertada.

La escala a utilizar, según el tipo de impacto, es la siguiente:

	Pérdida Económica / Costo de Oportunidad		Seguridad de la Información	Operativo	Continuidad del Negocio	Atención al Cliente	Legal
	Hasta X% del PT	Vlr en Pesos					
No significativo	0,002%	$ 9.701.732,83	Uso inadecuado de información pública	El reproceso dura entre 1 y 2 días	La interrupción del negocio dura entre 1 y 2 días	Se ven afectados hasta 3 clientes	no conformidades por órganos de control interno
Menor	0,010%	$ 48.508.664,17	Divulgación de información no oficial	El reproceso dura entre 2 y 4 días	La interrupción del negocio dura entre 2 y 4 días	Se ven afectados entre 4 y 6 clientes	incumplimientos contractuales
Moderado	0,030%	$ 145.525.992,50	Divulgación de información de clientes	El reproceso dura entre 5 y 10 días	La interrupción del negocio dura entre 5 y 10 días	Se ven afectados entre 7 y 15 clientes	Glosas por parte de órganos regulatorios
Mayor	1,500%	$ 7.276.299.625,01	Pérdida de información de clientes	El reproceso dura entre 11 y 20 días	La interrupción del negocio dura entre 11 y 20 días	Se ven afectados entre 16 y 30 clientes	Sanciones por parte de los órganos de control y vigilancia
Catastrófico	3,000%	$ 14.552.599.250,02	Pérdida total de la información de la entidad	El reproceso dura mas de 20 días	La interrupción del negocio dura mas de 20 días	Se ven afectados mas de 30 clientes	Destitución en inhabilitación de algún administrador

ARTÍCULO 7.6. EVALUACIÓN DEL RIESGO

Permite comparar los resultados de la calificación del riesgo con los criterios definidos para establecer el grado de exposición de la entidad al mismo; de esta forma, es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

De lo anterior, se genera un mapa de riesgos inherente para una primera evaluación de los riesgos identificados; esta es la definida en la política en el presente Manual y corresponde al mapa de calor establecido en el artículo 6.1 del presente Acuerdo.

Para poder realizar una adecuada gestión previa a la materialización del riesgo, debe realizarse una valoración de los controles según criterios objetivos donde se pueda realizar una comparación de la efectividad de estos frente al mapa de riesgo inherente previamente identificado.

Las categorías de control de mayor aplicación:

Controles de gestión	Políticas claras aplicadas
	Seguimiento al plan estratégico y operativo
	Indicadores de gestión
	Tableros de control
	Seguimiento a cronograma
	Evaluación del desempeño
	Informes de gestión
	Monitoreo de riesgos
Controles operativos	Conciliaciones
	Consecutivos
	Verificación de firmas
	Listas de chequeo

	Registro controlado
	Segregación de funciones
	Niveles de autorización
	Custodia apropiada
	Procedimientos formales aplicados
	Pólizas
	Seguridad física
	Contingencias y respaldo
	Personal capacitado
	Aseguramiento y calidad
Controles legales	Normas claras y aplicadas
	Control de términos

Para realizar el análisis y valoración de los controles existentes según su nivel de mitigación debe cumplirse lo siguiente:

Forma de realización del control:

- **Automático:** el control se ejecuta sin depender de ninguna acción humana
- **Semiautomático:** el control depende tanto de la intervención humana, como de la intervención de una máquina, sistema u otro
- **Manual:** el control depende en su totalidad de la intervención humana

Tipo de control:

- **Preventivo:** hace referencia a acciones que permiten mitigar el riesgo previo a su materialización
- **Detectivo:** tipo de control que genera una alarma cuando se está materializando el riesgo y donde posteriormente se debe generar una medida correctiva
- **Correctivo:** tipo de control que actúa después de la materialización del riesgo.

Estado del control:

- **Implementado y documentado:** durante la identificación de riesgos el control se encuentra en funcionamiento y documentado
- **Implementado no documentado:** corresponde a un control que se encuentra en funcionamiento, pero no está documentado
- **En desarrollo:** durante la identificación el control no se ejecuta; sin embargo, se está adelantado su puesta en marcha

Ejecución del control:

- **Siempre:** el control se ejecuta cada vez que se realiza el procedimiento

- **En la mayoría de veces:** el control se ejecuta la mayoría de las veces en que se realiza el procedimiento
- **Solo algunas veces:** el control se ejecuta ocasionalmente

Evidencia del control:

- **Siempre:** siempre queda evidencia de la ejecución del control
- **Algunas veces:** algunas veces queda evidencia de la ejecución del control
- **Nunca:** no hay ninguna evidencia de la ejecución del control

Se debe tomar la calificación de cada uno de los criterios enunciados para determinar el nivel de mitigación del control, lo que permite posteriormente establecer el nivel de riesgo residual, el criterio de medición se establecerá en el procedimiento respectivo.

