MANUAL DEL SISTEMA ADMINISTRATIVO DEL RIESGO OPERATIVO - SARO DEL INSTITUTO DE DESARROLLO DE ARAUCA – IDEAR

TITULO I
OBJETIVO Y ALCANCE DEL MANUAL SARO

Artículo 1. Sistema Administrativo del Riesgo de Operación. En las actividades que llevan a cabo los INFIS, en sentido financiero y en el contexto de los mercados financieros, persiste con preocupación la buena gestión de recursos y de la administración del riesgo asociada.

La gestión y administración de riesgo operativo se estructura desde la identificación, medición valoración y monitoreo de los eventos de riesgo inherentes y potenciales que pueden generar situaciones adversas al logro de los objetivos institucionales y que por consiguiente deben ser mitigados para evitar la posible materialización de los mismos, es por esto que la aplicación e implementación de metodologías válidas permiten disminuir la probabilidad de ocurrencia y asegurar al instituto en efectividad operatividad.

El sistema de administración de riesgo operativo -SARO- permite agregar valor a la gestión operativa del Idear, toda vez que la actividad sistémica del cumplimiento de su ciclo operacional se desarrolla a la luz de los procesos y da como resultado la generación de conocimiento de las vulnerabilidades y debilidades de los controles del Instituto identificadas por cada uno de los líderes de procesos y como resultado final el mejoramiento continuo de los mismos.

Artículo 2. Objetivo. Desarrollar e implementar en el Idear, un modelo de 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.

- Riesgo Operacional. “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 reputacional, asociados a tales factores.1”

- 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 del Instituto 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 Idear, en el desarrollo de sus operaciones.

[1] Circular Externa 041 del 29 de junio de 2007 de la Superintendencia Financiera de Colombia.

- 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.

  Eventos de Pérdida: Son aquellos eventos que tienen una causalidad de riesgo operativo y se les puede realizar una cuantificación económica.

  Pérdidas Directas: Reconocidas en las cuentas de balance, las cuales se pueden obtener a partir de la información contable de la Entidad. Algunos ejemplos de tipo de pérdidas son los fraudes internos, robos y demás.

  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.

- 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 en los procesos del Instituto.

  Procesos: Todos los procesos y procedimientos identificados con el IDEAR 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 que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses del IDEAR 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, política social, fiscales, monetarias, de desarrollo o bien pueden ser eventos relacionados con inestabilidad política en el país.

  Salud Ocupacional: Conjunto de eventos que puedan afectar el bienestar físico, mental y social de los servidores públicos del IDEAR.

  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 el dinero ilícito parezca lícito.

FT- Es el apoyo financiero, de cualquier forma, al terrorismo o a aquellos que fomenten, planifican o están implicados en el mismo. No obstante, es más complicado definir al terrorismo en sí mismo, porque el término puede tener connotaciones políticas, religiosas y nacionales, dependiendo de cada país.

- 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. Las categorías más usuales definidas son las siguientes:

Fraude interno. Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos del IDEAR o incumplir normas o leyes, en los que está implicado, al menos un empleado o administrador de la entidad. Algunos eventos de Fraude interno pueden ser los siguientes:

a) Desfalco.
b) Recibir coimas o comisiones para ejecutar labores o favorecer en la ejecución de créditos o solicitudes de usuarios del IDEAR
c) Falsas contrataciones de proveedores
d) Deliberado sabotaje a la reputación del IDEAR
e) Robo físico.

Fraude externo. Actos realizados por una persona externa al IDEAR, que buscan defraudar, apropiarse indebidamente de activos de esta o incumplir normas o leyes. Este evento se puede subdividir en los siguientes:

a) Fraudes de falsificación de cheques.
b) Chantaje.
c) Robo.
d) Lavado de dinero.
e) Terrorismo.
f) Daño físico a la propiedad.

Relaciones laborales**.** Actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y en general, la legislación vigente sobre la materia. Este evento se puede subdividir en los siguientes:

Clientes**.** Fallas negligentes o involuntarias de las obligaciones frente a los clientes y que impiden satisfacer una obligación profesional frente a éstos.

Fallas tecnológicas**.** Pérdidas derivadas de incidentes por fallas tecnológicas, todas las interrupciones que se producen en el negocio por motivos tecnológicos y mal funcionamiento del sistema.

Ejecución y administración de procesos: Fallas 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 IDEAR.

Daños a activos físicos**.** Pérdidas derivadas de daños o perjuicios a activos físicos del IDEAR. Este evento se puede subdividir en los siguientes:

a) Incendio.
b) Inundación.
c) Desastres civiles.
d) Falla de energía.

- Riesgo Residual o Neto. Es el nivel resultante del riesgo después de aplicar los controles.

- Riesgo de Corrupción: El riesgo de corrupción es la posibilidad de ocurrencia de una conducta o comportamiento que puede derivar es 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.

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

- Matriz de Riesgo: Herramienta de control y gestión normalmente utilizada para identificar en los procesos y procedimientos, el tipo y nivel de riesgo al que está expuesta inherente al desarrollo de esta actividad, así como los factores internos y externos relacionados con estos riesgos (Factores de riesgo). Igualmente, una matriz de riesgo permite evaluar la efectividad de una adecuada gestión y administración de los riesgos financieros que pudieran impactar los resultados y por ende al logro de los objetivos de una organización.

- Mapa de calor: Herramienta para comparar datos categóricos utilizados mediante color. Generalmente se construyen como una tabla que usa cuadros de colores para representar los datos y un rango continuo de colores según el tipo de escala que se defina. Los mapas de calor le permiten ver variaciones en los datos analizados a través de variaciones de color.

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

- Plan de continuidad del negocio: Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación en caso de interrupción.

TÍTULO II

POLÍTICA PARA LA ADMINISTRACION DEL RIESGO OPERATIVO Y LA CONTINUIDAD DEL NEGOCIO

Artículo 4. Política: Con las siguientes políticas se consideran los riesgos operativos propios de los procesos y actividades desarrolladas al interior del Idear, 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. Es así como las políticas dispuestas son las siguientes:

- 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 RO (potenciales y ocurridos), en todos los procedimientos y procesos que contemplan el Modelo de Operación por Proceso del Idear.

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

- 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 el Consejo Directivo del comportamiento general de estos riesgos y su tendencia en el tiempo.

- Establecer las actividades necesarias que permitan controlar y mitigar el RO. 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 Idear, siendo el insumo principal para establecer el mapa de riesgo residual y perfil de riesgo del Idear.

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

- Idear adoptará un Plan de Continuidad del Negocio enfocado en dar soporte a las actividades desarrolladas en el Instituto, el cual, deberá ser liderado por el área de requerimientos tecnológicos y deber considerar los controles de seguridad, disponibilidad de la información y pasos a seguir en materia de contingencia para cada una de estas actividades.

TÍTULO III
ESTRUCTURA ORGANIZACIONAL, ROLES Y RESPONSABILIDADES EN EL SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO Y PCN

Artículo 5. Estructura Funcional del SARO. Para la adecuada administración del Riesgo Operacional, el Consejo Directivo y la Gerencia del IDEAR son las encargadas de definir y evaluar las políticas generales, encaminadas a garantizar la adecuada Administración del Riesgo Operativo.

La política general del IDEAR es la de poseer una estructura adecuada, que involucre personal idóneo y competente que garantice una eficiente administración del riesgo, su manejo ético y transparente, que favorezca el resultado financiero del Instituto, para el efecto se define la siguiente estructura funcional con sus respectivas responsabilidades:

1. Consejo Directivo
2. Gerente
3. Comité de Riesgos
4. Jefe de Oficina de Riesgos

5. Entes de Control:
    a. Control Interno
    b. Revisoría Fiscal

Artículo 6. Consejo Directivo. El Consejo Directivo es el órgano de dirección permanente del IDEAR, responsable de la administración superior de los negocios y operaciones de la entidad con miras a la realización del objeto social. La definición de los integrantes, funciones y responsabilidades están determinados por los estatutos de la entidad.

Es compromiso institucional del Consejo Directivo definir las políticas sobre los diversos procesos de administración de riesgos, y el de la puesta en marcha de un sistema adecuado de administración de riesgos. La definición de las políticas involucra un conjunto de decisiones institucionales como las estrategias de crecimiento y mercados objetivos.

Dentro de sus funciones estará la de evaluar por lo menos, una vez al año, los modelos operativos aplicables para verificar que dichas metodologías aún sean ajustadas a la necesidad del Instituto.

Respecto al SARO, las siguientes son las competencias más relevantes del Consejo Directivo sin menoscabo de las que se encuentren en los Estatutos.

a) Establecer y aprobar las políticas relativas al SARO.
b) Aprobar los reglamentos, procedimientos y funciones del Instituto.
c) Aprobar el Manual de Riesgo Operativo y sus actualizaciones.
d) Hacer seguimiento y pronunciarse sobre el perfil de riesgo operativo del Instituto.
e) Establecer las medidas relativas al perfil de riesgo operativo, teniendo en cuenta el nivel de tolerancia al riesgo de la entidad, fijado por el mismo Consejo Directivo.
f) Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente el Representante Legal.
g) Pronunciarse sobre la evaluación periódica del SARO, que realicen los órganos de control.
h) Hacer seguimiento sobre los reportes periódicos presentados por el Gerente sobre las medidas correctivas aplicadas para la mitigación de los riesgos operacionales.
i) Aprobar las políticas de inversión que debe verificar el Jefe de Oficina de Riesgos, para identificar y monitorear periódicamente el cumplimiento de las políticas del SARO y comportamiento de este.
j) Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente del SARO.

