MANUAL DE ADMINISTRACIÓN DE RIESGOS DEL FONDO NACIONAL DE TURISMO FONTUR

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

TABLA DE CONTENIDO

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

1 CAPÍTULO I – GENERALIDADES

1.1 Introducción

En el marco del Contrato de Fiducia Mercantil CTO-413-2023 suscrito entre el Ministerio de Comercio, Industria y Turismo y la Fiduciaria Colombiana de Comercio Exterior, con el objeto de administrar los recursos del Fondo Nacional de Turismo - FONTUR, señalados en los artículos 1° y 8° de la Ley 1101 de 2006, el impuesto al turismo, los asignados en el Presupuesto General de la Nación y los demás que le sean asignados para el desarrollo de la infraestructura, promoción y la competitividad turística; y el recaudo y la administración de la Contribución Parafiscal, se establecieron en la sección IV. Obligaciones de la Fiduciaria las siguientes:

"Circular Básica Contable y Financiera (Circular Externa 100 de 1995) (…) a. Administrar los recursos del P.A. FONTUR dando cumplimiento a los principios de eficiencia, transparencia, economía y responsabilidad. f. Cumplir todas las normas establecidas para la administración de riesgos, reguladas en el Estatuto Orgánico del Sistema Financiero y en la Parte I, Título IV, Capítulo IV de la Circular Básica Jurídica, expedidas por la Superintendencia Financiera de Colombia. l. Aplicar las metodologías y los procedimientos estándar para la identificación, prevención, mitigación y gestión de los riesgos a los que están expuestos los recursos administrados y velar por su adecuado tratamiento y mitigación. (…)"

De la misma manera, en la sección VI. Numeral 10. Gestión de Riesgos, se estableció que los servicios ofrecidos por la Fiduciaria se ven expuestos a los riesgos operacionales, de liquidez y de mercado y que los mecanismos para controlar, medir y gestionar los riesgos del negocio anteriormente referidos están soportados en los parámetros, políticas y métodos de medición de los sistemas de riesgos operativos, de liquidez y de mercado con que cuenta la Fiduciaria, conforme lo establecido para cada Sistema de Riesgos en la mencionada Circular Externa No. 100 de 1995.

En virtud de lo anterior, en el presente Manual se describirán las políticas, lineamientos, metodologías y demás criterios que aplicará la Fiduciaria en materia de gestión de riesgos, seguridad de la información y continuidad del negocio, en cumplimiento de las obligaciones contractuales y normativas.

1.2 Objetivo del Manual

El propósito del presente Manual es establecer las políticas, lineamientos, procedimientos, metodologías, indicadores y controles que permitan gestionar y mitigar los riesgos a los que se pueda ver expuesto el P.A. FONTUR, la Fiduciaria y el Fideicomitente, en desarrollo del objeto del contrato CTO-413-2023, considerando en su alcance los Riesgos Operacionales y de Lavado de Activos y Financiación del Terrorismo.

Así mismo, definir las gestiones, actividades y responsabilidades en las etapas del ciclo de gestión de riesgos (Identificación, Medición, Control y Monitoreo) de cada una de las

instancias de la estructura organizacional del P.A. FONTUR, con el fin de promover que los sistemas de administración de riesgos y la gestión de la Seguridad de la Información y la Continuidad del Negocio sea efectiva, eficiente y oportuna, soportada en los principios de autocontrol, autogestión y en una cultura de prevención y monitoreo permanente.

A continuación, se plantean los objetivos específicos:

1.2.1 Gestión del Riesgo Operacional

Tiene por propósito identificar, medir, controlar y monitorear los riesgos operacionales asociados a los procesos definidos en la estructura del P.A. FONTUR con el fin de identificar situaciones que puedan afectar el cumplimiento de los objetivos del Patrimonio, definir y/o fortalecer los controles, asegurar la operación para que se desarrolle de manera eficiente y oportuna, se minimice la exposición al riesgo y se dé cumplimiento a los requerimientos normativos estipulados por la Superintendencia Financiera de Colombia en el capítulo XXXI de la Circular Básica, Contable y Financiera.

1.2.2 Gestión de los Riesgos de Lavado de Activos y Financiación del Terrorismo

Tiene por objetivo desarrollar las etapas y establecer mecanismos y controles que permitan prevenir la pérdida o daño reputacional o legal que pueda sufrir el P.A. FONTUR por la propensión a ser utilizado como mecanismo o instrumento para el lavado de activos o para la canalización de recursos hacia la financiación del terrorismo, de acuerdo con su naturaleza y objeto. Así mismo, asegurar el cumplimiento de las disposiciones de la Superintendencia Financiera de Colombia estipuladas en la Parte I, Título IV, Capítulo IV de la Circular Básica Jurídica y de las definidas por la Junta Directiva de la Sociedad Fiduciaria, con relación al Sistema de Administración de Riesgos de Lavado de Activos y la Financiación del Terrorismo (SARLAFT).

1.2.3 Gestión de Seguridad y Ciberseguridad de la Información

Tiene por objetivo establecer los lineamientos, metodologías, actividades y responsabilidades, así como las soluciones y controles que permitan proteger los activos de información del P.A. FONTUR, asegurando la integridad, disponibilidad y confidencialidad de la información que se almacene, reproduzca o procese en los sistemas de información del Patrimonio.

Así mismo, la gestión de Ciberseguridad está orientada a establecer las políticas, mecanismos y acciones para fortalecer la capacidad de defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones del P.A. FONTUR en el ciberespacio que son esenciales para su operación.

1.2.4 Gestión de Continuidad de Negocio

Identificar los procesos críticos del P.A. FONTUR, de tal forma que se genere una estrategia de recuperación y planes de acción que permitan garantizar el restablecimiento de estos, teniendo en cuenta los tiempos aceptables del P.A. FONTUR

a fin de mitigar los impactos económicos, legales, reputacionales y operacionales que se podrían generar ante la ocurrencia de una contingencia.

1.2.5 Protección de Datos

Dar los lineamientos que permitan proteger, garantizar la privacidad y seguridad de la información de los datos del P.A. FONTUR, garantizando los tres pilares de seguridad: disponibilidad, integridad y confidencialidad de la información.

1.3 Alcance del Manual

La Gestión de Riesgos del P.A. FONTUR, comprende los Riesgos Financieros (mercado, liquidez, emisor y contraparte) y Operacional y de Lavado de Activos y Financiación del Terrorismo (LAFT). No obstante, en el presente Manual se establecen las políticas, estructura organizacional, lineamientos, metodologías, procedimientos, límites, alertas y controles para gestionar los riesgos operacionales y LAFT. Así mismo, se incorporan las directrices y lineamientos específicos para la gestión de la seguridad de la información, la ciberseguridad, la continuidad del Negocio y la protección de datos personales. Es importante anotar que las directrices para la gestión de los riesgos financieros están incorporadas en el Manual de Inversiones con el fin de asegurar su efectividad.

De la misma manera, el Manual de Riesgos contiene los lineamientos generales para que en desarrollo de la etapa precontractual de bienes y servicios se identifiquen y evalúen los riesgos que podrían presentarse en la ejecución contractual y se definan e implementen acciones y controles a cargo de los supervisores y/o interventores, así como para la implementación del respectivo esquema de monitoreo. Las directrices específicas para estos riesgos harán parte del Manual de Contratación y/o Supervisión e interventoría.

1.4 Referencias Normativas

- Ley 1226 de 2008, *"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"*
- Ley 1474 de 2011, *"Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública"*
- Ley 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales"
- Ley 1712 de 2014, *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*
- Decreto 663 de 1993, *"Por medio del cual se actualiza el Estatuto Orgánico del Sistema Financiero y se modifica su titulación y numeración"*
- Decreto 2555 de 2010, *"Por el cual se recogen y reexpiden las normas en materia del sector financiero, asegurador y del mercado de valores y se dictan otras disposiciones."*

- Decreto 830 de 2021, *"Por el cual se modifican y adicionan algunos artículos al Decreto 1081 de 2015, Único Reglamentario del Sector Presidencia de la República, en lo relacionado con el régimen de las Personas Expuestas Políticamente (PEP)".*
- Circular Externa Superfinanciera 100 de 1995, *"Circular Básica Contable y Financiera"*, Capítulo XXXI Sistema Integral de Administración de Riesgos (SIAR) de la Superintendencia Financiera de Colombia.
- Circular Externa Superfinanciera 029 de 2014, *"Circular Básica Jurídica"*, Parte I del Título IV, Capitulo IV, Instrucciones Relativas a la Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo de la Superintendencia Financiera de Colombia y Parte I del Título IV, Capitulo V, Requerimientos Mínimos para la Gestión de la Seguridad de la Información y la Ciberseguridad de la Superintendencia Financiera de Colombia.
- Circular Externa Superfinanciera 018 de 2021, *"Sistema Integral de Administración de Riesgos (SIAR) y Sistema de Administración de Riesgos de las Entidades Exceptuadas del SIAR (SARE)"*
- Documento CONPES 3793 de diciembre 18 de 2013, *"Política Nacional Anti Lavado de Activos y Contra la Financiación del Terrorismo"*
- Estándar ISO/IEC 22301, Sistemas de Gestión de la Continuidad de Negocio.
- Estándar ISO/IEC 27001, Sistemas de Gestión de Seguridad de la Información.
- Contrato de Fiducia No.413-2023 suscrito entre el Ministerio de Comercio Industria y Turismo y Fiducoldex S.A.
- Manuales descritos en la Sección "X.1 Adopción y Modificación de Manuales" del contrato de fiducia No.413-2023 suscrito entre el Ministerio de Comercio Industria y Turismo y FIDUCOLDEX S.A.