ARTÍCULO 7.7. EVALUACIÓN DE OPORTUNIDAD, EFECTIVIDAD Y EFICIENCIA

Oportunidad: un control oportuno es determinado por la parte del proceso en la que se ejecuta y el momento en el que se presenta la actividad generadora de riesgo.

Efectividad: un control efectivo es aquel que reduce el impacto y/o probabilidad de materialización del riesgo

Eficiencia: un control eficiente es aquel que no perjudica el desempeño general del proceso, su relación costo beneficio es positiva y es claro para todas las personas involucradas en su ejecución.

Las calificaciones para cada uno de los criterios se ordenan de 0 hasta 3, siendo 3 la calificación de mejor condición.

Esta calificación debe registrarse en la matriz de riesgo operacional.

Cada uno de los criterios anteriores tiene la siguiente ponderación:

Realización	Tipo	Estado	Ejecución	Evidencia
25 %	10 %	25 %	20 %	20 %

CRITERIOS DE CALIFICACIÓN DE LOS CONTROLES IDENTIFICADOS									
Realización	Calif	Tipo	Calif	Estado	Calif	Ejecución	Calif	Evidencia	Calif
Automático	*3*	*Preventivo*	*3*	*Implementado y documentado*	*3*	*Siempre*	*3*	*En medios Digitales*	3
Semiautomático	*2*	*Detectivo*	*2*	*Implementado y no documentado*	*2*	*La mayoría de las veces*	*2*	*Fisica y Digital*	3
Manual	*1*	*Persuasivo*	*2*	*No implementado y documentado*	*1*	*Algunas veces*	*1*	*Solo fisica*	2
		Correctivo	*1*	*En desarrollo*	*0*	*Nunca*	*0*	*No se evidencia*	0

El porcentaje de mitigación se calcula mediante un tipo de distribución normal y se calcula automáticamente según la calificación obtenida en el punto anterior:

Calificación Promedio >	y <=	% de Mitigación	Desplaza en probabilidad
1	1,25	38,3 %	0
1,25	1,5	46,0 %	0
1,5	1,75	53,7 %	0
1,75	2	61,3 %	0
2	2,25	69,0 %	1
2,25	2,5	76,7 %	1
2,5	2,75	84,3 %	2
2,75	3	92,0 %	2

Obteniendo como resultado:

Calificación	% Mitigación	Desplaza
2,20	69,0 %	1

De igual manera, cuando se tengan controles o mitigadores dirigidos a disminuir el impacto (pólizas de seguro, por ejemplo), estos se analizarán puntualmente y se definirá el desplazamiento en caso de darse.

Por último, se generan los mapas de riesgo inherente y residual (con el efecto de los controles calificados).

ARTÍCULO 7.8. PLAN DE ACCIÓN Y TRATAMIENTO

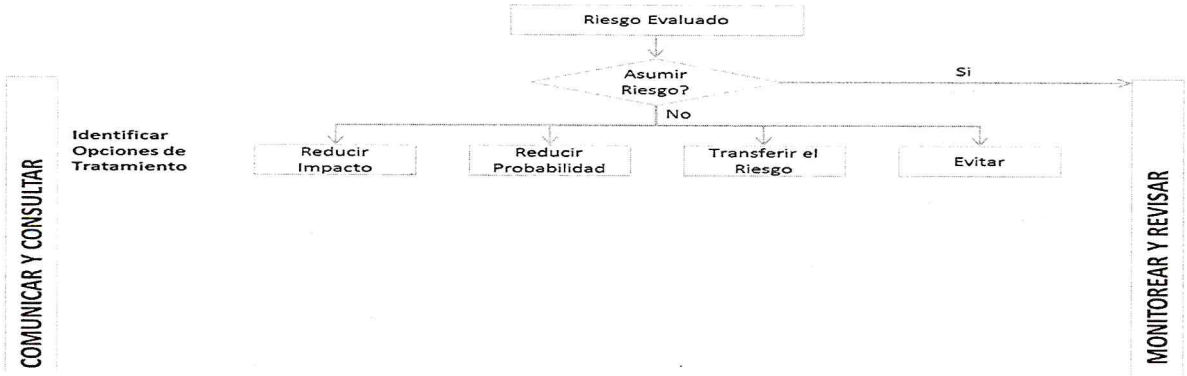
Como resultado de los riesgos identificados, y según la estrategia definida para cada nivel de severidad, se establecen los planes de acción que mitigan el riesgo; estos planes de acción deben quedar identificados y listados en la matriz de riesgo operacional.