Artículo 7. Gerente. El Gerente es el responsable ejecutivo del IDEAR, sus funciones generales están definidas en los estatutos del Instituto; en lo que respecta al SARO el Gerente del IDEAR se constituye en un coordinador y dinamizador de las políticas de riesgo; es responsable de la implementación, dirección y control del sistema de administración de riesgo operativo acorde con las metodologías adoptadas por el Consejo Directivo, además de velar por el cumplimiento de los límites y demás políticas establecidas en el presente manual.

Sin perjuicio de las funciones definidas para la Gerencia del IDEAR en el estatuto de la entidad, y que involucran al riesgo operacional, se reconocen las siguientes responsabilidades para la Gerencia:

a) Velar por el cumplimiento efectivo de las políticas establecidas por el Consejo Directivo.

b) Recepcionar y evaluar los informes de seguimiento permanente de las etapas y elementos constitutivos del SARO.
c) Velar porque se implementen estrategias permanentes de las etapas y elementos constitutivos del SARO.
d) Desarrollar y velar porque se implementen estrategias, con el fin de establecer el cambio cultural a la administración del riesgo.
e) Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por el Consejo Directivo.
f) Aprobar los planes de contingencia y de continuidad del negocio, además de disponer de los recursos necesarios para su oportuna ejecución.
g) Presentar un informe periódico, como mínimo semestral, al Consejo Directivo sobre la evolución y aspectos relevantes del SARO, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.
h) Someter a aprobación del Consejo Directivo, el plan de continuidad del negocio y sus correspondientes actualizaciones.
i) Recibir y evaluar los informes presentados por el Jefe de Oficina de Riesgos.
j) Velar porque las etapas y elementos del SARO cumplan, como mínimo, con las disposiciones señaladas en la normatividad vigente.
k) Velar porque se implementen los procedimientos para la adecuada Administración del Riesgo Operativo a que se vea expuesta la entidad en desarrollo de su actividad.
l) Establecer un procedimiento para alimentar el registro de eventos de riesgo operativo, de acuerdo con lo previsto en el numeral 3.2.5 de la Circular Externa 041 de 2007.
m) Informar al Consejo Directivo el resultado anual del plan de continuidad del negocio.

Artículo 8. Comité de Riesgo. En apoyo a la gestión estratégica del Consejo Directivo y la Gerencia, se establece que el Comité de Riesgos tiene como misión la de proponer las políticas y estrategias de mejoramiento sobre diversos procesos de administración del riesgo operacional, así como la evaluación, calificación y control que garanticen la efectividad de dicho sistema. Dentro de sus funciones estará la de evaluar por lo menos una vez al año las metodologías pertinentes.

El Comité de Riesgos está encargado de velar por el cabal cumplimiento de las disposiciones del Consejo Directivo en torno al tema de riesgo, y es un órgano de apoyo estratégico a la labor del Consejo Directivo y de la Gerencia en la definición de políticas y el mejoramiento continuo de la administración integral, activa y preventiva de riesgos.

El Comité tendrá las siguientes funciones*:*

- Proponer a la Gerencia las políticas relativas a la Administración del Riesgo Operacional.
- Establecer y garantizar el efectivo cumplimiento de las políticas aprobadas por el Consejo Directivo.
- Recepcionar y evaluar los informes de gestión presentados por el Jefe de Oficina de Riesgos.
- Son igualmente políticas, impulsar y fortalecer la cultura organizacional en materia de Administrar el Riesgo de Operación, creando una conciencia colectiva sobre los beneficios de su aplicación y sobre los efectos nocivos de su desconocimiento.

Artículo 9. Jefe Oficina de Riesgo. Dentro de la estructura organizacional del IDEAR, el Jefe de Oficina de Riesgos estará bajo la dirección de la Gerencia, y deberá cumplir con la gestión adecuada de los procesos de riesgo a través de las etapas de identificación medición, control y monitoreo. Así mismo, es importante considerar que el Jefe de Oficina de Riesgos tiene el compromiso de revelar oportunamente a las autoridades

competentes, tanto de control interno como externo, los eventos de riesgo que se materialicen y que sean identificados.

Sin perjuicio del cumplimiento de otras disposiciones, el IDEAR cuenta con un Jefe de Oficina de Riesgo, funcional y organizacionalmente independiente, de control interno, su función consiste en administrar todos los riesgos objeto de vigilancia y, además:

- Definir los instrumentos, metodologías y procedimientos tendientes a que la entidad administre efectivamente sus riesgos operativos.
- El Jefe de Oficina de Riesgos es el encargado de Administrar el riesgo, a través del análisis continuo de las situaciones internas y externas, que puedan amenazar la estabilidad y crecimiento de la organización o que propicien cambios en las políticas definidas.
- Desarrollar e implementar el sistema de reportes, internos y externos, del riesgo operativo de la entidad.
- Administrar el registro de eventos de riesgo operativo.
- Coordinar la recolección de la información para alimentar el registro de eventos de riesgo operativo.
- Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los riesgos operativos medidos.
- Establecer y monitorear el perfil de riesgo de la entidad e informarlo al órgano correspondiente.
- Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con el SARO, y proponer sus correspondientes actualizaciones y modificaciones.
- Desarrollar los modelos de medición del riesgo operativo.
- Desarrollar los programas de capacitación de la entidad relacionados con el SARO.
- Realizar seguimiento a las medidas adoptadas para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.
- Reportar semestralmente al Representante Legal la evolución del riesgo, los controles implementados y el monitoreo que se realice sobre el mismo, en los términos de la Circular 041 de 2007.
- El Jefe de Oficina de Riesgos, desarrollará e implementará planes de contingencia para asegurar la continuidad de los procesos.
- Los eventos de Riesgo que se materialicen deben ser reportados y revelados, contable y posteriormente llevados al comité de riesgo.
- Informar al Comité de Riesgos o en su defecto al Consejo Directivo sobre los siguientes aspectos:
- Informar mensualmente al comité de riesgos sobre el comportamiento del riesgo operacional del IDEAR.
- Verificar que los controles cumplan efectivamente con su función de mitigar el riesgo.
- Establecer programas de capacitación relacionados con la efectiva administración de riesgos, para todos los funcionarios del Instituto, en colaboración de Talento Humano y la Gerencia.
- Liderar la difusión de la cultura de administración de riesgo operacional.

Artículo 10. Control Interno. IDEAR cuenta con un asesor de Control Interno, quien, respecto al SARO, es quien adelantará 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 del riesgo 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 11. Revisor Fiscal. El Revisor Fiscal tiene la responsabilidad, de acuerdo con la Ley y con normas de Auditoría aceptadas, de evaluar si tal administración del Riesgo Operativo está de acuerdo con las normas que le apliquen al IDEAR y las mejores prácticas de la industria.

Sin perjuicio de las normas que le asigna el Código de Comercio y la normatividad expedida por parte de la Superintendencia Financiera de Colombia, serán funciones de la Revisoría Fiscal las siguientes:

a) Incluir dentro de su plan de actividades, la auditoría al Sistema de Riesgo Operativo de la Entidad y formular las recomendaciones que considere pertinentes.
b) Elaborar un reporte al cierre de cada ejercicio contable, en el que informe al Consejo Directivo acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos establecidos sobre el SARO.
c) Poner en conocimiento del Representante Legal los incumplimientos del SARO.

El Revisor Fiscal es el órgano de control encargado de reportar al Consejo Directivo acerca de las desviaciones en el cumplimiento de los instructivos externos e internos, de las deficiencias en los controles internos sobre esta materia, así como de las irregularidades encontradas, que surjan como resultado del examen del SARO. Estos aspectos deberán quedar suficientemente documentados en los papeles de trabajo y en los informes presentados.

TÍTULO IV
UNIDADES DE APOYO AL SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO DE IDEAR

Artículo 12. Oficina de Requerimientos Tecnológicos: Le corresponde todo lo relacionado con la identificación de riesgos operativos relacionados con tecnología y el liderazgo de la implementación del PCN del Idear:

- Liderar la recuperación tecnológica, basada en la estrategia de continuidad definida.
- Identificar y valorar los posibles riesgos tecnológicos que puedan afectar la continuidad de la operación normal del Instituto.
- Mantener comunicación constante con los demás actores del PCN durante el estado de contingencia, informando el estado de recuperación de esta a la cadena de mando establecida para su atención.
- Asegurar la seguridad y continuidad de la información, así como oportunidad de esta.
- Implementar las acciones correspondientes a la recuperación y puesta a punto de la información en los establecidos dentro del PCN.
- Informar oportunamente a la administración de los eventos que por su nivel de severidad afecten la continuidad del negocio y requieran de tratamiento especial.
- Efectuar monitoreo continuo a las acciones y tratamientos implementados como medidas de aseguramiento de los procesos críticos del Instituto.
- Valorar y determinar el nivel de vulnerabilidad y posibles eventos vandálicos informáticos en los que pueda verse involucrado el Instituto.
- Medir permanentemente la efectividad de los controles implementados y solicitar los ajustes y modificaciones en caso de requerirse.