1.5 Términos y Definiciones

- **Administración de Riesgo:** Proceso continuo de identificación, medición, control y monitoreo de los riesgos, con el fin de reducir las pérdidas derivadas de los riesgos operacionales.

- **Amenazas cibernéticas:** Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

- **Análisis de Riesgo:** Método por el cual se estudian las causas que generan posibles amenazas, su frecuencia y en caso de su materialización la magnitud de sus consecuencias.

- **Apetito de Riesgo:** El o los niveles y tipos de riesgos que el Patrimonio Autónomo está dispuesta a asumir con el fin de cumplir con su plan de negocio.

- **Autoevaluación de Riesgos y Controles:** RCSA (Risk and Control Self-Assessment) o proceso a través del cual las diversas áreas de negocio identifican y evalúan el nivel de control que se tiene en sus procesos.
- **Beneficiario final:** Son las personas naturales a las que se refiere el art. 631-5 del Estatuto Tributario, o cualquier norma que lo modifique o sustituya. Entiéndase por beneficiario final la(s) persona(s) natural(es) que finalmente posee(n) o controla(n), directa o indirectamente, a un cliente y/o la persona natural en cuyo nombre se realiza una transacción. Incluye también a la(s) persona(s) natural(es) que ejerzan el control

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

efectivo y/o final, directa o indirectamente, sobre una persona jurídica u otra estructura sin personería jurídica.

A) Son beneficiarios finales de la persona jurídica las siguientes:

1. Persona natural que, actuando individual o conjuntamente, sea titular, directa o indirectamente, del cinco por ciento (5%) o más del capital o los derechos de voto de la persona jurídica, y/o se beneficie en cinco por ciento (5%) o más de los activos, rendimientos o utilidades de la persona jurídica; y
2. Persona natural que, actuando individual o conjuntamente, ejerza control sobre la persona jurídica, por cualquier otro medio diferente a los establecidos en el numeral anterior del presente artículo; o
3. Cuando no se identifique ninguna persona natural en los términos de los dos numerales anteriores del presente artículo, se debe identificar la persona natural que ostente el cargo de representante legal, salvo que exista una persona natural que ostente una mayor autoridad en relación con las funciones de gestión o dirección de la persona jurídica.

B) Son beneficiarios finales de una estructura sin personería jurídica o de una estructura similar, las siguientes personas naturales que ostenten la calidad de:

1. Fiduciante(s), fideicomitente(s), constituyente(s) o posición similar o equivalente;
2. Fiduciario(s) o posición similar o equivalente;
3. Comité fiduciario, comité financiero o posición similar o equivalente;
4. Fideicomisario(s), beneficiario(s) o beneficiario(s) condicionado(s); y
5. Cualquier otra persona natural que ejerza el control efectivo y/o final, o que tenga derecho a gozar y/o disponer de los activos, beneficios, resultados o utilidades.

En caso de que una persona jurídica ostente alguna de las calidades establecidas previamente para las estructuras sin personería jurídica o estructuras similares, será beneficiario final la persona natural que sea beneficiario final de dicha persona jurídica conforme al artículo 631 - 5 de la Resolución 164 de 2021 emitida por la DIAN.

- **Capacidad de Riesgo de Liquidez:** Nivel máximo de riesgo que el Patrimonio Autónomo puede asumir dado su nivel actual de recursos antes de sobrepasar las necesidades mínimas de liquidez.

- **Capacidad de Riesgo:** Nivel máximo de riesgo que el Patrimonio Autónomo puede asumir dado su nivel actual de recursos antes de incumplir los controles de ley, los límites de liquidez, y/o comprometer la continuidad del negocio.

- **Ciberataque o ataque cibernético:** Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de esta o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

- **Comité de Administración de Riesgos (CAR):** Órgano técnico en el cual la Junta Directiva se apoya para realizar el seguimiento del sistema integral de administración de riesgos de la Sociedad.

- **Conducta Irregular:** Hace referencia a incumplimientos de leyes, regulaciones, políticas internas, reglamentos o expectativas del P.A. FONTUR respecto a la conducta ética empresarial y comportamientos no habituales.

- **Clasificación de los Riesgos Operacionales:** Disposición por clase de evento de riesgo operacional:

    - **Fraude Interno:** Actos que tienen como resultado defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales vigentes en los que se encuentra implicado, al menos, un empleado o tercero contratado para ejecutar procesos a nombre del Patrimonio Autónomo.
    - **Fraude Externo:** Actos realizados por una persona externa al Patrimonio Autónomo, que buscan defraudar o apropiarse indebidamente de activos de esta o incumplir normas o leyes.
    - **Clientes, productos o prácticas empresariales:** Incumplimiento involuntario o negligente de una obligación profesional/empresarial frente a clientes o eventos derivados de la naturaleza o diseño de un producto.
    - **Daños a Activos Físicos:** Pérdidas derivadas de daños o perjuicios a activos físicos del Patrimonio Autónomo como consecuencia de desastres naturales, actos de terrorismo, vandalismo u otros acontecimientos.
    - **Ejecución y Administración de Procesos:** Errores en el procesamiento de operaciones o en la gestión de procesos, así como en las relaciones con contrapartes comerciales y proveedores.
    - **Relaciones Laborales:** Actos que son incompatibles con la legislación laboral o con acuerdos relacionados con la higiene o la seguridad en el trabajo, o que versen sobre el pago de reclamaciones por daños personales o casos relacionados con la diversidad y/o discriminación en el ámbito laboral.
    - **Fallas Tecnológicas:** Hechos o cambios originados por fallas del hardware, software, telecomunicaciones o servicios públicos que puedan afectar, además de la operación interna del Patrimonio Autónomo, la prestación del servicio a los clientes.
    - **Eventos Externos:** Corresponde a la ocurrencia de eventos externos asociados u ocasionados por factores exógenos, que escapan en cuanto a su causa y origen al control del Patrimonio Autónomo como movimientos fuertes del mercado, políticas monetarias, coyuntura económica y demás variables que de una u otra manera pueden comprometer la capacidad de respuesta del Patrimonio Autónomo, afectando la operación y/o el cumplimiento de los objetivos misionales.

- **Cliente:** Es toda persona natural o jurídica con la cual el Patrimonio Autónomo establece y mantiene una relación contractual o legal para el suministro de cualquier producto propio de su actividad. Para este manual el término cliente es sinónimo de Fideicomitente y de Beneficiario del Contrato de Fiducia.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

- **Conocimiento del Cliente:** Proceso mediante el cual la Fiduciaria analiza un cliente frente al Sistema de Prevención de Lavado de Activos y Financiación Terrorismo.

- **Control:** Mecanismo de aseguramiento implementado para mitigar o minimizar los riesgos; de los cuales se puede identificar como control la implementación de políticas, prácticas, procedimientos y otros mecanismos.

- **Corrupción**: Obtención de un beneficio particular por acción u omisión, uso indebido de una posición o poder, o de los recursos o de la información.

- **Determinación del Nivel de Riesgo:** Resultado de confrontar el riesgo inherente con la evaluación de las actividades de control que se realizan al interior de los diferentes procesos, procedimientos, actividades y el resultado será el riesgo residual.

- **Evento de Riesgo Operacional:** Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado que materializa un riesgo que puede o no generar pérdida económica.

- **Factores de Riesgo:** Fuentes generadoras de riesgos operacionales que pueden o no generar pérdidas. Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

    - **Procesos:** Conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.
    - **Tecnología:** Conjunto de herramientas empleadas para soportar los procesos del Patrimonio Autónomo. Incluye: hardware, software y telecomunicaciones.
    - **Recurso Humano:** Conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos del Patrimonio Autónomo. Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente. La vinculación indirecta hace referencia a aquellas personas que tienen con el Patrimonio Autónomo una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo.
    - **Infraestructura:** Conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.
    - **Externos:** Situaciones asociadas a la fuerza de la naturaleza u ocasionadas por terceros, que escapan en cuanto a su causa y origen al control del Patrimonio Autónomo.

- **Financiación del Terrorismo:** Por su parte, el artículo *16 de la Ley 1121 de 2006* modificó el artículo *345 de la Ley 599 de 2000*, quedando así:

> *"Financiación del terrorismo y administración de recursos relacionados con actividades terroristas. El que directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye,*

mantenga, financie o sostenga económicamente a grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas, incurrirá en prisión de trece (13) a veintidós (22) años y multa de mil trescientos (1.300) a quince mil (15.000) salarios mínimos legales mensuales vigentes".

