POLITICA GENERAL DE ADMINISTRACIÓN DEL RIESGO DEL INSTITUTO DE DESARROLLO DE ARAUCA – IDEAR

TÍTULO I
GENERALIDADES

Artículo 1. Objetivo General. La política de Administración del Riesgo del Instituto de Desarrollo de Arauca - IDEAR, tiene como propósito orientar las acciones necesarias que conduzcan a identificar los riesgos inherentes al desarrollo de su actividad, para posteriormente medirlos, controlarlos, gestionarlos y monitorearlos con el fin de mitigar las situaciones que puedan interferir en el cumplimiento de las funciones y en el logro de los objetivos institucionales.

Artículo 2. Objetivos específicos.

a) Actualizar e identificar los riesgos que se puedan presentar durante el desarrollo de las actividades propias de los procesos institucionales.

b) Dar la importancia y notar la incidencia que tiene la identificación los posibles factores de riesgo que se pueden materializar en cada proceso de la entidad.

c) Evaluar si las acciones implementadas para la mitigación de los eventos y/o factores de riesgos son adecuadas.

d) Establecer el sistema de controles y planes de contingencia para cada evento de riesgo.

e) Orientar la toma de decisiones oportunas y minimizar efectos adversos al interior de la entidad, con el fin de garantizar la continuidad a la gestión institucional y el logro de los objetivos estratégicos del Instituto.

f) Direccionar la cultura organizacional, en función del desarrollo de un pensamiento basado en riesgos.

g) Establecer condiciones institucionales para la gestión del riesgo.

Artículo 3. Alcance. La Política de Administración del Riesgo del Instituto de Desarrollo de Arauca –IDEAR, se aplicará en toda la organización, así como en todos los procesos establecidos en el mapa de procesos institucional y en cada uno de los cinco (5) Sistemas de Administración del Riesgos, así:

a) Sistema Administrativo de Riesgo Operativo SARO.
b) Sistema Administrativo de Riesgo de Liquidez SARL.
c) Sistema Administrativo de Riesgo de Mercado SARM.
d) Sistema Administrativo de Riesgo de Lavado de Activos y Financiación del Terrorismo SARLAFT.
e) Sistema Administrativo de Riesgo de Crédito SARC.

Artículo 4. Definiciones:

Administración del riesgo: Es la capacidad que tiene la entidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales, protegerla de los efectos ocasionados por su ocurrencia.

Amenaza: La fuente de daño potencial o una situación que potencialmente cause afectación en el desarrollo de la operación.

Análisis del riesgo: El uso sistemático de información disponible para determinar con qué frecuencia un determinado evento puede ocurrir y la magnitud de sus consecuencias.

Área de Impacto: Es todo recurso, bien u oportunidad al cual se le ha de asignar un valor y su afectación podría comprometer el cumplimiento de sus objetivos y metas.

Autocontrol: Es la capacidad que tiene cada servidor público, independientemente de su nivel jerárquico dentro de la entidad, para evaluar su trabajo, detectar desviaciones, efectuar correctivos, mejorar y solicitar ayuda cuando lo considere necesario, de tal manera que la ejecución de los procesos, actividades y tareas bajo su responsabilidad, garanticen el ejercicio de una función administrativa transparente y eficaz.

Consecuencia: Es el resultado o impacto de un evento (causa) expresado cualitativa o cuantitativamente, que genera pérdida, perjuicio, daño, desventaja o ganancia.

Nota 1. Puede haber más de una consecuencia de un evento.
Nota 2. Las consecuencias pueden variar desde positivas hasta negativas.
Nota 3. Las consecuencias se pueden expresar cualitativa o cuantitativamente.
Nota 4. Las consecuencias se consideran en relación con el logro de los objetivos.

Control: Proceso, política, dispositivo, practica u otra acción existente que actúa para minimizar el riesgo negativo o potenciar oportunidades positivas.

Nota: La palabra control también se puede aplicar a un proceso diseñado para suministrar aseguramiento razonable con relación al logro de los objetivos.

Costo: De una actividad, tanto el costo directo como el indirecto, involucran un impacto negativo, incluyendo dinero, trabajo, interrupción, pérdidas políticas e intangibles.