- Asegurar la capacitación y entrenamiento del personal de sistemas.
- Asegurar que las personas involucradas en todas las etapas del PCN tengan una correcta y adecuada capacitación en ese tema.
- Coordinar, apoyar y hacer seguimiento a la gestión del PCN de cada área.
- Efectuar y valorar el resultado de las pruebas efectuadas.

Artículo 13. Líderes de procesos y procedimientos:

- Identificar y valorar riesgos, controles y planes de acción en cada uno de sus procesos y procedimientos.
- Mantener una aversión al riesgo en todas sus actuaciones.
- Conservar una posición prudente en la administración de los recursos públicos, los cuales deben ser asegurados y expuestos al menor riesgo posible.
- Impulsar y promover la cultura del riesgo operativo para el personal a su cargo como un hábito en todos los procesos y actividades que se ejecuten.
- Participar en el control y mitigación de los riesgos a los cuales se encuentren expuestos sus procesos.
- Conservar en un nivel óptimo de actualización las matrices de riesgo operativos de los procedimientos a su cargo.
- Establecer y conocer el nivel de exposición de riesgo operativo en que se encuentra los procedimientos a su cargo.
- Articular la estrategia institucional con la gestión y administración de riesgos operativos.
- Solicitar oportunamente al área encargada de la documentación de los procedimientos, las actualizaciones debidas, cuando se identifiquen desviaciones de estos.
- 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.
- Buscar por el control y mitigación de los riesgos presentes en sus procesos.
- Ejecutar de manera oportuna los planes de acción que se establezcan para la mitigación de riesgos operativos en su área.

Artículo 14. Servidores públicos y contratistas del Idear:

-Reportar oportunamente los eventos de RO que ocurran en el transcurso diario de sus actividades, según lo indicado en la metodología para tan fin.
- Conservar plena conciencia de que los recursos públicos deben ser asegurados y expuestos al riesgo en la menor medida posible.
- Adoptar la cultura de autocontrol y mitigación de RO en todas las actividades diarias.
- Participar, presentar y aprobar la capacitación que se brinde en materia de RO en el Instituto.

TÍTULO V
LINEAMIENTOS DE ADMINISTRACIÓN DEL RIESGO OPERATIVO

Artículo 15. Límites de exposición de riesgo operativo. El siguiente mapa de calor, determina la 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)
CASI SEGURO (5)	A	A	E	E	E
PROBABLE (4)	M	A	A	E	E
POSIBLE (3)	B	M	A	E	E
IMPROBABLE (2)	B	B	M	A	E
RARO (1)	B	B	M	A	A

Donde las estrategias se definen según su nivel de severidad, en los siguientes términos:

SEVERIDAD	ESTRATEGIA
BAJA (B)	Asumir el riesgo y conservar un monitoreo permanente sobre los mismos, pueden implementarse controles sencillos asegurados 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 de este, dejando claro tiempos y formar, 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 de este, coordinación con el responsable del proceso de las valoraciones de las actividades pertinentes.

Artículo 16. Identificación: Los líderes de proceso y procedimiento, 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 17. Áreas de Impacto: El Idear establece como áreas 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:

-Pérdidas económicas /Costo de oportunidad
-Seguridad de la información.
-Operativo.
-Continuidad del negocio
-Atención al cliente
-Legal

Artículo 18. Medición. La medición de los riesgos será realizada contemplando la frecuencia y el impacto de estos, obteniendo así la medición individual. Lo anterior, permitirá realizar una consolidación de todos los riesgos identificados para poder establecer el mapa de riesgo inherente del Instituto.

El Idear en su desarrollo metodológico establecerá la categoría 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 técnico-soportada.

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

Artículo 19. Seguimiento: El seguimiento debe estar direccionado 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 el Comité de Riegos 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 20. Control. Deben establecerse los procesos y procedimientos necesarios que permitan controlar y mitigar el RO. Es así como el conocimiento, actuaciones e implementación de las medidas de control respectivas recae sobre cada uno de los integrantes de las diferentes áreas del Idear, siendo el insumo principal para establecer el mapa de riesgos residual y perfil de riesgo del Idear.

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

De calificarse la oportunidad, efectividad y eficiencia de estos.

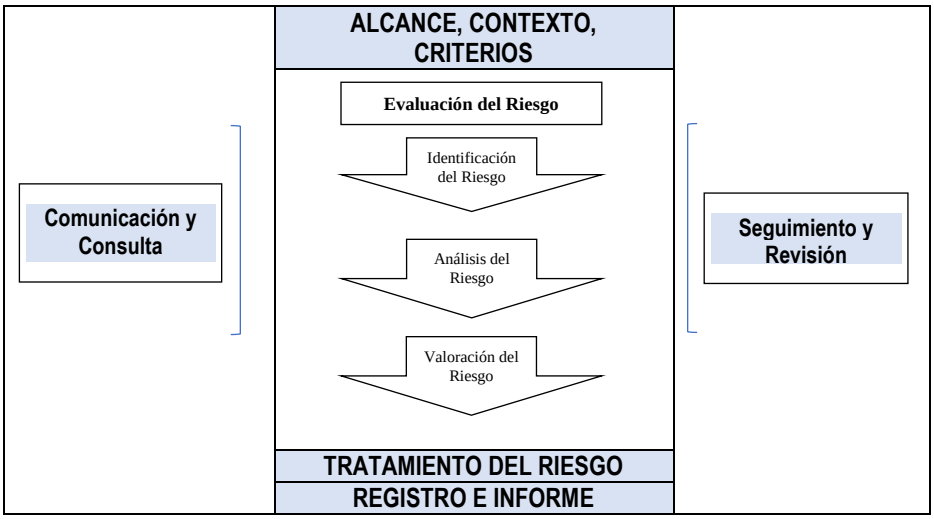
TÍTULO VI
METODOGOLOGÍA DE IMPLEMENTACIÓN DEL SARO

Artículo 21. Metodología. Para adoptar las políticas del presente manual, el Idear adopta e implementa mejores prácticas propuestas en estándares internacionales como lo son el Comité de Basilea 2, la NTC 5254, la ISO 31000: 2018, así como las directrices impartidas en materia de riesgo operativo por el Departamento Administrativo de la Función Pública -DAFP.

La Oficina de Riesgos es la dependencia encargada de diseñar, implementar, y realizar seguimiento a la implementación de este sistema de administración del riesgo en IDEAR.

Una implementación exitosa de un Sistema de Administración de Riesgo Operativo debe estar sustentado en la consolidación de una cultura de "Mitigar Riesgos", que debe permitir 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 los funcionarios de la entidad.

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:



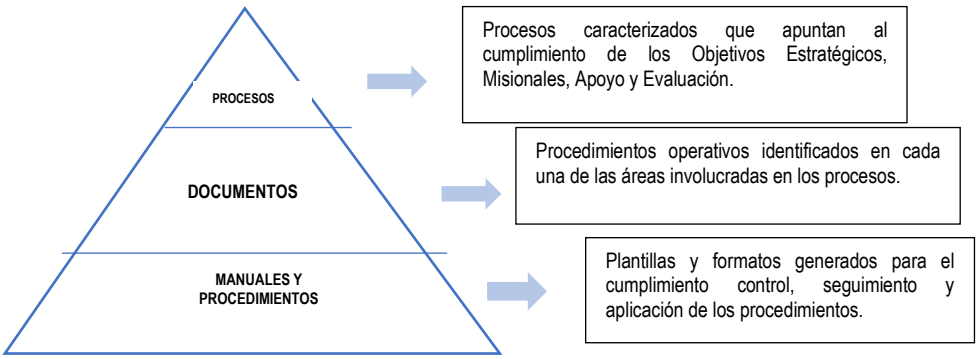
Fuente: ISO 31000:2018

Artículo 22. Alcance, contexto y criterios. El establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo. El alcance, el contexto y los criterios implican definir el alcance del proceso, y comprender los contextos externos e internos.

El Idear en la construcción y elaboración de los Planes Estratégicos Institucionales vigentes 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, definiendo los parámetros externos e internos que se considerarán a la gestión del riesgo y establecer el alcance y los criterios para el desarrollo del proceso.

Ahora bien, para cumplir los objetivos estratégicos descritos, el Idear realiza su gestión operativa a través de un modelo de operación por proceso (MOP), categorizándolos de la siguiente manera:



Parágrafo 1. Procesos: Cada entidad con el fin de dar cumplimiento a su misión, estructura cada uno de sus procesos, Idear formuló los suyos, según la siguiente calificación:

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 Idear, 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 Idear. Así como su nivel de competitividad con el propósito de anticipar y decidir sobre el direccionamiento de la organización hacia el futuro.