- **Frecuencia:** Número de veces que se ejecuta la actividad en donde se encuentra el punto de riesgo, dentro de un proceso.

- **Gestor de Riesgo:** Para efectos de la gestión de riesgos operacionales por procesos, es quien ha sido designado por el dueño del proceso para apoyar las actividades de identificación y valoración de los riesgos y controles, según el conocimiento del proceso y experiencia técnica, además posee información relevante para su posterior medición y análisis, y contribuye en la definición de planes de acción para los riesgos materializados en el proceso que representa.

- **Identificación de Riesgos:** Etapa en donde se determina qué puede suceder, cómo y porqué y cuáles son los posibles impactos de su materialización.

  En esta etapa se determinan los riesgos (actuales y potenciales) inherentes a las actividades que desarrolla o planea desarrollar del Patrimonio Autónomo. Esta etapa debe realizarse previamente en el caso de la implementación de nuevas actividades o modificación sobre las que están en operación y/o cambios en el plan de negocio.

- **Impacto:** Consecuencia que puede generarse en caso de materialización del riesgo; puede expresarse de forma cualitativa o cuantitativa.

- **Jurisdicciones:** Corresponde a las regiones donde se encuentran domiciliados los clientes.

- **Lavado de Activos:** Está tipificado como delito contra el orden económico social, en el Capítulo Quinto del Título X del Código Penal, artículo *323*, así:

  "El que adquiera, resguarde, invierta, transporte, transforme, custodie o administre bienes que tengan su origen mediato o inmediato en actividades de tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias sicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito, incurrirá por esa sola conducta, en prisión de ocho (8) a veintidós (22) años y multa de seiscientos cincuenta (650) a cincuenta mil (50.000) salarios mínimos legales vigentes.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

La misma pena se aplicará cuando las conductas descritas en el inciso anterior se realicen sobre bienes cuya extinción de dominio haya sido declarada.

El lavado de activos será punible aun cuando las actividades de que provinieren los bienes, o los actos penados en los apartados anteriores, se hubiesen realizado, total o parcialmente, en el extranjero.

Las penas privativas de la libertad previstas en el presente artículo se aumentarán de una tercera parte a la mitad cuando para la realización de las conductas se efectuaren operaciones de cambio o de comercio exterior, o se introdujeren mercancías al territorio nacional.

El aumento de pena previsto en el inciso anterior, también se aplicará cuando se introdujeren mercancías de contrabando al territorio nacional".

- **Marco de Apetito de Riesgo (MAR):** Conjunto de políticas, metodologías, procedimientos, controles y umbrales y/o límites a partir del cual el Patrimonio Autónomo: (I) identifica los riesgos asociados al plan de negocio, (II) evalúa si dichos riesgos se asumen, mitigan, evitan o transfieren, y (III) monitorea y controla que dichos riesgos se encuentren dentro de los umbrales y/o límites definidos por la Alta Gerencia (AG) y aprobados por la Junta Directiva (JD).

- **Medición:** En esta etapa se cuantifica y/o evalúa la exposición a los riesgos inherentes a las actividades que desarrolla o planea desarrollar del Patrimonio Autónomo y su impacto en caso de materializarse. Esta medición podrá realizarse mediante metodologías cualitativas y/o cuantitativos, previamente aprobadas.

- **Monitoreo:** Observar el curso de uno o varios parámetros para detectar posibles anomalías, con el fin de identificar los cambios de una actividad, proceso, acción o sistema.

- **Oficial de Cumplimiento:** Empleado responsable de verificar y orientar la adecuada observancia de los procedimientos y normas legales sobre SARLAFT de acuerdo con lo establecido en las regulaciones emitidas por la Superintendencia Financiera de Colombia.

- **Obligaciones Contractuales**: Obligaciones contractuales se entenderán como la responsabilidad del Patrimonio Autónomo en realizar las erogaciones de recursos, definida en los contratos de negocios fiduciarios y/o en los contratos de administración del portafolio.

- **Operación Inusual:** Es aquella transacción que cumple, cuando menos con las siguientes características: 1) no guardar relación con la actividad económica o se sale de los parámetros adicionales fijados por la Fiduciaria y, 2) respecto de las cuales la Fiduciaria no ha encontrado explicación o justificación que se considere razonable.

- **Operación Sospechosa:** De conformidad con el numeral 2. literal d. del *art. 102 del EOSF*, constituye una operación sospechosa cualquier información relevante

sobre manejo de activos, pasivos u otros recursos, cuya cuantía o características no guarden relación con la actividad económica de sus clientes, o sobre transacciones de sus usuarios que por su número, por las cantidades transadas o por las características particulares de las mismas, puedan conducir razonablemente a sospechar que los mismos están usando al Patrimonio Autónomo para transferir, manejar, aprovechar o invertir dineros o recursos provenientes de actividades delictivas o destinados a su financiación.

- **Organización Internacional:** Es una entidad establecida mediante acuerdos políticos oficiales entre sus Estados Miembros, los cuales tienen el estatus de tratados internacionales; ejemplo: ONU (Organización de las Naciones Unidas), OEA (Organización de los Estados Americanos), OTAN (Organización del Tratado del Atlántico Norte), entre otras.

- **Partes Relacionadas:** Personas naturales o jurídicas, tiene la facultad de influir significativamente en la gerencia o en las políticas operacionales de las partes involucradas en una transacción, o cuando una tercera entidad o persona tiene interés patrimonial en una de las partes y la facultad de influir significativamente en la otra, de tal forma que una o más de las partes involucradas pudiera estar impedida de perseguir completamente sus propios intereses.

- **Pérdidas:** Cuantificación económica de la ocurrencia de un evento de riesgo operacional, así como los gastos derivados de su atención.

- **Pérdida Bruta:** Pérdida antes de recuperaciones de cualquier tipo.

- **Pérdida Neta:** Pérdida después de tener en consideración los efectos de las recuperaciones. La recuperación es un hecho independiente, relacionado con el evento de pérdida bruta, que no necesariamente se efectúa en el mismo periodo por el que se perciben fondos o flujos económicos.

- **Perfil de Riesgo:** Resultado consolidado de la medición de los riesgos a los que se ve expuesta al Patrimonio Autónomo.

- **Personas Expuestas Políticamente:** Son las personas que ocupen los cargos señalados en el *Artículo 2.1.4.2.3. del Decreto 830 del 26 de julio de 2021*. Para efecto del cumplimiento de las obligaciones derivadas de ese capítulo, durante el periodo en el que ocupen sus cargos y durante los dos (2) años siguientes a su dejación, renuncia, despido o declaración de insubsistencia del nombramiento, o de cualquier otra forma de desvinculación, se consideraran como Personas Expuestas Políticamente (PEP).

- **Plan de Acción:** Instrumento de programación y control para la ejecución de acciones orientadas a mitigar riesgos operacionales.

- **Plan de Contingencia:** Conjunto de acciones y recursos para responder a las situaciones adversas, fallas e interrupciones específicas de un sistema o proceso, así como para resolver las vulnerabilidades identificadas en los ejercicios de estrés.

El plan debe ser realista, viable y coherente con el plan de negocio y apetito de riesgo.

- **Plan de Continuidad del Negocio - PCN:** Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para responder, recuperar, reanudar y restaurar la operación, en caso de interrupción.

- **Proveedores:** Son aquellas personas naturales o jurídicas que proveen o abastecen de bienes o servicios necesarios a una entidad vigilada, para el desarrollo de su actividad y funcionamiento, a través de la celebración de un contrato.

- **Probabilidad:** Posibilidad de ocurrencia de un riesgo.

- **Riesgo:** Efecto de incertidumbre sobre los objetivos.

- **Riesgo Operacional:** Posibilidad de que el Patrimonio Autónomo incurra en pérdidas por las deficiencias, fallas o inadecuado funcionamiento de los procesos, la tecnología, la infraestructura o el recurso humano, así como por la ocurrencia de acontecimientos externos asociados a éstos. Incluye el riesgo legal.

- **Riesgo de Lavado de Activos y Financiación del Terrorismo (LA/FT):** Es definido por la Superintendencia Financiera de Colombia como: "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, éstos son: el legal, reputacional, operativo y de contagio, a los que se expone al Patrimonio Autónomo, con el consecuente efecto económico negativo que ello puede representar para su estabilidad financiera cuando es utilizada para tales actividades."

- **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 del Patrimonio Autónomo. Esta contingencia (riesgo de liquidez de fondeo) se manifiesta en la insuficiencia de activos líquidos disponibles para ello y/o en la necesidad de asumir costos inusuales de fondeo. A su turno, la capacidad del Patrimonio Autónomo para generar o deshacer posiciones financieras a precios de mercado se ve limitada bien sea porque no existe la profundidad adecuada del mercado o porque se presentan cambios drásticos en las tasas y precios (Riesgo de Liquidez y de Mercado).

- **Riesgo Inherente:** Probabilidad de que el Patrimonio Autónomo incurra en una pérdida como resultado de su exposición a eventos presentes y futuros, antes de aplicar los mecanismos de mitigación. Esto incluye los riesgos actuales y potenciales.