Compartir el riesgo: Compartir con otras de las partes el peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular.

Nota 1. Los requisitos legales o estatutarios pueden limitar, prohibir u ordenar compartir algunos riesgos.
Nota 2. El compartir el riesgo se puede realizar a través de seguros u otros acuerdos.
Nota 3. Compartir el riesgo puede crear riesgos nuevos o modificar un riesgo existente.

Criterios del riesgo: Términos de referencia mediante los cuales se evalúa la importancia del riesgo.

Nota: Los criterios del riesgo pueden incluir costos y beneficios asociados, requisitos legales y estatutarios, aspectos socioeconómicos y ambientales, preocupaciones de las partes interesadas, prioridades y otras entradas para la evaluación.

Evaluación del Control: Revisión sistemática de los procesos para garantizar que los controles aún son eficaces y adecuados.

Nota. La revisión periódica de la gestión en línea de los controles con frecuencia se denomina "autoevaluación del control".

Evaluación del riesgo: El proceso utilizado para determinar prioridades en la administración del riesgo por la comparación de niveles de riesgo frente a estándares determinados, límites de niveles del riesgo u otros criterios.

Nota 1. La evaluación del riesgo ayuda en las decisiones sobre el tratamiento del riesgo.

Evento: Ocurrencia de un conjunto particular de circunstancias.

Nota 1. El evento puede ser cierto o incierto.
Nota 2. El evento puede ser una sola ocurrencia o una serie de ocurrencias.

Evento de pérdida. Son aquellos incidentes que generan pérdidas por riesgo operativo a las entidades.

Clasificación de los eventos de riesgo operativo. Son los siguientes:

a) ***Fraude Interno***. Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la entidad o incumplir normas o leyes, en los que está implicado, al menos, un empleado o administrador de la entidad.

b) ***Fraude Externo***. Actos, realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos de esta o incumplir normas o leyes.

c) ***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.

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

e) ***Daños a activos físicos***. Pérdidas derivadas de daños o perjuicios a activos físicos de la entidad.

f) ***Fallas tecnológicas***. Pérdidas derivadas de incidentes por fallas tecnológicas.

g) ***Ejecución y administración de procesos***. Pérdidas derivadas de errores en la ejecución y administración de los procesos.

Exposición al riesgo: Nivel de vulnerabilidad que tiene el riesgo después de los controles.

Frecuencia: Medición del número de ocurrencias por unidad de tiempo Ej.: una vez cada día / una vez cada semana / una vez cada 15 días / una vez cada mes.

Fuente de Riesgo: Es toda persona, grupo humano, entidad, elemento físico o fenómeno del entorno, de los cuales se pueden derivar eventos que podrían afectar las áreas de impacto, cuya ocurrencia se debe evitar (minimizar) o maximizar para incrementar la posibilidad del logro de los objetivos y metas.

Identificación del riesgo: Proceso que determina que, cuando, donde, porque y como podría suceder algo.

Lineamientos estratégicos: Son aquellos que se establecen sin que se les asigne un periodo de validez determinado. Comprenden los fines, la misión y los valores.

Metas: Son los puntos de referencia o aspiraciones que la entidad debe lograr con el objeto de alcanzar en el futuro los objetivos formulados. Establecen qué es lo que se va a lograr y cuándo serán alcanzados los resultados, pero no indican cómo serán logrados.

Monitorear: Verificar, supervisar observar críticamente o medir regularmente el progreso de una actividad, una acción o un sistema para identificar los cambios en el nivel de desempeño requerido o esperado.

Organización: Grupo de personas e instalaciones con distribución de responsabilidades, autoridades y relaciones. Ejemplo: Incluye compañías, corporaciones, firmas, empresas, instituciones, caridad, comerciante único, asociación o partes o combinación de estas.

Nota 1. La distribución generalmente es ordenada.
Nota 2. Una organización puede ser pública o privada.

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.

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

Peligro: Una fuente de daño potencial.

Pérdida: Cualquier consecuencia negativa, o efecto adverso, financiera u otro.

Posibilidad: Se utiliza como descripción general de la probabilidad o la frecuencia.

Nota. Se puede expresar cualitativa o cuantitativamente.