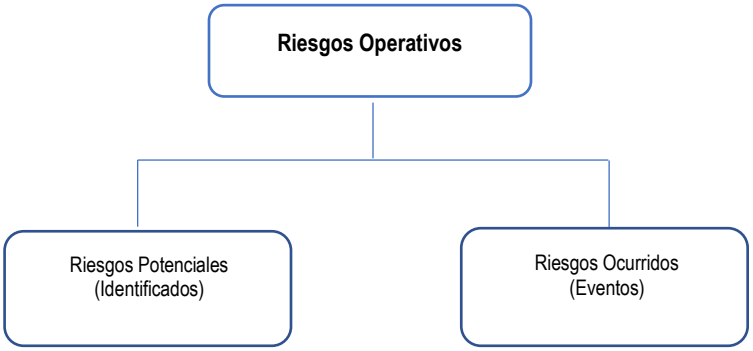
Procesos de apoyo: Son los procesos que respaldan y proveen de diferentes recursos a los misionales, estratégicos y de evaluación, generando valor agregado al Idear.

Proceso 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.

TÍTULO VII
EVALUACIÓN DEL RIESGO

Artículo 23. Identificación del riesgo: La identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.

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



Parágrafo 1: Riesgos Potenciales: Estos riesgos son identificados y utilizados como herramienta principal, conforme a los conocimientos que tienen cada uno de los líderes de los procesos y procedimientos existente en el MOP del Idear, partiendo de los siguientes cuestionamientos:

- ¿Qué puede suceder?
- ¿Cómo puede suceder y por qué?

Esta identificación debe estar orientada y acompañada por la Oficina de Riesgos y debe quedar diligenciada en el formato "Mapa de Riesgos", o en la herramienta que se disponga para tal fin, garantizando la posterior administración y seguimiento a los controles, tratamientos e indicadores de los riesgos identificados.

Para ello se tendrá en cuenta un Mapa de Riesgo, que contará como mínimo con los siguientes conceptos:

-Proceso: Se debe identificar qué proceso se afecta en la identificación del riesgo o potencial riesgo.

- Nombre del Riesgo: Hace referencia al riesgo identificado por el líder del procedimiento, se debe identificar de manera clara el nombre del riesgo conforme a los procesos definidos en la entidad.

- Tipología del Riesgo: Fuente generadora de riesgo de acuerdo con las definidas en el presente manual, estas pueden ser:

Riesgos Financieros: Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas al proceso tales como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

Riesgos Operativos: Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad, son eventos provenientes del funcionamiento y operatividad de los sistemas de información de la entidad.

Riesgos Estratégicos: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.

Legal o de Cumplimiento: Se asocian con el cumplimiento por parte de la entidad con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgos Tecnológicos: Están relacionados con la posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

Riesgos de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio particular.

Riesgo de Imagen: Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.

Riesgo de liquidez: Contingencia de no poder cumplir plenamente, de manera oportuna y eficiente los flujos de caja esperados e inesperados, vigentes y futuros, sin afectar el curso de las operaciones diarias o la condición financiera de la entidad.

Riesgo de mercado: Posibilidad de que las entidades incurran en pérdidas asociadas a la disminución del valor de sus portafolios, la caída del valor de la cartera colectiva o fondos que administran, por efecto de cambios en el precio de los instrumentos financieros en los cuales se mantienen posiciones. Además, se debe tener en cuenta lo dispuesto en el Manual del Sistema Administrativo de Riesgo de Mercado del Instituto de Desarrollo de Arauca.

Riesgo de lavado de activos y financiamiento del terrorismo: Posibilidad de pérdida o daño que puede sufrir una entidad vigilada por su propensión a ser utilizada directamente o a través de sus operaciones, como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

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

- **Consecuencias Potenciales:** Describir brevemente cual es el impacto que puede tener la materialización de este riesgo, puede ser económico, cualitativo o cuantitativo.

- **Riesgo Inherente:** Son los riesgos que están inmersos en el desarrollo del objeto social del instituto.

- **Controles existentes:** Se deben describir cada uno de los mecanismos, implementados en la entidad, con el fin de mitigar los efectos del riesgo inherente.

- **Riesgo Residual:** Es el riesgo que resultado de aplicar los diferentes controles dispuestos en la entidad.

- **Opción de Manejo:** Son las alternativas con las que cuenta la entidad, frente al Riesgo Inherente, Reducir, Mitigar, Compartir, Aceptar.

- **Acciones preventivas:** Se consagran todas las acciones con las que dispone la entidad para mitigar la materialización de un riesgo.

- **Responsables**: Se debe indicar el líder de proceso o funcionario de la entidad responsable de adelantar las acciones necesarias en la no materialización del riesgo.

- **Acción de contingencia:** Se refiere a cada una de las acciones que se deben implementar con el ánimo de retomar la normal operación de la entidad y subsanar el evento ocurrido.

Parágrafo 2. Riesgos Ocurridos: Para poder dar un mejor control del comportamiento de los eventos de riesgo que se materializan en la operatividad diaria del Idear, 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 estos.

El registro de eventos de RO tiene los siguientes objetivos:

- Desarrollar estrategias de mitigación ante la materialización de estos.
- Generar conciencia en los costos resultantes de situaciones de riesgo que impactan negativamente los resultados del Idear.
- Construir una base de datos que permita cuantificar la exposición al RO 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 mejora en áreas y/o procesos del Idear.

Deben registrarse todos los eventos ocurridos, así generen o no pérdida por parte del Líder o cualquier funcionario de acuerdo con el formato de reporte diario de eventos.

La base de datos deber ser administrada por la oficina de riesgos de la entidad y deberán ser revisados por lo menos una (1) vez al año.

Artículo 24. Análisis del Riesgo: El análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel de riesgo. El análisis implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos.

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 las bases de datos de RO.

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 Idear la materialización de estos, bien sea por la frecuencia de ocurrencia o por el impacto.

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

Teniendo en cuenta que la Gestión del RO es un proceso que agrega valor al Idear, 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 del riesgo se alinea a los objetivos estratégicos de administrar eficientemente la estructura de gastos y aumentar la capacidad de gestión institucional.

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.

Artículo 25. Probabilidad (frecuencia de ocurrencia): La valoración de la probabilidad de la ocurrencia del riesgo se establecerá mediante los criterios construidos en la correspondiente matriz y se expondrán en el procedimiento respectivo.

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de ocurrencia o factibilidad, donde ocurrencia implicará analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda. Bajo el criterio de Probabilidad, el riesgo se debe medir a partir de las siguientes especificaciones:

Se establecerán las escalas de valoración bajo 5 niveles, los cuales buscarán cubrir las posibles asignaciones de medición de este componente.

La fijación de las tablas de valoración permanecerá por periodos máximo de 1 año, permitiendo la estabilización de los criterios de medición.

La escala de ocurrencia a utilizar es la siguiente:

ID	ESCALA	PROBABILIDAD DE OCURRENCIA	DESCRIPCIÓN
1	Raro	2 o menos veces al año	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).
2	Improbable	Entre 3 y 4 veces al año	El evento puede ocurrir en algún momento.
3	Posible	Entre 5 y 10 veces al año	El evento podrá ocurrir en algún momento.
4	Probable	Entre 11 y 24 veces al año	Es viable que el evento ocurra en la mayoría de las circunstancias.
5	Casi Seguro	Mas de 24 veces al año	Se espera que el evento ocurra en la mayoría de las circunstancias.

Artículo 26. Impacto (Consecuencia en caso de materialización): El impacto puede ser cualitativo o cuantitativo según el riesgo identificado o el evento ocurrido, para esto, el Idear define en el respectivo procedimiento 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 y la estrategia definida en el presente manual dice:
Lo anterior, debe ser registrado en el Mapa de Riesgos del Idear.

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

	Pérdida económica/ Costo oportunidad Hasta X% del PT	Seguridad de la información	Operativo	Continuidad del Negocio	Atención al Cliente	Legal
No significativo	0,005%	Uso inadecuado de información pública.	No existe interrupciones de las operaciones de la entidad.	No existe interrupción de las operaciones.	Se ven afectados hasta 3 clientes.	No conformidades por órganos de control interno.
Menor	0,015%	Divulgación de información no oficial.	El proceso dura unas horas.	La interrupción del negocio dura unas horas.	Se ven afectados entre 4 y 6 clientes.	Incumplimientos contractuales. Investigaciones disciplinarias internas.
Moderado	0,050%	Divulgación de información de clientes.	El proceso dura un (1) día.	La interrupción del negocio dura un (1) día.	Se ven afectados entre 7 y 15 clientes.	Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.
Mayor	2.00%	Pérdida de información de clientes.	El proceso dura más de dos (2) días.	La interrupción del negocio dura más de dos (2) días.	Se ven afectados entre 16 y 30 clientes.	Sanciones por parte de órganos de control y vigilancia.
Catastrófico	5.00%	Pérdida total de la información de la entidad, lo cual implica el incumplimiento de las metas institucionales.	El proceso dura más de 5 días	La interrupción del negocio de más de 5 días.	Se ven afectados más de 30 clientes.	Intervención por parte de un ente de control u otro ente regulador.