- **Riesgo Legal o Jurídico:** Posibilidad de pérdida en que incurre el Patrimonio Autónomo al ser sancionado u obligado 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. Aplica a todas las actividades e incluye a terceros que actúen en representación del Patrimonio Autónomo respecto de los procesos y/o actividades tercerizadas.

- **Riesgo de Mercado:** Posibilidad de que el Patrimonio Autónomo incurra en pérdidas asociadas a la disminución del valor de sus portafolios, las caídas del valor de los fondos de inversión colectivos o fondos que administran, por efecto de cambios en el precio de los instrumentos financieros en los cuales se mantienen posiciones dentro o fuera del balance.

- **Riesgo Reputacional:** Posibilidad de pérdida en que incurre al Patrimonio Autónomo 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. Este tipo de riesgo es inherente al desarrollo de las actividades del Patrimonio Autónomo.

- **Riesgo Residual:** Nivel de riesgo teniendo en cuenta el efecto de los controles establecidos en los procesos.

- **Señales de Alerta:** Son hechos, situaciones, eventos, cuantías o indicadores financieros que la experiencia nacional e internacional ha identificado como elementos de juicio a partir de los cuales se puede inferir la posible existencia de un hecho o situación que escapa a lo que el Patrimonio Autónomo en el giro ordinario de sus operaciones ha determinado como normal. Estas señales de alerta deben considerar la naturaleza específica de cada entidad, las diversas clases de productos o servicios que ofrece, los niveles de riesgo, cualquier otro criterio que a su juicio resulte adecuado y los demás mecanismos e instrumentos señalados en el presente manual.

- **Sistema de Gestión de Calidad (SGC):** Un conjunto de políticas, procesos y procedimientos utilizados por una organización para asegurar que sus productos o servicios cumplan con los estándares de calidad y satisfagan las necesidades y expectativas de sus clientes.

- **Sistema Integral de Administración de Riesgos (SIAR):** Es un conjunto de políticas, estrategias, prácticas, procedimientos, metodologías, controles y umbrales y/o límites que, de manera integrada y coordinada, le permiten a Fiducoldex:

    - Establecer y fomentar una cultura de riesgo.
    - Diseñar, implementar y monitorear el marco de apetito de riesgo y la estrategia para su ejecución.
    - Articular la gestión de riesgos con el plan del negocio, los niveles de capital y liquidez y el apetito de riesgo.
    - Identificar, medir, controlar, monitorear y reportar oportuna e integralmente los riesgos inherentes al desarrollo del negocio, incluidos los derivados de la administración de activos de terceros.
    - Contribuir a la evaluación de la suficiencia de capital y liquidez.

- Guardar coherencia entre sus políticas de gestión de riesgos y las de sus subordinadas

- **Tercero:** Persona jurídica o natural que tenga algún tipo de vínculo o relación con la fiduciaria o sus negocios administrados, (proveedores, trabajadores, contraparte, etc.)

- **Tolerancia al Riesgo:** Nivel aceptable de variación o desviación frente al apetito de riesgo que el Patrimonio Autónomo está dispuesta a aceptar en la búsqueda del logro de sus objetivos.

- **Tratamiento de Riesgos:** Decisión que se toma frente a un determinado nivel de riesgo operacional, los cuales pueden ser: aceptar o reducir o transferir.

    - **Aceptar Riesgos:** Decisión informada de aceptar los impactos ocasionados por la materialización de un riesgo.
    - **Reducir Probabilidad / Impacto Riesgos:** Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina no aceptar el riesgo, y se inicia una aplicación selectiva de técnicas apropiadas y principios de administración para reducir las probabilidades de ocurrencia, de sus consecuencias, o de ambas.
    - **Transferir Riesgos:** Cambiar la responsabilidad económica a un tercero mediante legislación, contrato, seguros u otros medios. Transferir riesgos también se puede referir a cambiar un riesgo o parte de este a otro sitio.

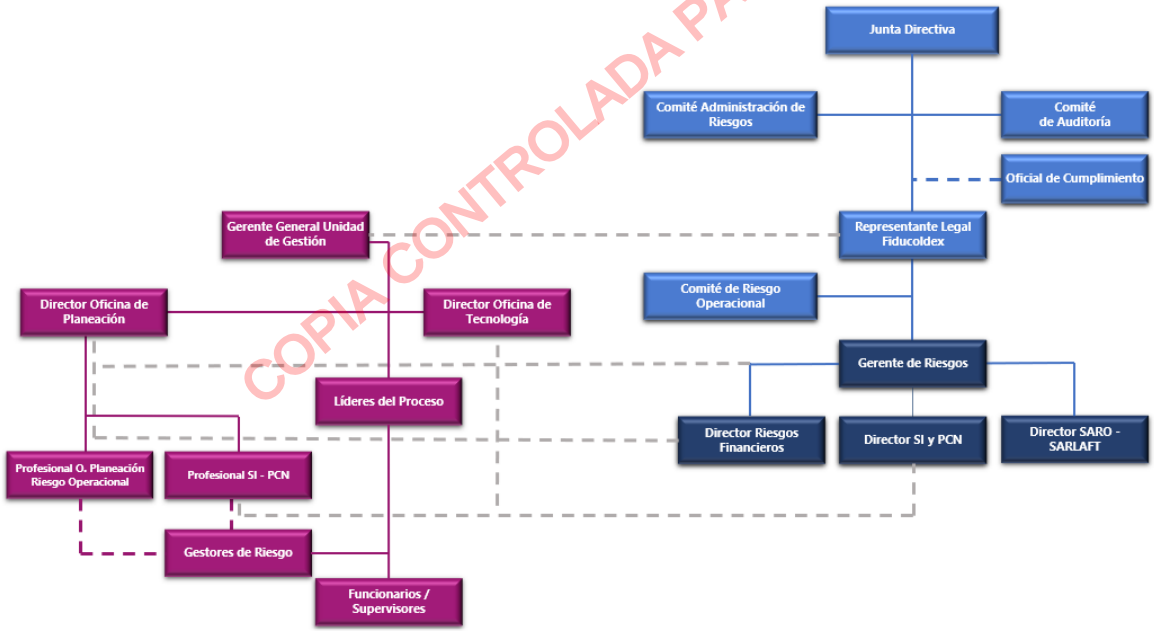
Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

2 CAPÍTULO II – RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS

A continuación, se presenta la estructura de Gobierno de Riesgos del P.A. FONTUR y se especifican las funciones de las instancias y áreas del nivel estratégico de Fiducoldex, así como las correspondientes al Patrimonio Autónomo, incluyendo las líneas de relacionamiento, con el objetivo de hacer una efectiva gestión de los riesgos operacionales, de lavado de activos, seguridad y continuidad de negocio, con el propósito de asegurar el cumplimiento de los objetivos del P.A. FONTUR y de las obligaciones establecidas para Fiducoldex S.A en el Contrato No.413-2023 suscrito con el Ministerio de Comercio, Industria y Turismo.

2.1 Organigrama de Gobierno de Riesgos

Gráfica 1. Organigrama de Gobierno de Riesgos



NOTA: *La línea punteada indica canales de comunicación.*

2.2 Responsabilidades de la línea estratégica de Fiducoldex para la Gestión de Riesgos del P.A. FONTUR

2.2.1 Junta Directiva de Fiducoldex

En cuanto al SIAR y la Gestión de Riesgo Operacional

Acorde con lo establecido en el numeral 3.1. de la Parte 1, del Capítulo XXXI de la Circular Básica Contable y Financiera y con lo definido en el numeral 1.8.1.1 del Manual SIAR de FIDUCOLDEX, hace parte de las funciones de la Junta Directiva aprobar las

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

políticas del Sistema Integral de Administración de Riesgos (SIAR) de Fiducoldex, la estructura de gobierno de riesgos, el Marco de Apetito de Riesgo y los límites generales de exposición y concentración. Así mismo, realizar el monitoreo del SIAR y el seguimiento a la exposición a los riesgos adoptando las medidas frente a las desviaciones de este sistema.

De manera específica, le compete a la Junta Directiva hacer seguimiento a la evolución del riesgo Operacional a partir de los informes semestrales de gestión de riesgo operacional que le presente la Gerencia de Riesgos, lo cual incluye las gestiones realizadas tanto en la Sociedad Fiduciaria como en el P.A. FONTUR y los demás patrimonios administrados, incluyendo el monitoreo del perfil de riesgos y el estado de los controles implementados.

La conformación y funciones de la Junta Directiva de Fiducoldex se encuentran definidos en su reglamento, RE-GJU-003.

En cuanto a SARLAFT

Le corresponde a la Junta Directiva aprobar las políticas, manual de procedimientos, estructura y mecanismos del SARLAFT, así como el procedimiento para el conocimiento del potencial cliente, así como las metodologías de segmentación, identificación, medición y control del SARLAFT, y efectuar seguimiento a la exposición del riesgo LAFT, acorde con lo estipulado en el numeral 4.2.4.1. de la Parte I – Título IV – Capítulo IV de la Circular Básica Jurídica.