Probabilidad: Es la posibilidad de un evento especifico o resultado, medido por la rata de eventos específicos o resultados sobre el número total de posibles eventos o resultados (Rango de 0-1/ %).

Proceso de Gestión del Riesgo: Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las labores de comunicar, establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y revisar el riesgo.

Partes involucradas: Personas y organizaciones que pueden afectar, verse afectadas o percibirse como afectadas por una decisión, una actividad o un riesgo.

Reducción del riesgo: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas, o ambas, asociadas con un riesgo.

Riesgo: Es toda posibilidad de ocurrencia de una situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.
Nota 1. Un riesgo a menudo se especifica en términos de un evento o circunstancia y las consecuencias que se pueden presentar por él.
Nota2. El riesgo se mide en términos de una combinación de consecuencias de un evento y su posibilidad.
Nota3. El riesgo puede tener un impacto positivo o negativo.

Riesgo Operativo (RO): 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 reputacional, asociados a tales factores.

Riesgo de Mercado. Se entiende por riesgo de mercado la posibilidad de que las entidades incurran en pérdidas asociadas a la disminución del valor de sus portafolios, las caídas del valor de las carteras colectivas o fondos que administran, por efecto de cambios en el precio de los instrumentos financieros en los cuales se mantienen posiciones.

Riesgo de Crédito. En sentido general, el riesgo crediticio es la posibilidad de que una entidad incurra en pérdidas y se disminuya el valor de sus activos, como consecuencia de que sus deudores fallen en el cumplimiento oportuno o cumplan imperfectamente los términos acordados en los contratos de crédito. Toda la cartera de créditos está expuesta a este riesgo, en mayor o menor medida.

Riesgo de Liquidez. Se entiende por riesgo de liquidez la 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 Lavado de Activos y Financiamiento del Terrorismo. Se entiende por riesgo LA/FT la 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.

El riesgo de LA/FT se materializa a través de los riesgos asociados, estos son; el legal, reputacional, operativo y de contagio, a los que se expone la entidad, con el consecuente efecto económico negativo que ello puede representar para su estabilidad financiera cuando es utilizada para tales actividades.

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 negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

Riesgo inherente. Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Perfil de Riesgo: Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.

Factores de riesgo: Se entiende por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operativo.

Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

Dichos factores se deben clasificar en internos o externos, según se indica a continuación.

Internos.

a) **Recurso Humano**. Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad.

b) **Procesos.** Es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.

c) **Tecnología.** Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: hardware, software y telecomunicaciones.

d) **Infraestructura.** Es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

Externo. Eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

Riesgo absoluto: Es la evaluación de la consecuencia y probabilidad que ignora los controles que están vigentes, excepto los controles inherentes, tales como el comportamiento racional, por parte de los funcionarios.

Riesgo residual: Se refiere al margen o residuo de riesgo que puede darse a pesar de las medidas de tratamiento tomadas para la administración del riesgo.

Sistema para la gestión del riesgo: Conjunto de elementos del Sistema de Gestión de una organización involucrados en la gestión del riesgo.

Nota 1. Los elementos del sistema de gestión pueden incluir planificación estratégica, toma de decisiones y otras estrategias, procesos y prácticas para abordar el riesgo.
Nota 2. La cultura de una organización se refleja en su sistema de gestión del riesgo.

Tratamiento del Riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Nota 1. El termino tratamiento del riesgo en ocasiones se utiliza para las medidas en sí.
Nota2. Las medidas para el tratamiento del riesgo pueden incluir evitar, modificar, compartir o retener el riesgo.

Valoración del riesgo: Proceso total de identificación del riesgo, análisis del riesgo y evaluación del riesgo

TÍTULO III
METODOLOGÍA MEDICIÓN DEL RIESGO

En la administración del riesgo operativo, las entidades deben desarrollar las siguientes etapas:

Artículo 5. Identificación. En desarrollo del SARO, Idear debe identificar los riesgos operativos a que se ve expuesta, teniendo en cuenta los factores de riesgo definidos de la Circular Externa 041 de 2007 de la Superintendencia Financiera de Colombia, son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

Para identificar el riesgo se debe como mínimo:

a) Identificar y documentar la totalidad de los procesos.

b) Establecer metodologías de identificación, que sean aplicables a los procesos, con el fin de determinar los riesgos operativos.

c) Identificar los **riesgos operativos**, potenciales y ocurridos, en cada uno de los procesos.

d) La etapa de identificación debe realizarse previamente a la implementación o modificación de cualquier proceso, así como en los casos de fusión, adquisición, cesión de activos, pasivos y contratos, entre otros.