Artículo 27. Valoración del Riesgo: Busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL). Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

- **Riesgo antes de controles (Riesgo Inherente).** Se identifican los riesgos inherentes o subyacentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso.
- **Causas o fallas.** Se identifican las causas o fallas que pueden dar origen a la materialización del riesgo.
- **Controles**. Para cada causa se identifica el control o controles.
- **Riesgo después de controles (Riesgo Residual)**. Evaluar si los controles están bien diseñados para mitigar el riesgo y si estos se ejecutan como fueron diseñados.

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 de límites definida en el presente manual, siendo el siguiente:

PROBABILIDAD	IMPACTO				
	NO SIGNIFICATIVO (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
CASI SEGURO (5)	A	A	E	E	E
PROBABLE (4)	M	A	A	E	E
POSIBLE (3)	B	M	A	E	E
IMPROBABLE (2)	B	B	M	A	E
RARO (1)	B	B	M	A	A

SEVERIDAD	ESTRATEGIA
BAJA (B)	Asumir el riesgo y conservar un monitoreo permanente sobre los mismos, pueden implementarse controles sencillos asegurados 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 de este, dejando claro tiempos y formar, 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 de este. coordinación con el responsable del proceso de las valoraciones de las actividades pertinentes.

Artículo 28. Nivel del riesgo residual. Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).

Tenemos el riesgo 1 con una calificación de riesgo inherente de probabilidad e impacto como se muestra en la siguiente gráfica:

PROBABILIDAD	IMPACTO				
	NO SIGNIFICATIVO (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)

CASI SEGURO (5)	A	A	E	E	E
PROBABLE (4)	M	A	A	E **R1**	E
POSIBLE (3)	B	M	A	E	E
IMPROBABLE (2)	B	B	M	A	E
RARO (1)	B	B	M	A	A

Como podemos observar, es probable que el riesgo suceda y, en caso de materializarse, tiene un impacto mayor para la entidad. Ahora, supongamos que existen controles bien diseñados, que siempre se ejecutan, y que estos controles disminuyen de manera directa la probabilidad.

PROBABILIDAD	IMPACTO				
	NO SIGNIFICATIVO (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
CASI SEGURO (5)	A	A	E	E	E
PROBABLE (4)	M	A	A	E	E
POSIBLE (3)	B	M	A	E	E
IMPROBABLE (2)	B	B	M **R1**	A	E
RARO (1)	B	B	M	A	A

En nuestro ejemplo disminuiría dos cuadrantes de probabilidad, pasa de probable a improbable y un cuadrante de impacto, pasa de mayor a moderado.

Artículo 29. Controles. La entidad, cuenta con categorías de control de mayor aplicación, siendo las siguientes:

CONTROL DE GESTIÓN	Políticas claras aplicadas
	Seguimiento al plan estratégico y operativo
	Indicador de gestión
	Tableros de gestión
	Seguimiento de cronogramas
	Evaluación del desempeño
	Informe de gestión
	Monitoreo de riesgos
CONTROLES OPERATIVOS	Conciliaciones
	Consecutivos
	Verificación de firmas
	Lista de chequeo
	Registro controlado
	Segregación de funciones
	Niveles de autorización
	Custodia apropiada
	Procedimientos formales aplicados
	Pólizas
	Seguridad física
	Contingencias y respaldos
	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:

MITIGA:

- **Probabilidad:** El control ejecutado disminuye la cantidad de veces en que se presenta el riesgo.
- **Impacto:** El control ejecutado disminuye los posibles inconvenientes que presente el riesgo.

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.

- Persuasivo. Tipo de control que pretende convencer al responsable de efectuar la actividad que mitigue el riesgo.

ESTADO DE CONTROL:

- **Implementado y documentado:** Durante la identificación de riesgos el control se encuentra en funcionamiento y documentado.
- **Implementado y 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 adelantando su puesta en marcha.
- **No implementado y documentado:** Durante la identificación de riesgos, el control no se encuentra en funcionamiento, pero si está documentado.

EJECUCIÓN DEL CONTROL:

- **Siempre:** El control se ejecuta cada vez que se realiza el procedimiento.
- **En la mayoría de las veces:** El control se ejecuta la mayoría de las veces en que se realiza el procedimiento.
- **Solo algunas veces:** El control se ejecuta ocasionalmente.
- **Nunca:** El control de ningún modo se ha ejecutado.

EVIDENCIAS DEL CONTROL:

- En medios digitales: Siempre queda evidencia de la ejecución del control.
- **Física y digital:** Siempre queda evidencia de la ejecución del control.
- Solo física: algunas veces queda evidencia de la ejecución del control.
- **No se evidencia:** No existe ninguna evidencia de la ejecución del control.

Artículo 30. Criterios de calificación de los controles identificados:

Al momento de definir si un control o controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción de este, las siguientes variables:

a) Debe tener definido el responsable de llevar a cabo la actividad de control.
b) Debe tener una periodicidad definida para su ejecución.
c) Debe indicar cuál es el propósito del control.
d) Debe establecer cómo se realiza la actividad de control.
e) Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
f) Debe dejar evidencia de la ejecución del control.

Mitiga 15	Realización 15	Tipo 15	Estado 20	Ejecución 20	Evidencia 15
Probabilidad 15	Automático 15	Preventivo 15	Implementado y Documentado 20	Siempre 20	Física y Digital 15
Impacto 0	Semiautomático 9.90	Detectivo 9.90	Implementado y no Documentado 13.22	La mayoría de las veces 13.20	En medios digitales 9.90
	Manual 4.95	Correctivo 4.95	En desarrollo 6.60	Algunas veces 6.60	Solo física 4.95
		Persuasivo 3	No Implementado y documentado 0	Nunca 0	No se evidencia 0

Rango de Ponderación	Calificación del Diseño del Control
Mayor o igual a 60%	Fuerte
Mayor o igual a 30%y menos a 60%	Moderado
Menor a 30%	Débil

Fuerte: El control está bien diseñado para mitigar el riesgo.

Moderado: El control tiene oportunidades de mejora en el diseño.

Débil: El control tienen debilidades significativas en su diseño para mitigar en forma adecuada la causa o falla.

Es así como se recomienda la evaluación de cada control de la siguiente manera:

		EVALUACIÓN DE CONTROLES						CÓDIGO: XX VERSIÓN: XXX FECHA: XX PÁGINA: XXX		
Id Riesgo	**Riesgo**	**Id Control**	**Control**	**Mitiga**	**Realización**	**Tipo**	**Estado**	**Ejecución**	**Evidencia**	**Calificación del Control**

Artículo 31. Valoración del riesgo. Busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL). Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

- **Riesgo antes de controles (Riesgo inherente).** Se identifican los riesgos inherentes o subyacentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso.
- **Causas o fallas.** Se identifican las causas o fallas que pueden dar origen a la materialización del riesgo.
- **Controles**. Para cada causa se identifica el control o controles.
- **Riesgo después de controles (Riesgo residual)**. Evaluar si los controles están bien diseñados para mitigar el riesgo y si estos se ejecutan como fueron diseñados.

Artículo 31. Tratamiento del riesgo y seguimiento: El tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo. La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos, esfuerzo o desventajas de la implementación.

Como resultado de los riesgos identificados, y según la estrategia definida para cada nivel de severidad, se establecen los planes de seguimiento que mitigan el riesgo, estos planes de acción deben quedar identificados y enlistados en el Mapa de Riesgos.

Cada uno de estos, debe indicar una fecha de cumplimiento establecida para realizar su implementación, y responsable, los cuales deben quedar documentados.

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. La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

El Instituto acepta los riesgos residuales ubicados en zona baja del mapa de calor y ningún riesgo de corrupción podrá ser aceptado. En este caso, se formulará el respectivo plan de acción y su responsable.

a) **Mitigar el riesgo**. El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

En el Instituto se adoptarán medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo que el riesgo residual conlleva a la implementación de acciones preventivas.

b) **Evitar el riesgo**. Cuando los escenarios de riesgo identificados se consideran demasiado extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

Cuando no es una opción eliminar la actividad, el Comité de Riesgos analizará en detalle los controles o las acciones preventivas a aplicar para evitar su materialización.

c) **Transferir el riesgo**. Se reduce la probabilidad o el impacto del riesgo y se transfiere o comparte una parte de este. Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

En el Instituto, los mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual o figura legal, haciendo el seguimiento correspondiente.