En cuanto a la Gestión de Seguridad de la Información

Le compete a la Junta Directiva la aprobación de la Política de Seguridad de la información de la Fiduciaria, aplicable también al P.A. FONTUR.

2.2.2 Comité de Administración de Riesgos de Fiducoldex – CAR

Acorde con lo establecido en su reglamento RE-GRI-001 y en la normatividad vigente de la Superintendencia Financiera de Colombia (SFC) le corresponde al CAR realizar el seguimiento al perfil y apetito de riesgos de la Fiduciaria, asesorar a la Junta Directiva sobre las operaciones, eventos o actividades que pueda afectar la exposición y perfil de riesgos del Patrimonio Autónomo e informar los análisis de resultados de los reportes recibidos desde la Gerencia de Riesgos, revisar las políticas del SIAR, así como las propuestas de manuales, metodologías para la gestión de riesgos y proponer a la Junta Directiva para su respectiva aprobación. Así mismo, el Comité realiza la evaluación sobre la idoneidad del plan de continuidad del negocio y los planes de contingencia.

2.2.3 Comité de Auditoría de Fiducoldex

Es un órgano conformado para el adecuado cumplimiento de la labor que le corresponde a la Junta Directiva de FIDUCOLDEX en la definición de las políticas y en la ordenación del diseño de los procedimientos del Sistema de Control Interno. Su conformación y funciones están estipuladas en su reglamento interno, RE-ACO-001, así como en la normatividad vigente de la Superintendencia Financiera de Colombia.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

2.2.4 Representante Legal de Fiducoldex

Acorde con lo establecido el numeral 1.8.1.2 del Manual SIAR de Fiducoldex es función del Representante Legal someter a aprobación de la Junta Directiva el plan de negocio, el MAR, las políticas del SIAR, los límites, la estructura de gobierno de riesgos y las estrategias de capital y liquidez. Así mismo, aprobar el manual del SIAR y los planes de contingencia y de continuidad del negocio. Igualmente, realizar monitoreo al SIAR y seguimiento a activos, pasivos, capital, liquidez y estrategia de fondeo e informa a la Junta Directiva sobre el desempeño financiero y la gestión de riesgos.

De la misma forma, le corresponde someter a aprobación de la Junta Directiva en coordinación con el Oficial de Cumplimiento, el manual de procedimientos del SARLAFT y sus actualizaciones, velar porque los procedimientos establecidos desarrollen todas las políticas adoptadas, y adoptar las medidas adecuadas como resultado de la evolución de los perfiles de riesgo de los factores de riesgo y de los riesgos asociados.

Con relación al P.A. FONTUR, el Representante Legal de Fiducoldex se encargará de revisar el cumplimiento por parte del P.A. FONTUR de las políticas, funciones y actividades definidas en el presente Manual y en los planes de trabajo, a través de los informes que le presente la Gerencia de Riesgos y sus direcciones, así como por parte del Gerente General del Patrimonio.

2.2.5 Comité de Riesgo Operacional de Fiducoldex

Acorde con su reglamento RE-GRI-002, el Comité de Riesgo Operacional es la instancia interna, que asesora y vela en Fiducoldex por el cumplimiento de los requerimientos normativos en materia de gestión del riesgo operacional, lidera la definición de directrices y lineamientos para fortalecer la cultura de riesgo operacional, realiza seguimiento al cumplimiento de los planes, procedimientos y metodologías definidas para la identificación, control, monitoreo de este riesgo, así mismo realiza seguimiento a la evolución del riesgo operacional de la Fiduciaria y los negocios administrados y de los eventos de riesgo operacional, entre estos los relacionados con el P.A. FONTUR. Igualmente, hace parte de sus funciones, realizar seguimiento a la implementación y mantenimiento de los sistemas de Gestión de Seguridad de la Información, Continuidad de Negocio y Protección de Datos Personales.

Este Comité podrá requerir la participación del Gerente General del P.A. FONTUR, del director de la Oficina de Planeación o de algún líder de proceso del Patrimonio Autónomo, cuando lo considere necesario, para efectos de realizar seguimiento a la gestión de riesgo operacional en el Patrimonio y de los sistemas previamente mencionados.

2.2.6 Oficial de Cumplimiento de Fiducoldex

El Oficial de Cumplimiento es el responsable de velar por el adecuado funcionamiento dentro de la Fiduciaria y sus patrimonios administrados, de las etapas y elementos específicos que conforman el SARLAFT, vigilar la adecuada observancia de los procedimientos específicos diseñados dentro de las políticas y manuales con el fin de prevenir el riesgo LAFT, proponer a la Junta Directiva la actualización del Manual y velar por su divulgación. Así mismo, verificar que existan los controles y que se presenten los

reportes en materia de SARLAFT, definidos por las autoridades competentes, entre otras funciones establecidas en el numeral 4.2.4.1. de la Parte I – Título IV – Capítulo IV de la Circular Básica Jurídica.

En Fiducoldex la función de Oficial de Cumplimiento Principal la ejerce el Gerente de Riesgos y el Oficial de Cumplimiento Suplente la ejerce la Dirección SARO-SARLAFT, acorde con la designación de la Junta Directiva de FIDUCOLDEX y la posesión realizada por la Superintendencia Financiera, quienes en cumplimiento de sus funciones vigilarán que en el P.A. FONTUR cumpla con las obligaciones impartidas en el marco del SARLAFT.

2.2.7 Gerente de Riesgos

El Gerente de Riesgos en cumplimiento de las funciones asignadas en el numeral 1.8.1.3 del Manual SIAR de Fiducoldex es responsable de desarrollar las políticas, los procedimientos, las estrategias, las metodologías, los modelos, umbrales y/o los límites, los controles, los planes de contingencia y el plan de continuidad del negocio y el marco de indicadores de alertas tempranas y de seguimiento del MAR. Así mismo, de realizar seguimiento a los niveles de exposición y reportados a la Junta Directiva, el Representante Legal y al Comité de Administración de Riesgos.

En este sentido, la Gerencia de Riesgos, a través de las Direcciones SARO – SARLAFT y la Dirección de Seguridad de la Información y PCN, brindará y comunicará los lineamientos para el cumplimiento de la gestión de riesgos, de seguridad de la información, de continuidad del negocio y de protección de datos por parte del P.A. FONTUR. De la misma manera, en el marco de sus funciones, analizará, hará seguimiento y presentará al Representante Legal de la Fiduciaria, al CAR y a la Junta Directiva el estado de cumplimiento por parte del P.A. FONTUR de las políticas, funciones y actividades definidas en el presente Manual y sus documentos asociados.

2.2.8 Director SARO – SARLAFT de Fiducoldex

Le corresponde a esta Dirección liderar la planeación y seguimiento a la Gestión del Riesgo Operacional y del Riesgo de Lavado de Activos de la Fiduciaria, de los negocios empresariales y los negocios fiduciarios, la cual incluya las actividades de actualización de las matrices de riesgo, monitoreo de controles, sensibilización y capacitación, gestión de eventos de riesgo, entre otras. Así mismo, es responsable de proponer las políticas, lineamientos, procedimientos, metodologías e instrumentos para la gestión de los riesgos LAFT y operacionales, incluyendo los de fraude y corrupción, ASG, estratégicos y emergentes en todas sus etapas (identificación, medición, control y monitoreo).

El director SARO-SARLAFT dará las directrices y lineamientos a la Oficina de Planeación del P.A. FONTUR para la definición y ejecución del plan anual de actividades en materia de gestión de riesgo operacional, así como para la gestión de los eventos de riesgo operacional. Así mismo, realizará el respectivo seguimiento con el fin de reportarlo a las instancias internas y externas que lo requieran.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

2.2.9 Director de Seguridad de la Información y PCN Fiducoldex

El director de Seguridad de la Información y PCN tiene la responsabilidad de establecer las directrices respecto a la implementación, mantenimiento y fortalecimiento de la gestión de seguridad y ciberseguridad de la información, continuidad del negocio y protección de datos tanto de Fiducoldex como sus patrimonios administrados, incluyendo el P.A. FONTUR de acuerdo con lo establecido en la normatividad que le rige. Así mismo, reporta los avances al Gerente de Riesgos, al Comité de Riesgo Operacional, así como al Representante Legal y a la Junta Directiva de Fiducoldex y las instancias externas que lo requieran.

En este sentido, brindará las directrices para la gestión de seguridad de la información, ciberseguridad y continuidad de negocio del P.A. FONTUR y para la definición y ejecución del respectivo plan anual de actividades. Igualmente adelantará su seguimiento, así como a la gestión de riesgos, de incidentes y de vulnerabilidades, con el fin de reportarlo a las instancias internas y externas que lo requieran.

2.3 Responsabilidades para la Gestión de Riesgos en el P.A. FONTUR

2.3.1 Gerente General del P.A. FONTUR

Corresponde al Gerente General del P.A. FONTUR velar y promover el cumplimiento de las políticas, lineamientos, normatividad, metodologías y procedimientos en el P.A. FONTUR establecidos para gestionar los riesgos operacionales, de lavado de activos, seguridad de la información y continuidad del negocio, efectuar el seguimiento periódico a la evolución de los perfiles de riesgo, vigilando que estos se encuentren dentro de los niveles de apetito de riesgo definidos por la Junta Directiva de Fiducoldex; así como al cumplimiento de planes de actividades, planes de acción y tratamiento de riesgos, a través de los informes que le presente la Oficina de Planeación del Patrimonio.