Artículo 6. Políticas. La política que se adopte por parte de la entidad debe cumplir con los siguientes requisitos mínimos:

a) Impulsar a nivel institucional la cultura en materia de riesgo operativo riesgo de mercado, riesgo de liquidez, riesgo de crédito, riesgos de seguridad digital y riesgo LA/FT.

b) Establecer el deber de los órganos de administración, de control y de sus demás funcionarios, de asegurar el cumplimiento de las normas internas y externas relacionadas con la administración de los sistemas de riesgo.

c) Permitir la prevención y resolución de conflictos de interés en la recolección de información en las diferentes etapas de los sistemas de riesgo, especialmente para el registro de eventos de riesgo operativo.

d) Permitir la identificación de los cambios en los controles y en el perfil de riesgo.

e) Desarrollar e implementar planes de contingencia y continuidad del negocio.

f) El Instituto debe contar con un software de administración de riesgo que le permita desarrollar la estructura del SARO de acuerdo con las políticas, objetivos y metodologías de medición, que asiste a la entidad en la implementación de un sistema de cultura de Gestión del Riesgo efectivo en toda la organización, en aras de mejorar el desempeño del negocio y asegurar el logro de los objetivos y metas.

g) Se debe garantizar que el mapa de riesgos del Instituto sea de fácil acceso y de conocimiento de todos los funcionarios de la entidad.

h) El mapa de riesgos se debe actualizar cada vez que existan riesgos asociados a cambios de productos, servicios o programas, tecnología o nuevos proyectos, para presentarlos a la Gerencia, al Comité de Riesgos y al Consejo Directivo.

i) El monitoreo del mapa de riesgos es esencial para asegurar que las acciones se están llevando a cabo, y evaluar la eficiencia de su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores, que puedan estar influyendo en las acciones preventivas. El monitoreo está a cargo de los responsables de procesos, Jefe de Oficina de Riesgos y Control Interno.

j) Los líderes de procesos deben identificar riesgos asociados al proceso que lideran teniendo presente los sistemas administrativos de riesgo operativo, de mercado, de crédito, de liquidez y lavado de activos/financiamiento del terrorismo.

Artículo 7. Medición y seguimiento. Una vez concluida la etapa de identificación, la entidad debe medir la probabilidad de ocurrencia de los riesgos operativos y su impacto en caso de materializarse. Esta medición podrá ser cualitativa y, cuando se cuente con datos históricos, cuantitativa. Para la determinación de la probabilidad se debe considerar un horizonte de tiempo de un año. Además, el Instituto de Desarrollo de Arauca – IDEAR cuenta con el Manual del Sistema Administrativo del Riesgo Operativo, el cual describe la estructura para la medición, monitoreo y control de los riesgos operativos del Instituto.

TÍTULO IV
ESTABLECIMIENTO DEL CONTEXTO

Artículo 8. Establecimiento del Contexto. Definición de los parámetros interno y externos que se han de tomar en consideración para la administración del riesgo. Se debe establecer el contexto interno, externo de la entidad y el contexto del proceso y sus activos de seguridad digital. Es posible hacer uso de herramientas y técnicas.

Artículo 9. Establecimiento del Contexto del Proceso. Se determinan las características o aspectos esenciales del proceso y sus irregularidades. Se pueden considerar factores como:

CONTEXTO DEL PROCESO	**DISEÑO DEL PROCESO:** Claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIÓN CON OTROS PROCESOS: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: Grado de autoridad y responsabilidad de los

	funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: Efectividad en los flujos de información determinados en interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: Información, aplicación hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Artículo 10. Establecimiento del Contexto Externo. Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como:

CONTEXTO EXTERNO	**Circunstancias Económicas del Mercado:** Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	Circunstancias Políticas: Cambios de gobierno, legislación, políticas públicas, regulación, normatividad externa.
	Eventos Naturales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	Eventos Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	Comportamiento Humano: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.