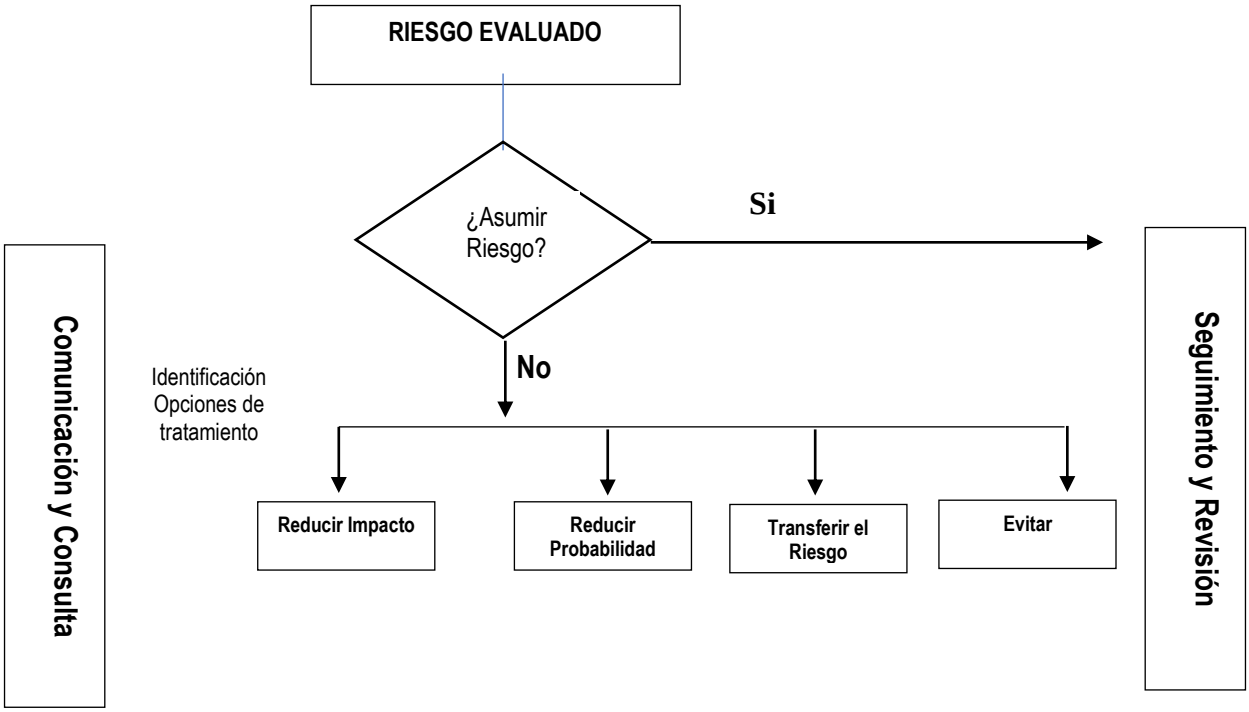
Dependiendo del nivel de riesgo, el tratamiento a seguir se muestra en el siguiente gráfico o de la decisión que tome el responsable del proceso.

APETITO DEL RIESGO	PROBABILIDAD	IMPACTO				
		NO SIGNIFICATIVO (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
	CASI SEGURO (5)	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar
	PROBABLE (4)	Aceptar / Mitigar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar
	POSIBLE (3)	Aceptar	Aceptar / Mitigar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar
	IMPROBABLE (2)	Aceptar	Aceptar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar
	RARO (1)	Aceptar	Aceptar	Aceptar / Mitigar	Transferir/Mitigar / Evitar	Transferir/Mitigar / Evitar
APETITO DEL RIESGO						

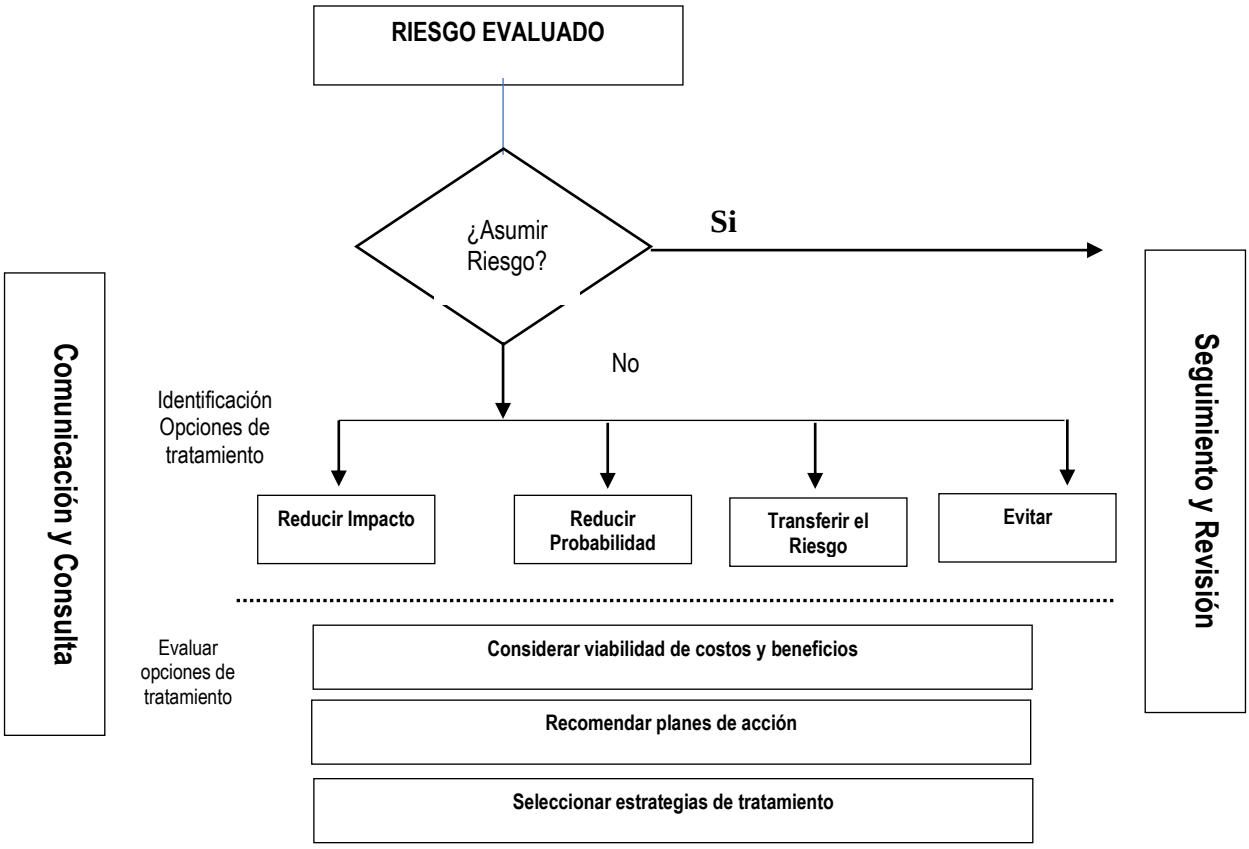
Artículo 32. Recomendaciones: La oficina de riesgo, durante el seguimiento a los eventos de riesgo y de conformidad a las inspecciones realizadas, emitirá recomendaciones atendiendo a los niveles de riesgo, conservando los siguientes criterios:

CLASIFICACIÓN DE LAS RECOMENDACIONES		SEVERIDAD DEL RIESGO
1. CRÍTICA	Recomendación de indispensable cumplimiento, considerando la existencia de un peligro inminente que puede generar afectaciones repentinamente. Debe considerarse como un requerimiento a corto plazo (de 1 a 3 meses).	EXTREMA
2. NECESARIAS	Recomendación para mantener un estado de seguridad y prevención aceptable considerando la existencia de deficiencia evidentes. Debe considerarse como un requerimiento a mediano plazo (de 6 meses a un (1) año).	ALTA
3. IMPORTANTE	Recomendación importante pero no urgente, se emite cuando se pretende sugerir ante una situación que, si bien no es inminente, si puede traer inherentes situaciones adversas. Debe considerarse como un requerimiento de mediano a largo plazo (un año a dos años).	MODERADA
4. COMPLEMENTARIA	Recomendación de carácter opcional, se emite cuando se identifican oportunidades de mejora. Debe considerarse como un requerimiento sujeto de los costos que genera su implantación.	BAJA