El Gerente General del P.A. FONTUR tendrá bajo su responsabilidad presentar con el apoyo de la Oficina de Planeación y las áreas del patrimonio que determine, los resultados de la gestión en materia de gestión de riesgos, seguridad de la información y continuidad de negocio al presidente de Fiducoldex, al Comité Fiduciario y al supervisor que determine el Ministerio de Comercio, Industria y Turismo.

2.3.2 Director Oficina de Planeación del P.A. FONTUR

- Formular propuesta del plan de acción anual para la gestión de riesgo operacional de los procesos del P.A. FONTUR, programas, proyectos y contratos, el cual incluya las actividades para la actualización de las matrices de riesgo, monitoreo de controles y sensibilización y capacitación.

- Dar cumplimiento a los procedimientos, metodologías e instrumentos para la gestión del riesgo operacional en todas sus etapas (identificación, medición, control y monitoreo) que tenga establecidas Fiducoldex.

- Definir y ejecutar el plan de sensibilización y capacitación en materia de gestión del riesgo operacional dirigida a los procesos y trabajadores del P.A. FONTUR, en los

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

tiempos y cobertura definidos y reportar a la Dirección SARO-SARLAFT de Fiducoldex, los indicadores de ejecución.

- Realizar acompañamiento a los procesos del P.A. FONTUR en las diferentes etapas de la gestión del riesgo operacional, con el fin de realizar la actualización de los respectivos perfiles de riesgo.

- Hacer seguimiento a las gestiones para la actualización del perfil de riesgo operacional de los procesos y elaborar y presentar a la Dirección SARO-SARLAFT de Fiducoldex un informe en las periodicidades que estas áreas acuerden.

- Consolidar los perfiles de riesgo operacional del P.A. FONTUR, acorde con el desarrollo del plan anual de actividades formulado y presentarlos a la Dirección SARO-SARLAFT de Fiducoldex para su revisión y validación, previa presentación al Comité de Riesgo Operacional los resultados.

- Exigir a los líderes de proceso el reporte de eventos de riesgo operacional materializados, de los cuales se tenga conocimiento y que hayan afectado los procesos, proyectos o negocios jurídicos, asegurando la calidad, confiabilidad y suficiencia de la información suministrada.

- Realizar los ejercicios de monitoreo a los controles a partir de la verificación de evidencias de su ejecución y presentar los informes de avance y resultados a la Gerencia de Riesgos de Fiducoldex por intermedio de la Dirección SARO-SARLAFT, acorde con el muestreo que el Comité de Riesgo Operacional de Fiducoldex defina.

- Acompañar la formulación y hacer el seguimiento al cumplimiento de la ejecución de los planes de tratamiento adoptados por los lideres de proceso para mitigar los riesgos y de los planes de acción frente a los eventos de riesgo materializados e informar a la Gerencia de Riesgos de Fiducoldex por intermedio de la Dirección SARO-SARLAFT, En caso de presentarse situaciones que no permitan el cumplimiento de los planes de acción en las fechas establecidas, deberán notifica a la Dirección SARO - SARLAFT, dentro de los tiempos establecidos en cumplimiento a la directriz impartida por el Comité de Riesgo operacional de Fiducoldex.

- Realizar la medición y reporte mensual a la Dirección SARO-SARLAFT de los indicadores descriptivos y prospectivos de riesgo, así como los que se establezcan en el tablero de control por parte de la Presidencia de Fiducoldex, para lo cual tendrá acceso a estos documentos.

- Informar a la Dirección SARO-SARLAFT las situaciones que hayan generado controversias o conflictos de interés en la gestión de riesgos, para que sean escalados al Comité de Riesgo Operacional.

- Consolidar las certificaciones trimestrales emitidas por los líderes de proceso frente al seguimiento a los riesgos operacionales asociados a los procesos y remitirlas a la Gerencia de Riesgos de Fiducoldex por intermedio de la Dirección SARO-SARLAFT.

- Atender de manera diligente y oportuna los requerimientos de entes de vigilancia y control, la Revisoría Fiscal y la Gerencia de Auditoría Interna, relacionados con el SIAR (Sistema Integral de Administración de Riesgos) y la Gestión de Riesgo Operacional en el P.A. FONTUR; analizar los informes y conclusiones, y proponer dentro de los plazos establecidos los planes de acción para subsanar los hallazgos u observaciones.

- Preparar los informes que requiera Fiducoldex y el Ministerio de Comercio, Industria y Turismo respecto a la gestión de riesgos.

En relación con la seguridad de la información, ciberseguridad y continuidad del negocio serán funciones de la Oficina de Planeación del P.A. FONTUR:

- Establecer un plan de trabajo anual para la gestión de seguridad y ciberseguridad de la información del P.A. FONTUR y preparar y entregar informes mensuales de avance al director de Seguridad de la Información y PCN de Fiducoldex para su consolidación y presentación al Ministerio de Comercio, Industria y Turismo.

- Realizar un diagnóstico y la documentación de procedimientos, instructivos, formatos y controles, entre otros, requerida para la Gestión de Seguridad de la Información, Ciberseguridad, Continuidad de Negocio y Protección de Datos Personales del P.A. FONTUR y para el fortalecimiento del respectivo nivel de madurez.

- Coordinar el análisis, evaluación y tratamiento de los riesgos relacionados con seguridad y privacidad de la información y de continuidad del negocio a los que se expone el P.A. FONTUR y acompañar a los diferentes procesos en el desarrollo de las etapas de la gestión de riesgos, garantizando la oportuna gestión y cumplimiento de la metodología establecida en la Fiduciaria.

- Participar en los análisis de riesgos para la implementación de nuevas soluciones tecnológicas y proyectos del P.A. FONTUR y proponer controles para su mitigación, así como apoyar la definición de requerimientos técnicos de seguridad a ser incorporados en los procesos de contratación.

- Preparar informes relacionados con la gestión de la seguridad, ciberseguridad de la información, continuidad del negocio y protección de datos del P.A. FONTUR que sean requeridos para diferentes instancias internas, para el Ministerio de Comercio, Industria y Turismo, así como para otros organismos de vigilancia y control.

- Desarrollar con la participación de los lideres de proceso del P.A. FONTUR, los ejercicios de identificación y valoración de activos de información y de análisis BIA, la definición de estrategias de continuidad de negocio y la planeación, ejecución y documentación de las pruebas de continuidad, atendiendo las directrices del director de Seguridad de la Información y PCN de Fiducoldex.

- Ejecutar el programa de divulgación y sensibilización al interior del P.A. FONTUR, y promover el cumplimiento a los lineamientos y normatividad relacionada con la

gestión de seguridad de la información, ciberseguridad, continuidad de negocio y protección de datos personales.

- Indagar e identificar las actualizaciones y novedades sobre los requerimientos regulatorios que apliquen al interior del P.A. FONTUR, respecto a seguridad, ciberseguridad de la información, continuidad del negocio y protección de datos personales, con el fin de suministrar a la Dirección de Seguridad de la Información y PCN, la información necesaria para el ajuste o definición de políticas, procedimientos y controles.

- Realizar la verificación de controles y apoyar la realización de monitoreos y pruebas de vulnerabilidad y Ethical Hacking que determine la Dirección de Seguridad de la Información y PCN de Fiducoldex, como parte de su plan de trabajo; y apoyar el análisis de los informes de monitoreo que adelanten proveedores externos; así como gestionar con la Oficina de Tecnología la formulación y seguimiento de los planes de remediación de vulnerabilidades y presentar los resultados a la Dirección Seguridad de la Información y PCN de Fiducoldex, así como al Gerente General del P.A. FONTUR y al Ministerio de Comercio, Industria y Turismo.

- Apoyar el desarrollo de las etapas para la gestión de los incidentes de seguridad de la información que se presenten en el P.A. FONTUR y adelantar su documentación.

- Adelantar la actualización del Registro Nacional de Bases de Datos (RNBD) dentro los plazos establecidos en la normatividad vigente.

- Efectuar el seguimiento al reporte de los eventos de riesgo e incidentes de seguridad y privacidad de la información y de continuidad y realizar el acompañamiento a los líderes de proceso del Patrimonio en la definición de los planes de acción y generar los informes de avance de estos planes, requeridos por el Gerente General del P.A. FONTUR, el Ministerio de Comercio, Industria y Turismo, el Director de Seguridad de la Información y PCN de Fiducoldex, el Comité de Riesgo Operacional de Fiducoldex y/o entes de vigilancia y control.

- Realizar la gestión, atención y acompañamiento a la Dirección de Seguridad de la Información y PCN de Fiducoldex y a los líderes de proceso del P.A. FONTUR en lo relacionado con la definición y/o mantenimiento de requisitos normativos en materia de Protección de Datos Personales.