Artículo 11. Establecimiento del Contexto Interno. Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos. Se pueden considerar factores como:

CONTEXTO INTERNO	**Comportamiento Humano:** Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	Asuntos Tecnológicos: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	Actividades de gestión y control: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo y seguimiento al cumplimiento del objeto misional.
	Desconocimiento del Proceso: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	Actividades Individuales: Competencia del personal, desconocimiento de los procesos y no capacitación.
	Error de Ingreso de Información: Integridad de datos, disponibilidad de datos y sistema, desarrollo producción, mantenimiento de sistema de información**.**
	Relaciones Legales y Comerciales: Relaciones legales y comerciales al interior de la organización y con otras organizaciones, por ejemplo, proveedores, subcontratistas arrendatarios.

TÍTULO V
MAPA DE RIESGO

Artículo 12. Mapa de Riesgo: En la administración del riesgo operativo, la entidad cuenta con un mapa de riesgo, en el que cada una de las áreas, registra los posibles eventos que, en caso de presentarse, afecten de

forma negativa, los procesos de la entidad. Es un elemento de autocontrol, medición y monitoreo que busca que la respuesta a la ocurrencia de un evento sea de manera inmediata y articulada.

El mapa de riesgo se constituye como una herramienta de gestión que permite determinar objetivamente cuáles son los riesgos que pueden afectar el funcionamiento del Instituto en el ejercicio de sus funciones. Bajo los lineamientos de construcción del mapa de riesgos se realiza un seguimiento permanente de los riesgos aplicando las medidas necesarias para la mitigación de estos.

El Mapa de Riesgo, 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 y se define conforme a la probabilidad e impacto de la ocurrencia.

- 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, conforme a la mitigación de la probabilidad de ocurrencia.

- Opción de Manejo**:** Son las alternativas con las que cuenta la entidad, frente al Riesgo Residual, correspondiente a las acciones de: Reducir, Mitigar, Compartir o Aceptar.

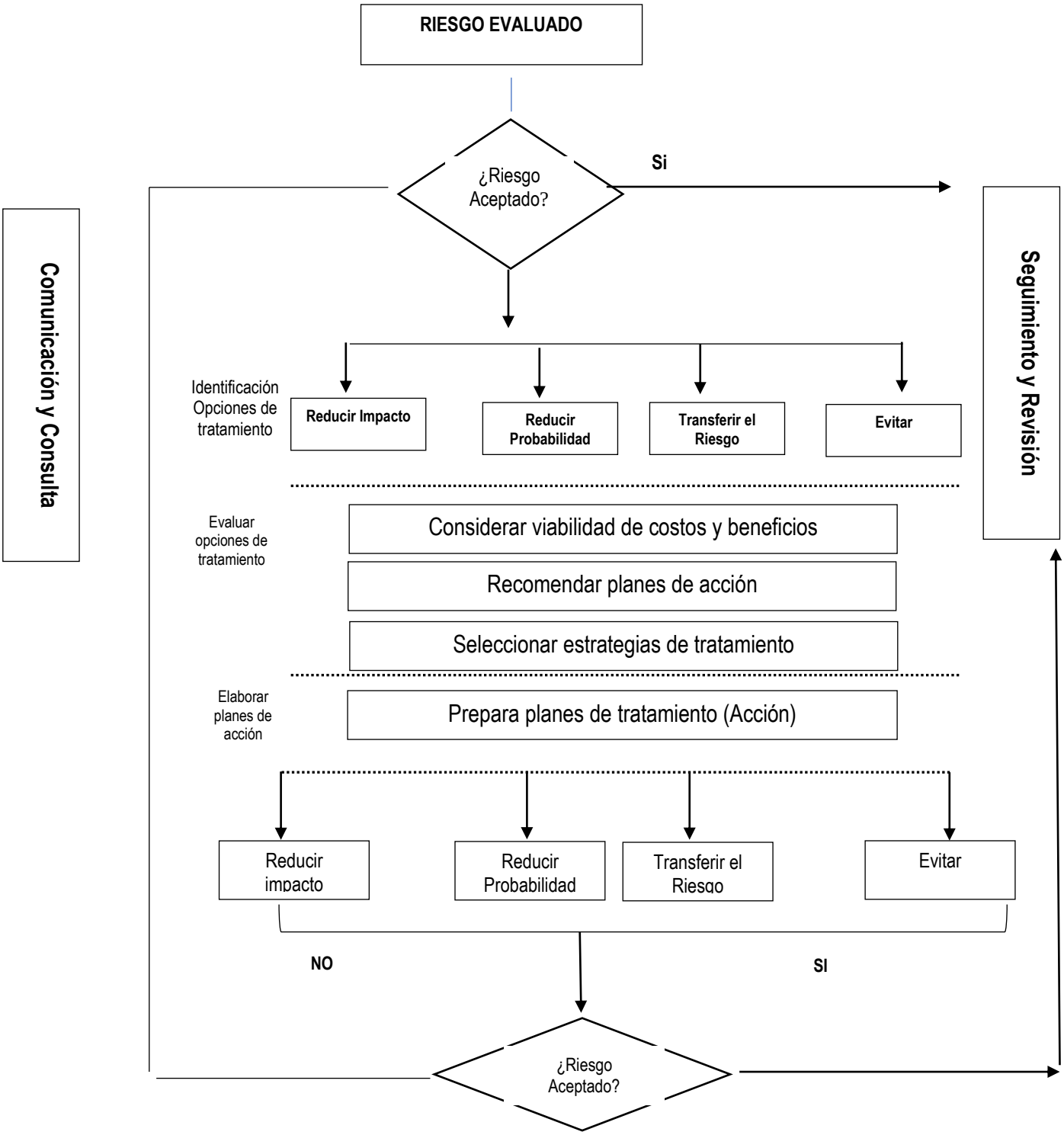
- Acciones Preventivas**:** Se consagran todas las acciones con las que dispone la entidad para mitigar la materialización de un riesgo.