Cada uno de estos debe contener una fecha de cumplimiento establecida para realizar su implementación, y el responsable, los cuales deben quedar en actas de reunión de cierre y presentación de resultados a las áreas evaluadas.

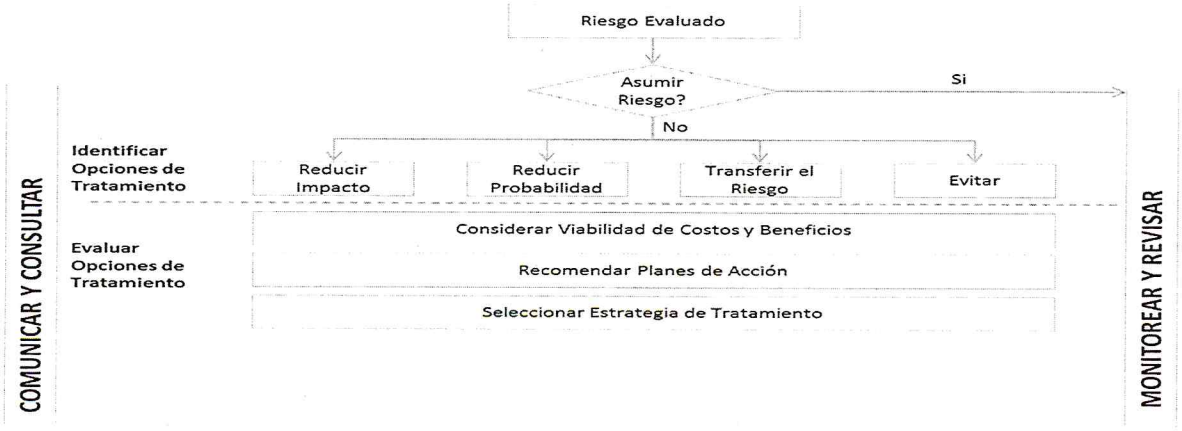
Los planes de acción deben ser llevados al Comité de Coordinación de Control Interno, quienes deben pronunciarse sobre el mismo y conocer el estado de los mapas de cada uno de los procedimientos.

Lineamientos a seguir para la implementación de un tratamiento:

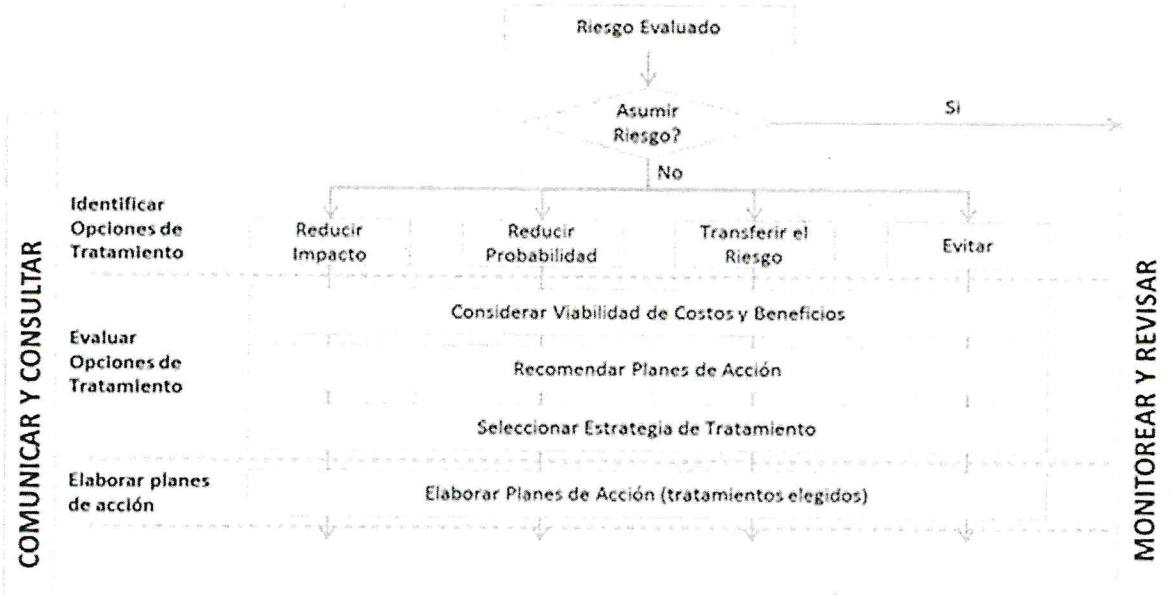
Una vez evaluados los riesgos, los tratamientos o planes de acción deben seguir la siguiente estructura para su creación, desarrollo y ejecución, teniendo como principales pilares el monitoreo y revisión, así como su comunicación y permanente consulta; por lo cual, según la estrategia a seguir según su severidad (definida previamente) el proceso continuaría de la siguiente manera:



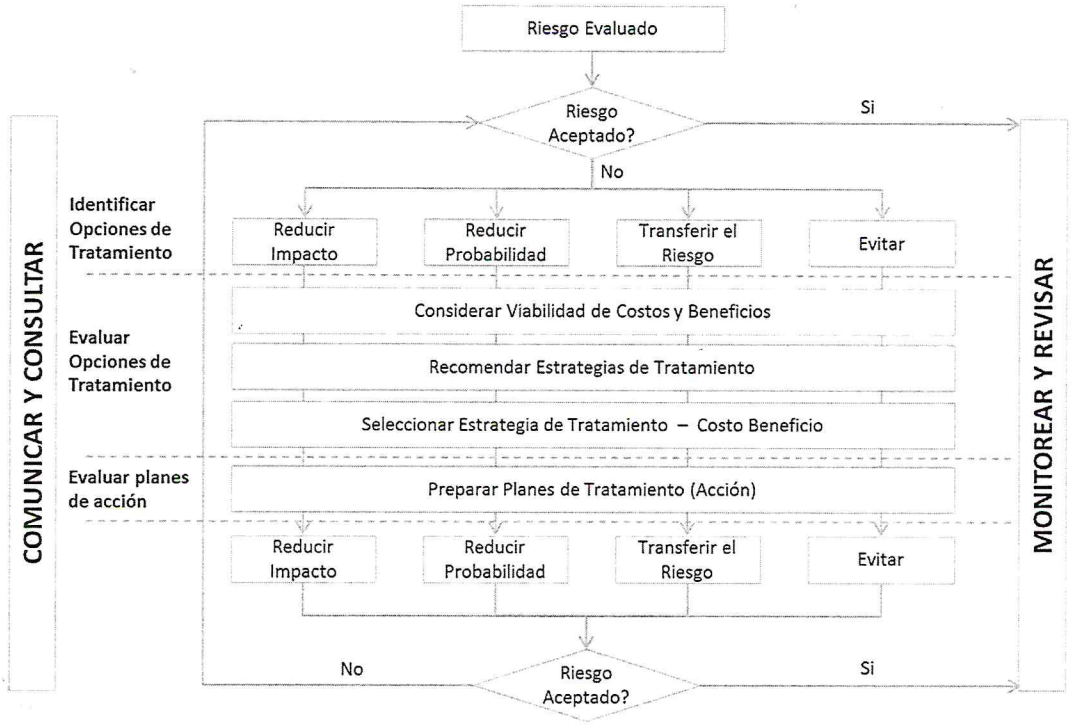
Una vez identificadas las opciones de tratamiento (reducir impacto, reducir probabilidad, transferir el riesgo o evitarlo completamente), debe procederse con la evaluación de las diferentes opciones de tratamiento, teniendo en cuenta la viabilidad del mismo en una relación costo beneficio, definir los planes de acción a implementar:



Posteriormente se lleva a cabo la elaboración de los planes de acción, definiendo los responsables y fechas de implementación para realizar su seguimiento y monitoreo, los cuales se deben dar a conocer al Comité de Coordinación de Control Interno.



Por último, se realiza la misma evaluación inicial del tratamiento y el resultado del riesgo completando el siguiente ciclo:



Una vez determinados los planes de acción, estos deben ser incluidos en la matriz de riesgo operacional, la cual debe ser diligenciada y entregada en el acta respectiva de la presentación del procedimiento al área que se está evaluando.

La estructura es la siguiente:

FORMATO DE IDENTIFICACION Y SEGUIMIENTO DE PLANES DE ACCION Y TRATAMIENTO								
#	PLAN DE ACCION (Tratamiento)	Riesgos Cubiertos	Responsable	Fecha de Implementació	Fecha de seguimiento 1	Observaciones	Fecha de seguimiento 1	Observaciones

Donde en la primera columna va numerado el plan de acción a implementar, la segunda columna la descripción del mismo, posteriormente los riesgos que ataca este plan de acción, determina el responsable del mismo (líder del área), la fecha estimada de implementación y dos fechas de seguimiento y observaciones encontradas.

ARTÍCULO 7.9. MONITOREO Y REVISIÓN BAJO INDICADORES

Los cumplimientos de los tratamientos establecidos deben estar alineados y consignados con el plan de auditorías a realizarse por la Oficina de Control Interno.

De igual manera, la Dirección Técnica de Administración de Riesgos debe realizar un constante monitoreo y seguimiento a los eventos ocurridos para poder ajustar los mapas de riesgo a que haya lugar.