- Gestionar la identificación y valoración de los activos de información y la conformación de los reportes de información clasificada y reservada del P.A. FONTUR.

- La Oficina de Planeación es responsable de desarrollar las políticas, procedimientos e instructivos necesarios para garantizar el cumplimiento de los lineamientos de seguridad de la información, continuidad de negocio y protección de datos, en estrecha colaboración con la Dirección de Seguridad de la Información y PCN.

2.3.3 Director de Auditoría Interna

Acorde con las funciones que le corresponden a la Auditoría Interna en materia del SIAR, SARLAFT y Seguridad y continuidad del negocio, le compete a la Dirección de Auditoría Interna de FONTUR, la cual se reporta de acuerdo con lo implementado en el otrosí No. 6 a la Gerencia de Auditoría de Fiducoldex, verificar y evaluar, a través de los procesos de auditoría que programe y ejecute periódicamente el cumplimiento de las políticas, lineamientos, procedimientos, controles para asegurar la efectividad de la Gestión de Riesgos, de Seguridad y privacidad de la información y continuidad del negocio del P.A. FONTUR. Así mismo, deberá presentar a la Gerencia General del Patrimonio los resultados de las auditorías realizadas enfocadas a evaluar y mejorar la efectividad de los procesos de gestión de riesgo, control y gobierno. Los informes generados de las auditorías deben ser compartidos a la Oficina de Planeación del P.A. FONTUR y a la Dirección SARO-SARLAFT de Fiducoldex.

2.3.4 Líderes de los procesos del P.A. FONTUR

Hace parte de las funciones de los líderes de proceso, relacionadas con la gestión de riesgos las siguientes:

- Promover en su proceso el cumplimiento de las políticas, procedimientos, metodologías y responsabilidades para la gestión de los Riesgos Operacional y de Lavado de Activos y Financiación del Terrorismo y del SIAR para el P.A. FONTUR.

- Socializar los instrumentos de Gestión del Riesgo aplicables a los procesos que lidera y sus actualizaciones, cuando haya lugar.

- Identificar y valorar de los riesgos operacionales, así como la definición, diseño y calificación de los controles correspondientes, en los procesos a su cargo, con base en las metodologías y procedimientos definidos por Fiducoldex aplicables al P.A. FONTUR, asegurando que las matrices de riesgo operacional, los documentos y registros del proceso a su cargo se mantengan actualizados para lo cual se debe tener en cuenta si se presentan cambios en el contexto, en la normatividad aplicable, forma de operación, recurso humano o en la tecnología e infraestructura de su proceso.

- Realizar la adecuada definición, documentación, implementación, seguimiento y mejora de los controles, capacitando a los responsables de su aplicación, de forma que se ejecuten y/o implementen de manera efectiva para mitigar los riesgos.

- Realizar el reporte de los eventos de riesgo operacional materializados, de los cuales tengan conocimiento y afecten los procesos que lidera o con los que interactúa, asegurando la calidad, confiabilidad y suficiencia de la información suministrada. Así mismo, formular e implementar oportunamente los respectivos planes de acción o tratamiento para prevenir la ocurrencia de nuevos eventos.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

- Participar en la formulación a cargo de la Oficina de Planeación de indicadores descriptivos y/o prospectivos de riesgo y realizar la medición de los indicadores que sean de su competencia.

- Adelantar las actividades que requieran la Dirección SARO- SARLAFT y la Gerencia de Riesgos de Fiducoldex para fortalecer la gestión del Riesgo Operacional y asegurar el cumplimiento normativo.

- Garantizar la permanente actualización de los documentos y registros de los procesos a cargo.

- Asistir a las capacitaciones que se programen desde Fiducoldex y el P.A. FONTUR sobre la administración de riesgos y promover la participación de sus equipos de trabajo en las mismas.

- Consolidar y conservar en forma adecuada la información que demuestre la implementación y mantenimiento del SIAR (Sistema Integral de Administración de Riesgos) y de la Gestión de Riesgo Operacional, así como la ejecución de los controles y proporcionarla en los plazos definidos por la Oficina de Planeación o la Dirección de Auditoría Interna del P.A. FONTUR cuando el ejercicio de sus funciones la requiera, la Dirección SARO-SARLAFT y/o la Gerencia de Riesgos de Fiducoldex.

- Emitir certificación trimestral del reporte de eventos de riesgo operacional asociados a los procesos que lidera y remitirla a la Dirección SARO – SARLAFT, a través de la Oficina de Planeación del P.A. FONTUR, conforme al formato establecido por Fiducoldex.

- Atender de manera diligente y oportuna los requerimientos de entes de vigilancia y control relacionados con el SIAR (Sistema Integral de Administración de Riesgos) o con relación al P.A. FONTUR y remitir la información y/o soportes que se requieran a la Oficina de Planeación del P.A. FONTUR, por cuyo intermedio se remiten a la Gerencia de Riesgos de Fiducoldex a través de la Dirección SARO-SARLAFT.

- Designar el Gestor de Riesgo Operacional de su proceso.

En relación con la seguridad de la información, ciberseguridad y continuidad del negocio serán funciones de los lideres de proceso:

- Identificar, medir, controlar y monitorear los posibles riesgos de seguridad de la información y ciberseguridad asociados a gestión del P.A. FONTUR y de sus activos de información.

- Adelantar la identificación y valoración de los activos de información correspondientes a su proceso y apoyar la definición de mecanismos para su protección, para lo cual contarán con el apoyo del profesional SI – PCN.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

- Participar cada vez que se requiera en los ejercicios de BIA, en la definición de estrategias de continuidad del negocio y en la planeación y ejecución de las pruebas de continuidad, para lo cual contara con el profesional del SI – PCN del P.A. FONTUR.

2.3.5 Director de la Oficina de Tecnología del P.A. FONTUR

- Formular y ejecutar los planes de trabajo para mitigar las vulnerabilidades que se identifiquen en los análisis correspondientes y de Ethical Hacking desde Fiducoldex y apoyar la presentación de los informes de las gestiones realizadas a las instancias internas o externas que se requieran.

- Apoyar el desarrollo de las etapas para la gestión de los incidentes de seguridad de la información que se presenten en el P.A. FONTUR y adelantar su documentación.

- Designar al interior de la Oficina de Tecnología el responsable de la gestión de usuarios y control de acceso.

- Participar en la definición de procedimientos para la gestión de usuarios, control de accesos y demás que se requieran para el fortalecimiento de la gestión de seguridad, ciberseguridad de la información y continuidad de negocio.

- Gestionar la definición, implementación y documentación del plan de contingencia tecnológica y ejecutar las pruebas del plan de continuidad de negocio con relación al componente tecnológico y de comunicaciones, en coordinación con la Dirección de seguridad de la información y PCN.

2.3.6 Gestores de Riesgo de P.A. FONTUR

- Asistir a las capacitaciones periódicas impartidas y coordinadas por el responsable de la Oficina de Planeación del P.A. FONTUR y por la Dirección SARO – SARLAFT de Fiducoldex para el adecuado desarrollo de su función y promover el cumplimiento por parte de los colaboradores de su proceso o área respectiva.

- Difundir la importancia de la gestión del riesgo operacional, así como de las políticas y procedimientos definidos, contribuyendo así a fortalecer la cultura de riesgo operacional en el P.A. FONTUR.

- Apoyar la ejecución de las etapas de identificación, medición y control de los riesgos operacionales, de fraude y corrupción, de seguridad de la información y continuidad de negocios del respectivo proceso. De igual forma, apoyar la formulación de medidas y planes de tratamiento para mitigar los riesgos, y reportar a la Oficina de Planeación del P.A. FONTUR el avance y cumplimiento de sus actividades.

- Registrar y reportar los eventos de riesgo operacional que se materialicen en los procesos a su cargo, en la herramienta tecnológica definida y atendiendo los procedimientos y tiempos establecidos por Fiducoldex; así mismo, apoyar al líder de proceso en la definición y seguimiento a la ejecución de los planes de acción para mitigarlos.

- Velar por el cumplimiento en el proceso, de las políticas y procedimientos de riesgo operacional definidos por Fiducoldex.

- Informar al responsable de la Oficina de Planeación del P.A. FONTUR cuando se requiera realizar la actualización de la matriz de riesgos del Patrimonio Autónomo.

- Atender las solicitudes que formule la Dirección SARO- SARLAFT y la Gerencia de Riesgos de Fiducoldex para la gestión del SIAR (Sistema Integral de Administración de Riesgos).

- Apoyar la atención diligente y oportuna los requerimientos de entes de vigilancia y control relacionados con el SIAR (Sistema Integral de Administración de Riesgos) del P.A. FONTUR y la consolidación de la información y/o soportes que requieran por parte de la Oficina de Planeación del P.A. FONTUR o la Dirección SARO-SARLAFT y/o la Gerencia de Riesgos de Fiducoldex.

- Atender las solicitudes que formule la Dirección del Seguridad de la Información y Plan de Continuidad del Negocio para la gestión de estos sistemas.