- 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.

TÍTULO VI
METODOLOGÍA DEL RIESGO

Artículo 13. Metodología: Con el ánimo de aplicar de manera razonable, un sistema de administración del riesgo, se plantea la siguiente metodología:


RIESGO EVALUADO
¿Riesgo Aceptado?
Si
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?

TÍTULO VII
VALORACIÓN DEL RIESGO

Artículo 14. Valoración del riesgo. Es el mecanismo para establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

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 expondrá 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 buscan 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.

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 Manual de Riesgo Operativo de la entidad:

Lo anterior, debe ser registrado en el Mapa de Riesgos del Idear.

	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) días.	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 mestas 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 15. Mapa de calor. Matriz de criticidad de 5x5 significa que para ubicar el nivel de riesgo se cuenta con 5 niveles en probabilidad y 5 niveles en impacto. Para evaluar los riesgos, se recomienda elaborar un mapa de calor, donde se clasifique el impacto y la probabilidad. Cada uno se identifica con un color diferente: Riesgo Extremo (Rojo) – Riesgo Alto (Naranja) - Riesgo Moderado (Amarillo) - Riesgo Bajo (Verde).
El Instituto de Desarrollo de Arauca Idear, adopta el siguiente mapa de calor:

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 severidad, en los niveles siguientes:

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 contingencia para el tratamiento de este, en coordinación con el responsable del proceso y de la valoración de las actividades pertinentes.

Artículo 16. Valoración de 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
	Conciliaciones
	Consecutivos
	Verificación de firmas

CONTROLES OPERATIVOS	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 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: Hacer 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 17. 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 el 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 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, mínimo una vez al año liderada por la Oficina de Riesgos en acompañamiento del líder de cada proceso, socializando el resultado de esta en el marco del Comité de Riesgos.

La evaluación tendrá en cuenta los siguientes parámetros:

		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 18. 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.