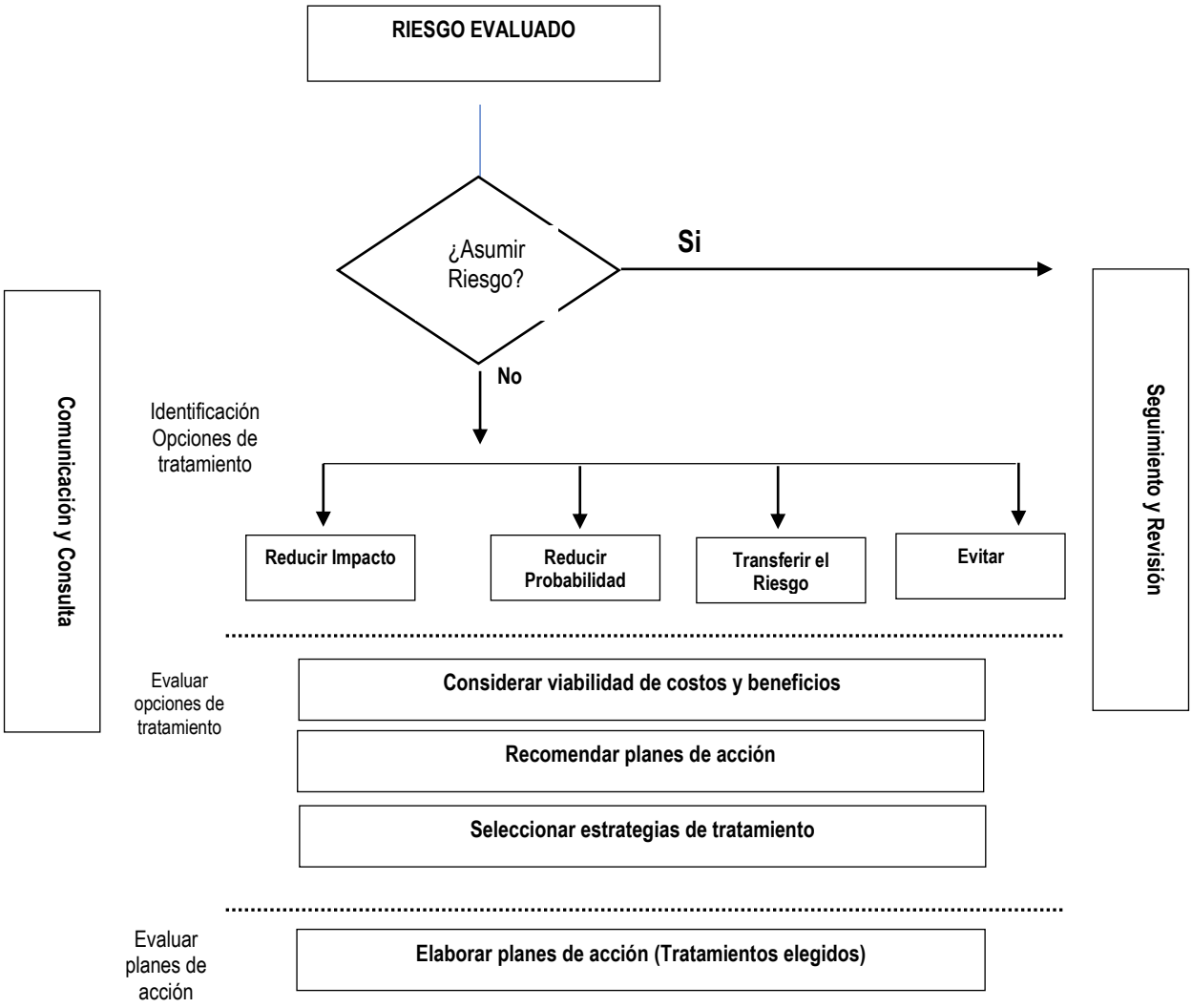
Artículo 33. Planes de Acción: Una vez evaluados y valorados los diversos riesgos, los tratamientos o planes de acción deben seguir la siguiente estructura para su creación, desarrollo y ejecución, teniendo como principal pilar el monitoreo y revisión, así como su comunicación y permanente consulta, por lo cual, según la estrategia a seguir según su severidad (definida previamente) el proceso continuaría de la siguiente manera:



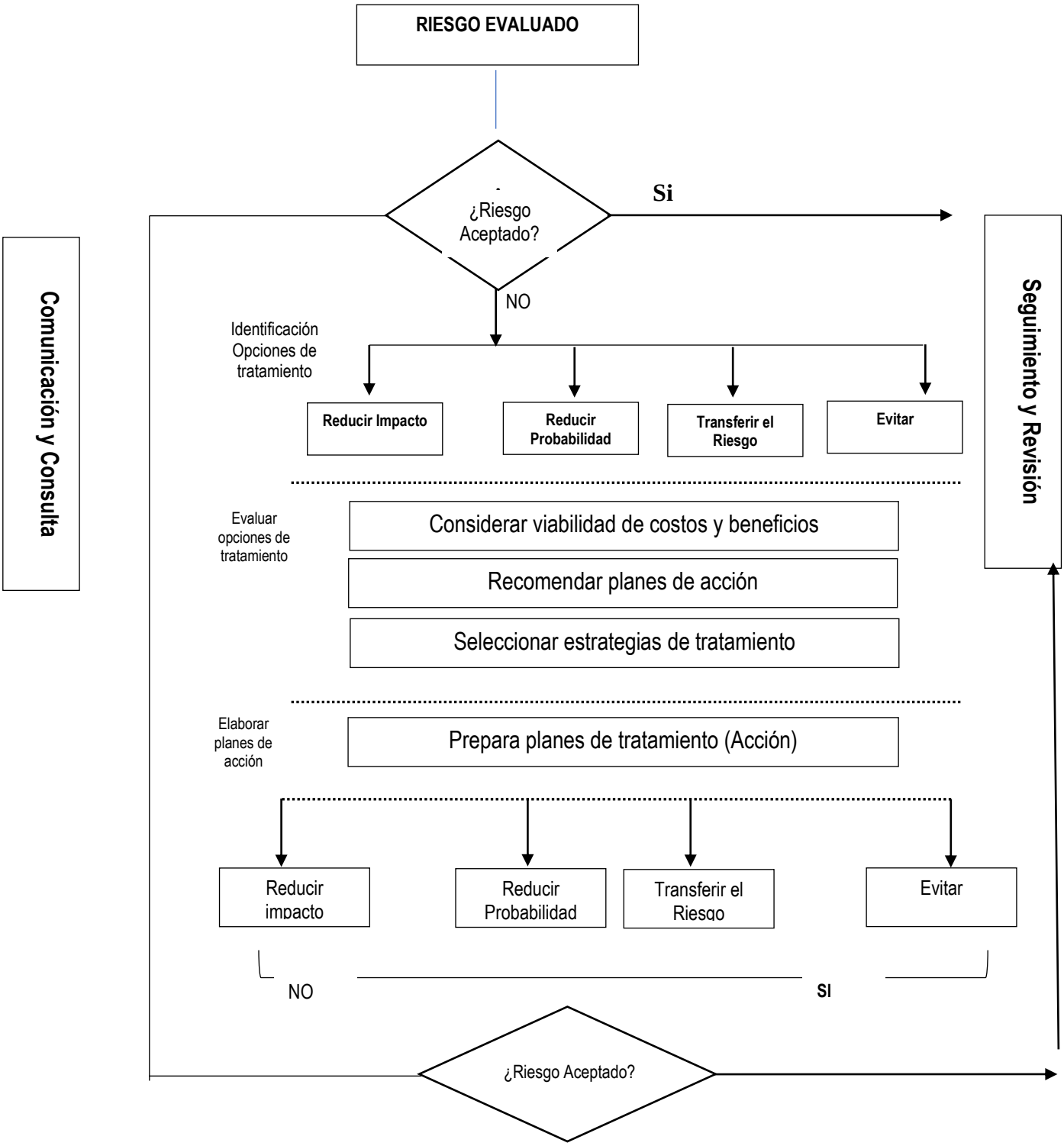
Una vez identificadas las opciones de tratamiento (Reducir Impacto, Reducir Probabilidad, Transferir el Riesgo o Evitar Completamente), debe procederse con la evaluación de las diferentes opciones de tratamiento, teniendo en cuenta la viabilidad de este en una relación costo- beneficio, definir los planes de acción e 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 Riesgos.



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


RIESGO EVALUADO
¿Riesgo Aceptado?
Si
NO
Comunicación y Consulta
Seguimiento y Revisión
Identificación Opciones de tratamiento
Reducir Impacto
Reducir Probabilidad
Transferir el Riesgo
Evitar
Evaluar opciones de tratamiento
Considerar viabilidad de costos y beneficios
Recomendar planes de acción
Seleccionar estrategias de tratamiento
Elaborar planes de acción
Prepara planes de tratamiento (Acción)
Reducir impacto
Reducir Probabilidad
Transferir el Riesgo
Evitar
NO
SI
¿Riesgo Aceptado?

Una Vez determinados los tratamientos y planes de acción, estos deben ser incluidos en el "Formato de Identificación y Seguimiento de Tratamientos y Planes de Acción, el cual debe ser diligenciado y entregado ante el comité de riesgos.

idear OPORTUNIDADES PARA TODOS		IDENTIFICACIÓN Y SEGUIMEINTO A PLANES DE ACCIÓN					CÓDIGO VERSIÓN FECHA PÁGINA	
No	Tratamiento (Plan de Acción)	Riesgo Cubierto	Responsable	Fecha de Implementación	Fecha de Seguimiento 1	Observación	Fecha de Seguimiento 2	Observación

Artículo 34. Seguimiento y Revisión: El seguimiento contribuye a mejorar la calidad y la eficiencia del diseño, la implementación y los resultados, del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados deberían ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

El seguimiento y la revisión deberían tener lugar en todas las etapas del proceso. El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.

Los resultados del seguimiento y la revisión deberían incorporarse a todas las actividades de gestión del desempeño, de medición y de informe de la organización.

El seguimiento a los riesgos debe estar consignado con el plan de auditorías a realizarse por control interno.

De igual manera la oficina de riesgos debe realizar un constante monitoreo y seguimiento a los eventos ocurridos, para poder ajustar el mapa de riesgo.

Este monitoreo y seguimiento se debe realizar mediante la implementación y ejecución de planes de seguimiento, 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 se sirvan como enlace entre el riesgo y su mitigación/control, permitiendo explicar el nivel de exposición del riesgo en función del esfuerzo impuesto en su mitigación o control.

Los planes 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 su pueden clasificar en:

CAUSALES: Indicadores relacionados con monitorear las causas identificadas del riesgo.
DE CONTROL: Indicadores relacionados a efectuar seguimiento a los controles o mitigar el 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 Idear, es este caso los créditos de fomento.