Este monitoreo y seguimiento se debe realizar mediante la implementación y ejecución de Indicadores de seguimiento o KRI *(Key Risk Indicators)*, los cuales son índices construidos a partir de variables extraídas de los procesos, cuyo comportamiento está correlacionado con el nivel de riesgo y que son medibles y comparables a través del tiempo. De tal manera que estos indicadores sirvan como enlace entre el riesgo y su mitigación/control, permitiendo explicar el nivel de exposición al riesgo en función del esfuerzo impuesto en su mitigación o control.

Los indicadores creados pueden clasificarse en las siguientes categorías:

Gestionables: relativos a condiciones que pueden manejarse o administrar por el responsable del riesgo o control. Estos indicadores a su vez se pueden clasificar en:

- **Causales:** indicadores relacionados con monitorear las causas identificadas del riesgo
- **De control:** indicadores relacionados a efectuar seguimiento a los controles o mitigadores del riesgo
- **De desempeño:** relativos al resultado de la ejecución del proceso

No gestionables: son aquellos que inciden en el riesgo pero son provenientes de eventos externos que no pueden controlarse por la persona que administra el riesgo; estos a su vez se pueden clasificar en:

- **De negocio:** son determinados por las circunstancias del mercado donde se desenvuelve el Infider, en este caso los créditos de Fomento
- **De entorno:** dependen de factores externos ajenos a las condiciones del mercado, políticas, sociales, culturales, etc.

ARTÍCULO 7.10. LINEAMIENTOS PARA EL DISEÑO E IMPLEMENTACIÓN DE INDICADORES

- Deben referirse a parámetros observables cuyo comportamiento guarde estrecha relación con el riesgo asociado.
- Deben tener lógica y ser conscientes de que la utilización de estos no solo mitiga el riesgo sino que ayuda al control de la gestión.
- Deben ser resultado de un trabajo consensuado entre el líder del proceso, los servidores públicos que ejecutan las actividades generadoras de riesgo y pueden ser apoyados por la Dirección Técnica de Riesgos.
- Debe definirse claramente un responsable de su construcción y mantenimiento.
- Establecer fuentes de información para su cumplimiento que no generen sobrecargas operativas innecesarias.
- Determinar claramente su forma de cálculo y ejecución.
- Deben ser utilizados como sensores indirectos del grado de exposición al riesgo o riesgos asociados.
- Deben enfocarse como herramientas que permitan cumplir los objetivos del área, que en algunos casos puedan generar señales de alerta para que activen actividades de mitigación en caso de sobrepasar los umbrales mínimos establecidos.
- Deben a su vez establecerse fechas de seguimiento al cumplimiento de los planes de acción a implementar, revisiones periódicas de la implementación de los mismos, así como su cumplimiento y ejecución.

ARTÍCULO 8°. LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO

ARTÍCULO 8.1. OBJETIVO

Establecer las directrices para el desarrollo de la continuidad del negocio del Instituto, que permita cumplir la misión y objetivos con sus clientes, la normatividad, la responsabilidad social con el entorno y el compromiso con la protección de los servidores públicos e infraestructura del negocio.

ARTÍCULO 8.2. ALCANCE

Con el fin de implementar un plan de contingencia y continuidad del negocio (PCCN) acorde a su tamaño y el desarrollo de su operación, el Infider ha decidido desarrollar un PCCN para todas las actividades sujetas a la vigilancia por parte de la Superintendencia Financiera de Colombia soportado en la herramienta tecnológica del *core* del negocio, las cuales se identifican dentro de los procesos misionales relacionados en el Modelo de Operación por Procesos del Instituto, así como los que se consideren críticos según el resultado del BIA.

- El plan de contingencia y continuidad del negocio del Infider debe enfocarse al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a la materialización de eventos de riesgo operativo de interrupción o desastre.
- Los líderes de los procesos y procedimientos deben tener total claridad de las actividades a realizar en materia de PCCN, previa capacitación del encargado de la implementación y administración del plan de contingencia y continuidad.
- En caso de presentarse un incidente significativo se deben aplicar los mecanismos de comunicación apropiados, tanto internos como externos, con directrices claras y consignadas en el PCCN sobre la comunicación en situaciones de crisis.
- La implementación y cumplimiento del PCCN es de obligatorio cumplimiento y ejecución por las áreas que ejecutan actividades sujetas de supervisión por la Superintendencia Financiera de Colombia, liderada por el área o persona encargada de sistemas y tecnología.
- Los jefes de las áreas que desarrollen actividades sujetas a supervisión por parte de la Superintendencia Financiera deben designar un líder de PCCN, quien será responsable de apoyar las actividades del PCCN para el área que representa.
- Los procesos críticos deberán ser recuperados dentro del RTO establecido en el Plan de Contingencia y Continuidad del Negocio.