			EVALUACIÓN DEL RIESGO														CÓDIGO: XX VERSIÓN: XXX FECHA: XX PÁGINA: XXX		
Identificación del Riesgo			**Valoración del Riesgo**														**Monitoreo y Revisión**		
Procesos/ Subproceso	**Sistema Asociado**	**Nombre del Riesgo**	**Tipología del Riesgo**	**Causa**	**Consecuencia**	**Análisis del Riesgo**			**Valoración del Riesgo**								**Periodo de Seguimiento**	**Acción de Contingencia ante Posible Materialización**	
						Riesgo Inherente													
						Probabilidad	**Impacto**	**Zona de Riesgo**	**Control Existente**	**Riesgo Residual**			**Acciones Asociadas al Control**						
										Probabilidad	**Impacto**	**Zona de Riesgo**	**Opción de Manejo**	**Acciones Preventivas**	**Responsable**				
Observación																			

Es así, como se recomienda la evaluación del riesgo a cargo del líder del proceso, y desde Control Interno en el marco de las auditorías de control interno se realizará una verificación de estas, socializando el resultado de esta en el marco del Comité de Auditoría y Control Interno. La Oficina de Riesgos hará el monitoreo del mapa de riesgos en los plazos establecidos y socializará en el Comité de Riesgos.

El producto de la evaluación de los riesgos, incluido los riesgos de corrupción se evaluarán mínimo una vez en la vigencia y en el marco del Comité de Riesgos.

Artículo 19. 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	A **R1**	E
RARO (1)	B	B	M	A	A

En nuestro ejemplo disminuiría dos cuadrantes de probabilidad, pasa de probable a improbable manteniendo el nivel de impacto.

Artículo 20. 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 contingencia que mitigan el riesgo, estos planes de acción deben quedar identificados y enlistados en el Mapa de Riesgos.

Cada uno de estos, debe contener 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:

a) **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.

b) **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.

c) **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.

d) **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

TÍTULO VIII
MONITOREO Y REVISIÓN

Artículo 21. 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, el Gerente y el Comité de Auditoría y Control Interno del Instituto de Desarrollo de Arauca – IDEAR.

Artículo 22. 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 lavado 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 lavado de activos y financiamiento del terrorismo, así como las causas que dieron origen a esos eventos de riesgo materializados conforme al formato de reporte de eventos dispuesto por la Oficina de Riesgos.

Artículo 23. 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 24. 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 componente 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.

Artículo 25. Elaboración del mapa de riesgo. La elaboración y actualización del mapa de riesgos será liderado por el jefe de Oficina de Riesgos del Instituto, quien impartirá la metodología correspondiente para que la primera línea de defensa elabore y documente los riesgos de sus procesos y sistemas de riesgo a cargo. El responsable del proceso de Planeación coadyuvará en la consolidación del Mapa de Riesgos.

Artículo 26. Seguimiento. La primera línea de defensa reporta a la segunda línea de defensa. El estado de avance del tratamiento del riesgo en la operación, y la consolidación de los riesgos en todos los niveles será reportado por el jefe de Riesgos a la línea estratégica del Instituto.

El seguimiento general del mapa de riesgos se realizará trimestralmente por el jefe de Oficina de Riesgos, quien realiza monitoreo permanente del riesgo individual y consolidado del Instituto, el cual informa en el Comité de Riesgos.

La primera línea de defensa se rige por el “autocontrol” como la capacidad de cada servidor público para controlar su trabajo, detectar desviaciones y efectuar correctivos; monitoreando los riesgos de sus procesos y reportando mensualmente sus resultados a la Oficina de Riesgos del Instituto, la segunda línea de defensa atiende lo concerniente a la autoevaluación y la tercera línea de defensa la evaluación independiente.

Control Interno realiza seguimiento del mapa de riesgo desde el punto de vista del cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos.

REVISÓ	APROBÒ
ORIGINAL FIRMADO PROFESIONAL UNIVERSITARIO PLANEACIÓN	ORIGINAL FIRMADO GERENTE

CONTROL DE CAMBIOS			
FECHA	**DESCRIPCIÓN DEL CAMBIO**	**VERSIÓN**	**APROBADO POR**
17 de octubre de 2019	Acuerdo 16/2019	01	Consejo Directivo
30 de junio de 2020	Acuerdo No. 20 de 2020	02	Consejo Directivo
27 agosto de 2021	Actualización del Manual Artículos 8, 9, 10, 11 y 17 Acuerdo No. 20	03	Consejo Directivo