- DE ENTORNO: Depende de factores externos ajenos a las condiciones del mercado, políticos, sociales, culturales, etc.

Artículo 35. Lineamientos para el diseño e implementación de planes de seguimiento:

- Deben referirse a parámetros observables cuyo comportamiento guarde estrecha relación con el riesgo asociado.
- Deben tener lógica y ser consciente que la utilización de estos no solo mitiga el riesgo sino ayudan al control de la gestión.
- Deben ser resultado de un trabajo consensuado entre el líder del proceso, los funcionarios que ejecutan la actividad generadora de riesgo y pueden ser apoyados por la Oficina de Riesgo.
- 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 a su vez establecerse fechas de seguimiento al cumplimiento de los planes de acción, revisiones periódicas de la implementación de estos, así como su cumplimiento y ejecución.

Para calificar el nivel de desarrollo de los planes de seguimiento, se utilizarán los siguientes parámetros:

NIVEL DE DESARROLLO	Elaboración
DESCONOCIDO	No hay conciencia del peligro o se desconoce el riesgo o la necesidad de controles asociados.
NO DESARROLLADO	Acciones informales con procedimientos escasos o no sistemáticos.
CONOCIDO	Se tienen establecidos programas y procedimientos, pero no se puede confirmar que sean totalmente conocidos.
FORMALIZADO	Los programas y procedimientos se comunican a toda la organización. Entrenamiento en desarrollo.
IMPLANTADO	Implantados en la mayor parte o en todos los niveles organizativos. Se realizan entrenamientos y algunos ejercicios.
OPTIMIZADO	Totalmente implantado con adecuados programas de mantenimiento, pruebas, ejercicios y mejora continua.

Artículo 36. Registro e Informe: La gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados. El registro e informe pretenden:

- Comunicar las actividades de la gestión del riesgo y sus resultados a lo largo del Instituto.
- Proporcionar información para la toma de decisiones.
- Mejorar las actividades de la gestión del riesgo.
- Asistir la interacción con las partes interesadas, incluyendo a las personas que tienen responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

Artículo 37. Capacitaciones: El Instituto utilizará cualquier medio o instrumento contenido en sus procesos de capacitación para divulgar el Sistema Administrativo de Riesgo Operativo SARO.

TÍTULO VIII
LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO

Artículo 38. Plan de Contingencia: Establecer las directrices para el desarrollo de la continuidad del negocio del Idear, permitirá cumplir la misión y objetivos con nuestros clientes, la responsabilidad social con el entorno y el compromiso con la protección de los servicios públicos e infraestructura del negocio.

Artículo 39. Alcance: Con el fin de implementar la continuidad del negocio (PCN) acorde a su tamaño y el desarrollo de su operación, el Idear ha decidido desarrollar un PCN para todas las actividades que se identifican con los procesos misionales así:

- El plan de continuidad del negocio del Idear debe enfocarse al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a la materialización de eventos de riesgo operativos de infraestructura o desastre.

- Los líderes de procesos y procedimientos deben tener total claridad de las actividades a realizar en materia de PCN, previa capacitación del encargado de la implementación y administración de plan de 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 PCN sobre la comunicación en situaciones de crisis.

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

Artículo 40. 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.

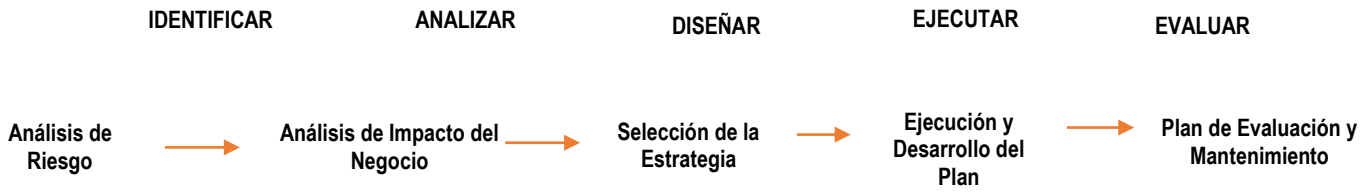
Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca tanto a las personas como a los procesos, la tecnología y la infraestructura, así como a situaciones externas que afecten el funcionamiento normal de las operaciones del Idear.

Previa a la implementación de un modelo de administración del PCN, se debe determinar lo siguiente:

- Establecer la necesidad de la continuidad del negocio.
- Comprometer a la Alta Gerencia en los procesos.
- Establecer el comité responsable.
- 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:

CICLO DE VIDA



Donde:

Análisis de Riesgo: Etapa previa a la implementación y debe estar acorde con los riesgos operativos identificados en el Idear.

Se debe cumplir en esta etapa como 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 crítica.
- Identificar oportunidades de mejora o exposiciones críticas a riesgos de fallas tecnológicas.
- Identificar las políticas y mejores prácticas de seguridad existentes.
- Revisión de instalaciones físicas, controles de cómputo e infraestructura tecnológica en general.

Análisis del Impacto del Negocio: Etapa en la cual se definen los procedimientos críticos del Idear, según el alcance mencionado en el presente documento para poder establecer su relevancia, tiempos y secuencia de recuperación.

Se debe cumplir con lo siguiente:

- Verificar el inventario de procesos y procedimientos.
- Identificación de impactos de interrupción de los procesos y procedimientos.
- Definir tiempo y secuencias de recuperación.
- Identificar 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 requisitos mínimos para cada recurso.
- Identificar configuraciones alternativas de recursos.
- Analizar las diferentes posibilidades en procesamiento y en comunicación.

- Determinar las opciones estratégicas de procesamiento internas, externas y acuerdos mutuos de servicio disponible.
- 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 los siguientes:

- 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 PCN del Idear al líder y a su vez a todos los funcionarios del Idear.

- Desarrollar las tareas necesarias para garantizar la operatividad del plan.
- Lograr una efectiva concientización sobre la importancia del plan.
- Socializar el plan de contingencia.
- Designar un responsable del plan para su actualización y mantenimiento.

TÍTULO IX
MONITOREO Y REVISIÓN

Artículo 41. Línea de defensa estratégica. Define el marco general para la gestión del riesgo y el control, supervisando su cumplimiento. La línea de defensa estratégica está compuesta por el Consejo Directivo y el Gerente del Instituto de Desarrollo de Arauca – IDEAR.

Artículo 42. Primera línea de defensa. Son las acciones para desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Estas acciones están a cargo de los líderes de procesos, subgerentes y equipos de trabajo, quienes son los encargados de diseñar, implementar y monitorear los controles, además deben gestionar de manera directa diariamente los riesgos de su competencia.

La primera línea de defensa debe identificar riesgos operativos y según la dependencia responsable, deben identificar riesgos financieros, riesgos de mercado, riesgos de liquidez, riesgos de crédito, riesgos de seguridad digital y riesgos de lavados de activos y financiamiento del terrorismo.

Todos los funcionarios que hacen parte de los diferentes procesos están en la obligación de reportar eventos de riesgo que se materialicen en el Instituto, incluyendo riesgos de corrupción, riesgos financieros, riesgos de mercado, riesgos de liquidez, riesgos de crédito, riesgos de seguridad digital y riesgos de lavados de activos y financiamiento del terrorismo, así como las causas que dieron origen a esos eventos de riesgos materializados conforme al formato de reporte de eventos dispuesto por la Oficina de Riesgos.

Artículo 43. Segunda Línea de Defensa. A cargo de la Oficina de Riesgos, Planeación, Subgerentes, Comités y Líderes responsables de sistemas de gestión, donde se ejecutan acciones para asegurar que los controles y los procesos de gestión de riesgo implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

El Jefe de la Oficina de Riesgos debe revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de estos, además de revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo del Instituto. Del mismo modo, hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos y de los diferentes sistemas de riesgos se encuentren documentadas y actualizadas en los procedimientos.

El Jefe de Oficina de Riesgos debe implementar y hacer seguimiento estricto a los reportes de eventos de riesgo en colaboración con los subgerentes y líderes de procesos, siendo esta una herramienta que permita conocer, documentar y mitigar posibles factores de riesgos potenciales y ocurridos.

Artículo 44. Tercera línea de defensa. A cargo de Control Interno o del Comité de Auditoría y Control Interno, quien proporciona información sobre la efectividad del Sistema de Control Interno, provee evaluación independiente y objetiva sobre la efectividad del Sistema de Gestión de Riesgos, validando que la línea estratégica, la primera línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de procesos, así como los riesgos de corrupción.

REVISÓ	APROBÓ
ORIGINAL FIRMADO PROFESIONAL UNIVERSITARIO PLANEACIÓN	ORIGINAL FIRMADO GERENTE

CONTROL DE CAMBIOS			
FECHA	**DESCRIPCIÓN DEL CAMBIO**	**VERSIÓN**	**MODIFICADO POR**
15 de diciembre de 2017	Adopción del Manual. Res 445/2017	01	
30 de junio de 2020	Actualización del Manual Acuerdo N° 19 de 2020	02	Consejo Directivo
27 de agosto de 2021	Actualización del Manual Artículos 30 y 31 Acuerdo No. 20 de 2021	03	Consejo Directivo