- Los límites tolerados al riesgo son los mismos implementados para la implementación del SARO del Infider.

- Los procesos o procedimientos de las actividades sujetas a supervisión por parte de la Superintendencia Financiera, desarrollados por terceros contratados, deben disponer de PCCN, responsabilidad que está en cabeza del supervisor del contrato, quien lo remitirá a la dirección técnica en administración de riesgos para obtener su visto bueno, incluyendo pruebas realizadas a dicho plan.

- Los planes de contingencia de las diferentes áreas deben mantenerse actualizados, para lo cual se deben desarrollar, probar y en los casos que así se requiera mejorar de forma periódica o ante cambios significativos en políticas, personas, procesos, tecnología, siendo necesario que en dicha revisión participen los líderes de los procesos involucrados.

- El PCCN debe ser probado por lo menos una vez al año y el resultado de las mismas debe ser llevado por el gerente a la Junta Directiva o quien haga sus veces.

ARTÍCULO 8.3. ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

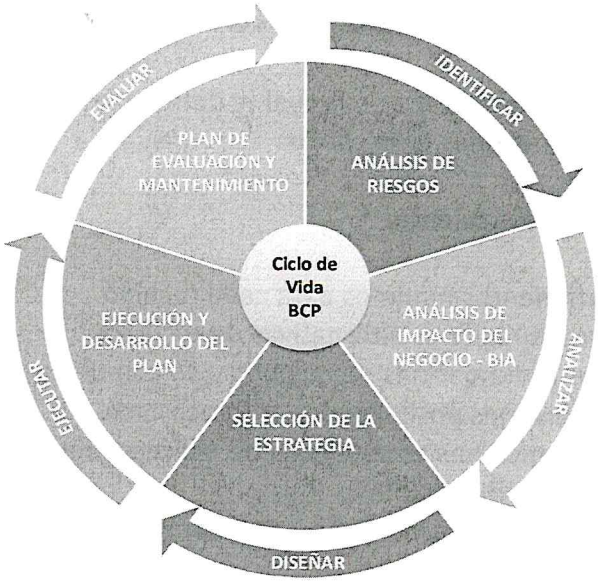
Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio.

Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca tanto a las personas como a los procesos, la tecnología y la infraestructura, así como a situaciones externas que afecten el funcionamiento normal de las operaciones del Infider.

Previo a la implementación de un modelo de administración de PCCN, se debe determinar lo siguiente:

- Establecer la necesidad de la continuidad del negocio
- Comprometer a la Alta Gerencia en los procesos de BCP
- Establecer el comité de proyecto
- Identificar los equipos de planificación y sus responsabilidades
- Diseño de metodología de seguimiento y aprobación avances del proyecto

Una vez establecido lo anterior, se definen las etapas en las que se va a desarrollar, dando como resultado:



Donde:

Análisis de riesgos: etapa previa a la implementación y debe estar acorde con los riesgos operativos identificados en el Infider.

Se debe cumplir en esta etapa mínimo con:

- Identificar los ambientes operativos que se pueden ver afectados en caso de una interrupción no deseada en sus operaciones.
- Identificar los principales escenarios de falla y los recursos e infraestructura critica.
- Identificar oportunidades de mejora o exposiciones críticas a riesgos de falla tecnológica
- Identificar las políticas y mejores prácticas de seguridad existentes
- Revisión de instalaciones físicas, centros de cómputo e infraestructura tecnológica en general.

Análisis del impacto del negocio (BIA): etapa en la cual se definen los procedimientos críticos del Infider, según el alcance mencionado en el presente documento, para poder establecer su relevancia, tiempos y secuencia de recuperación.

Se debe cumplir con lo siguiente:

- Verificación del inventario de procesos y procedimientos
- Identificación de impactos de interrupción de los procesos y procedimientos
- Definición de tiempos y secuencia de recuperación
- Identificación de interdependencias entre procesos

- Identificación de los procesos críticos del negocio

Selección de la estrategia: etapa en la cual se definen los recursos a utilizar, planes a seguir, tercerización de operaciones entre otros.

Se debe cumplir con lo siguiente:

- Definir requerimientos mínimos para cada recurso.
- Identificar configuraciones alternativas de recursos
- Determinar las redundancias de equipos y de comunicaciones
- Analizar las diferentes posibilidades en procesamiento y en comunicaciones
- Determinar las opciones estratégicas de procesamiento internas externas y acuerdos mutuos de servicio disponibles
- Establecer las principales ventajas y desventajas de cada una de las opciones

Desarrollo y ejecución del plan: etapa en la cual se desarrolla la implementación de las etapas anteriormente mencionadas.

Se debe cumplir con lo siguiente:

- Definir los planes de contingencia, restauración y vuelta a la operación según prioridades del negocio
- Elaborar el manual del plan
- Definir las condiciones que se deben cumplir para que el plan tenga éxito

Plan de evaluación y mantenimiento: última etapa en la cual se empodera el PCCN del Instituto al líder del mismo, integrando a su vez a todos los funcionarios del Infider.

- Desarrollar las tareas necesarias para garantizar la operatividad del plan
- Lograr una efectiva concientización sobre la importancia del plan
- Socializar el plan en el comité técnico de riesgo operativo y en toda la organización
- Designar un responsable del plan para su actualización y mantenimiento

ARTÍCULO 9°. GLOSARIO

El Manual de Políticas del Sistema de Administración del Riesgo Operativo del Infider en sus políticas de administración de riesgo emplea varios términos financieros y jurídicos; por ello se establece el siguiente glosario con los diferentes vocablos para obtener un contexto integral.

Sobre las tipologías de riesgo:

Riesgo inherente: son los riesgos que están inmersos en el desarrollo del objeto social del Instituto.

Riesgo legal: *Es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales. El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.*

Riesgo reputacional: *Es la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocio, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.*

Riesgo político: se refiere a la posibilidad de que no se alcancen los objetivos de una determinada acción económica, o estos se vean afectados, debido a cambios y decisiones políticas de los gobiernos

Riesgos potenciales: Hace referencia a los riesgos a los cuales se expone el Instituto en el desarrollo de sus operaciones.

Riesgos ocurridos: es la materialización de los riesgos operativos en los procesos del Instituto. Existen los siguientes tipos de eventos:

- ***Incidentes:*** son los eventos que tienen una causalidad de riesgo operativo y que no generan pérdidas.

  En el marco de la normatividad expedida por la SFC en materia de RO, los incidentes corresponden a eventos que no generan pérdidas y por lo tanto no afectan el estado de resultados del Instituto.

- ***Eventos de pérdida:*** son aquellos eventos que tienen una causalidad de riesgo operativo y se les puede realizar una cuantificación económica.

- ***Pérdidas directas:*** son aquellas reconocidas en las cuentas de balance, las cuales se pueden obtener a partir de la información contable de las entidades. Algunos ejemplos de este tipo de pérdidas son los fraudes internos, los robos y las indemnizaciones por litigios.

  De acuerdo con la normatividad expedida por la SFC, mencionada anteriormente, corresponden a aquellos que generan pérdidas y afectan el estado de resultados.

- ***Pérdidas indirectas:*** son eventos que generan pérdidas, pero que no son susceptibles de registrarse contablemente. Se pueden catalogar como pérdidas indirectas la disminución en los ingresos esperados y el costo de oportunidad.

Sobre los factores de riesgo operativo: son las fuentes generadoras de eventos de riesgo operativo:

Recurso humano: todos los funcionarios vinculados directa o indirectamente, los cuales intervienen de alguna forma con los procesos del Instituto.

Procesos: todos los procesos y procedimientos identificados en el Instituto para el desarrollo diario de su actividad.

Tecnología: conjunto de herramientas empleadas para soportar los procesos del Instituto tales como hardware, software, telecomunicaciones, redes.

Infraestructura: conjunto de elementos de apoyo para el funcionamiento del Instituto, por ejemplo: edificios, espacios de trabajo, almacenamiento y transporte.

Situaciones externas: son eventos ocasionados por terceros o por desastres naturales, que escapan en cuanto a su causa y origen al control del Instituto.

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 del Instituto y, en consecuencia, del Estado, para la obtención de un beneficio particular.

Situaciones políticas: factores o eventos que no son propios del comportamiento natural de un mercado, tales como: políticas sociales, fiscales, monetarias, de desarrollo, o bien pueden ser eventos relacionados con inestabilidad política en el país.

Sistema de Gestión Seguridad y Salud en el Trabajo, SG-SST: conjunto de eventos que puedan afectar el bienestar físico, mental y social de los servidores públicos del Instituto.

LA/FT: **LA:** el lavado de activos es el proceso mediante el cual organizaciones criminales buscan dar apariencia de legalidad a los recursos generados de sus actividades ilícitas. En términos prácticos, es el proceso de hacer que dinero ilícito parezca lícito, haciendo que las organizaciones criminales o delincuentes puedan hacer uso de dichos recursos y en algunos casos obtener ganancias sobre los mismos.

FT: es el apoyo financiero, de cualquier forma, al terrorismo o a aquellos que lo fomentan, planifican o están implicados en el mismo. No obstante, es más complicado

Riesgo de corrupción: el riesgo de corrupción es la posibilidad de ocurrencia de una conducta o comportamiento que puede derivar en una actuación corrupta. El enfoque de riesgo es preventivo, no reparativo; mediante su identificación es posible evitar la exposición al mismo y la presencia de los efectos indeseables que genera la corrupción.

Sobre planes y acciones

Plan de contingencia: conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Plan de Contingencia y Continuidad del negocio (PCCN): conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación en caso de interrupción.

Análisis del impacto del negocio, BIA (*Business Impact Analysis*): estudio que permite identificar, medir y documentar los impactos por una interrupción de las funciones normales del Instituto, determina la matriz de procesos críticos que soportan la organización y provee a la Alta Gerencia la información necesaria para la toma de decisiones dirigidas a la creación de estrategias dentro del Plan de Contingencia y Continuidad del Negocio.

Centro alterno de procesamiento: instalación especializada con la infraestructura física, lógica y de seguridad adecuadas dedicadas al almacenamiento y procesamiento de datos en un evento de excepción.

Plan de recuperación de desastres (DRP): estrategia a seguir para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.

Vulnerabilidad: debilidad que puede ser causada accidental o intencionalmente, originada por fallas en los controles permitiendo que se materialice un evento de riesgo que afecte los intereses de la institución.

Punto objetivo de recuperación (RPO): objetivo de cantidad máxima de tiempo entre la última copia de seguridad disponible y cualquier punto potencial de error. Se determina por la cantidad de datos que la entidad puede perder en caso de error.

definir al terrorismo en sí mismo, porque el término puede tener connotaciones políticas, religiosas y nacionales, dependiendo de cada país.

Sobre las categorías de eventos por riesgo operativo:

Todos los eventos de riesgo operativo deben tener asignada una categoría de riesgo dependiendo de la causa que originó el evento; las pérdidas registradas pueden ser agrupadas según la naturaleza de esta. Para ello, se utilizan una serie de categorías básicas que suministran una visión resumida del riesgo total existente. Las clases o categorías más usuales definidas son las siguientes:

Fraude interno: actos que de forma intencionada buscan defraudar, apropiarse indebidamente de activos propiedad del Instituto, evadir regulaciones, leyes o políticas del Instituto, excluyendo los sucesos de discriminación o diversidad laboral y que implican al menos a una persona del Instituto.
Fraude externo: actos cometidos por personas ajenas al Instituto que intentan defraudar o apropiarse indebidamente de sus activos y pasar por alto las leyes.

Relaciones laborales y legales: actos inconsistentes con las leyes o acuerdos de seguridad y salud en el trabajo, los cuales resultan en reclamaciones por daños personales o reclamaciones relacionadas con la discriminación o falta de diversidad laboral dentro del Instituto.

Clientes: fallos involuntarios o negligentes de las obligaciones frente a los clientes y que impiden satisfacer de forma profesional una obligación frente a ellos.

Fallas tecnológicas: son todas las interrupciones que se producen en el negocio por motivos tecnológicos y mal funcionamiento en los sistemas.

Ejecución y administración de procesos: fallos en el procesamiento de las transacciones o en la gestión de los procesos, así como la inexistencia de un procedimiento establecido para una actividad que pueda derivarse en una pérdida monetaria para el Instituto.

Daños en activos físicos: pérdidas derivadas de daños o perjuicios en activos físicos del Instituto.

Riesgo residual: nivel de riesgo resultante después de la implementación de los controles.

Severidad: magnitud de la pérdida definida en un horizonte de tiempo para un riesgo operativo, teniendo en cuenta la frecuencia y el impacto.

Tiempo objetivo de recuperación (RTO): objetivo de tiempo máximo que podría tardar un proceso de recuperación de datos. Se determina mediante la cantidad de tiempo que la entidad podría permitirse no tener disponible el sitio o servicio.

ARTÍCULO 10°. VIGENCIA
El presente Acuerdo rige a partir de la fecha de su expedición.

Dado en Pereira, a los veintisiete días del mes de junio del año 2018.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

MARÍA MERCEDES RÍOS AYALA
Delegada del gobernador de Risaralda
Presidente

FRANCISCO JAVIER RAMÍREZ RAMÍREZ
Director administrativo y financiero
Secretario

Elaboró: **CARLOS ANDRÉS VELEZ ESCOBAR**
Contratista

Revisaron: **GUILLERMO LEÓN HENAO FLÓREZ**
Jefe Oficina Control Interno

HERNÁN FELIPE AGUDELO VALENCIA
Director técnico en administración de riesgos