2.3.7 Trabajadores del P.A. FONTUR

En materia de Riesgo Operacional, los empleados vinculados por planta o temporal deben**:**

- Participar en la identificación y evaluación los riesgos operacionales que se puedan presentar en sus procesos o en nuevos procesos en coordinación con el gestor y/o líder del proceso.

- Aplicar efectivamente los controles a su cargo, definidos en los procesos que participa.

- Informar al gestor de riesgo respectivo sobre toda percepción de posibles riesgos operacionales y controles, en los procesos en los que intervienen, que no están incluidos en la matriz de riesgos, con el fin de actualizarla. De igual forma, informar sobre los eventos de riesgos operacional que se presenten para su registro y gestión.

- Informar al gestor de riesgo los eventos de riesgo operacional que se presenten en sus procesos y apoyar en las actividades que se requieran para la recuperación de pérdidas, si se hubiera presentado impacto económico y para el cierre y conclusión del evento.

- Cumplir con las políticas de administración de riesgos definidas por la Junta Directiva de Fiducoldex, en el SIAR y en particular las relacionadas con la entrega oportuna de información para la identificación, medición, control o monitoreo de los riesgos, así como para la atención de requerimientos de entes de vigilancia y control.

- Participar en las actividades de capacitación que hagan parte del Plan anual de Capacitación en gestión de riesgos y desarrollar las evaluaciones que se definan para la establecer el nivel de efectividad de estas.

En materia de Riesgo LAFT, los empleados vinculados por planta o temporal deben:

- Conocer, aplicar y cumplir las directrices y mecanismos de prevención y control descritas en el Manual SARLAFT, so pena de generar consecuencias de tipo penal, administrativo (sanciones personales e institucionales impuestas por la Superintendencia Financiera de Colombia), disciplinarias y/o laborales.

- Anteponer a las metas comerciales a los principios éticos, absteniéndose de celebrar cualquier tipo de negocio jurídico, con personas o entidades con las cuales no se pueda aplicar en su totalidad las políticas y procedimientos de Conocimiento de Terceros No Clientes.

- Comunicar a la Dirección SARO-SARLAFT y al Oficial de Cumplimiento, los hechos o circunstancias que puedan estar catalogados como señales de alerta u operaciones inusuales que puedan generar exposición a riesgos de LA/FT o sus delitos fuente, derivados de las relaciones comerciales o contractuales con Terceros No Clientes, proveedores, aliados o beneficiarios de los programas desarrollados dentro del P.A. FONTUR.

En materia de Riesgos de Seguridad de la Información:

- Los trabajadores tienen la responsabilidad de cumplir con los lineamientos en materia de seguridad de la información, ciberseguridad y continuidad establecidos en el presente manual y en los procedimientos que se definan.

- Participar en los ejercicios de análisis, evaluación y tratamiento de los riesgos relacionados con seguridad y privacidad de la información y de continuidad del negocio a los que se expone los procesos del P.A. FONTUR.

- Reportar los incidentes de seguridad de la información que sean de su conocimiento y apoyar la gestión de los mismos.

- Participar y/o dar cumplimiento a las actividades de sensibilización y capacitación de los lineamientos de Seguridad de la Información y Ciberseguridad en el P.A. FONTUR

2.3.8 Supervisores y/o interventores P.A. FONTUR

- Identificar y evaluar los riesgos operacionales que se puedan presentar en los negocios jurídicos suscritos por el P.A. FONTUR sobre los cuales se tenga a cargo la supervisión e interventoría.

- Aplicar efectivamente los controles a su cargo, definidos dentro de la matriz de riesgos del negocio jurídico a cargo de la supervisión y/o interventoría.

- Monitorear el cumplimiento de los controles definidos en la matriz de riesgos del negocio jurídico e informar al responsable de la Oficina de Planeación que hace parte del P.A. FONTUR, el resultado obtenido del monitoreo frente al cumplimiento y ejecución de controles por las partes, con el fin de evaluar y determinar si se requiere adoptar medidas o formular planes de mejoramiento.

- Informar al gestor de riesgo o líder de los procesos los eventos de riesgo operacionales que se materialicen sobre el negocio jurídico a cargo de la supervisión y/o interventoría, con el fin de que se efectúe el reporte del evento de riesgo operacional. Así mismo, deberá apoyar en las actividades que se requieran para definición del plan de acción o tratamiento del riesgo materializado hasta el cierre y conclusión del evento.

- Remitir los soportes que sean requeridos por el P.A. FONTUR, que se deban reportar a la Gerencia de Riesgos de Fiducoldex sobre la gestión y cumplimiento de riesgo operacional.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

3 CAPÍTULO III – GESTIÓN DEL RIESGO OPERACIONAL

3.1 Lineamientos y Procedimientos para la gestión del Riesgo Operacional

La gestión del riesgo operacional para el P.A. FONTUR se debe llevar a cabo en cumplimiento a los siguientes propósitos:

- Asegurar la calidad de los procesos y servicios.
- Contar con procesos más eficientes y mejor blindados.
- Minimizar impacto y frecuencia de riesgos operacionales.
- Apoyar la toma de decisiones.
- Reducir las pérdidas por fallas operativas.
- Permitir la detección de riesgos de manera proactiva.
- Monitorear el desempeño de los procesos del P.A. FONTUR.
- Fortalecer la cultura del control en el P.A. FONTUR y mejorar la efectividad de los controles.
- Fortalecer la cultura de riesgo operacional en el P.A. FONTUR.
- Realizar un seguimiento a la evaluación del riesgo operacional del P.A. FONTUR.
- Cumplir con los lineamientos establecidos por la Superintendencia Financiera de Colombia y las políticas establecidas por la Junta Directiva de Fiducoldex que hacen parte de Manual de Sistema Integral de Administración del Riesgos.
- Contribuir al cumplimiento del Programa de Prevención del Fraude y la Corrupción definida por la sociedad fiduciaria Fiducoldex, así como el cumplimiento de las políticas, procedimientos establecidos.

3.2 Alcance

La Gestión de Riesgos Operacional para el P.A. FONTUR comprende el cumplimiento de las políticas, procedimientos, metodologías, modelos, funciones y responsabilidades establecidas por Fiducoldex con el fin de realizar una eficiente identificación, medición, control y monitoreo del riesgo operacional al que se ve expuesto el P.A. FONTUR en el desarrollo de los procesos y actividades que ejecuta para dar cumplimiento a su objeto misional, así como de sus obligaciones contractuales.

Así mismo, la gestión de riesgo operacional debe implementarse desde la formulación y viabilidad de los programas y proyectos, hasta la contratación donde se deben identificar y medir los riesgos inherentes al programa/proyecto junto con sus respectivos controles a ejecutar, sobre los cuales se deberá ejecutar el monitoreo durante la ejecución del proyecto. Frente a la gestión de riesgo operacional de los programas/proyectos se deben atender y acatar por parte del Patrimonio los lineamientos, requerimientos y seguimientos que realice en cualquier momento Fiducoldex a través de la Gerencia de Riesgos.

3.3 Registro de Eventos de Riesgo y su tratamiento

Los eventos de riesgo son aquellos incidentes o situaciones que ocurre en un lugar particular durante un intervalo de tiempo determinado que materializa un riesgo que puede o no generar pérdida económica a Fiducoldex S.A. o al P.A. FONTUR. Teniendo en cuenta, que el registro de eventos de riesgo operacional es un mecanismo fundamental

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

para monitorear y retroalimentar el perfil de riesgo operacional del P.A. FONTUR, se deben adoptar medidas para fortalecer el reporte de los eventos materializados. En este sentido, las situaciones originadas por hallazgos, y no conformidades establecidas por la Oficina de Auditoría Interna o por entes de vigilancia y control deben ser reportados por los líderes de los procesos respectivos, una vez estos sean notificados; así mismo, deben ser reportados, los eventos relacionados con la ejecución de los programas/proyectos, o contratos que deriven acciones de tipo administrativo, contractual o judicial.

En el reporte y registro de los eventos de riesgo operacional se deben atender los siguientes lineamientos:

- La información de los eventos de riesgo operacional se debe reportar por los líderes de proceso del P.A. FONTUR, o sus gestores de riesgo a través del aplicativo que tenga implementado Fiducoldex para tal fin y esta integrará la Base de Eventos de Riesgo Operacional (BERO) de la Fiduciaria, para lo cual tendrán el apoyo y acompañamiento por parte de la Oficina de Planeación para hacer el análisis y validación previa de la información a registrar.

- El registro de eventos de riesgo operacional debe cumplir con los lineamientos mínimos establecidos en el numeral 4 de la parte 2, del Capítulo XXXI de la Circular Básica Contable y Financiera y las normas que lo modifiquen o complementen.

- El procedimiento para la gestión de eventos de riesgo operacional comprenderá las siguientes actividades:

    - Análisis de la causa raíz que generó el evento de riesgo operacional materializado que fue identificado con la participación de todos los actores involucrados.

    - Registro de eventos de riesgo operacional por parte de los procesos que reportan.

    - Análisis de eventos y definición de criticidad por el responsable de la gestión de riesgo operacional de la Oficina de Planeación que hace parte del P.A. FONTUR.

    - Seguimiento a eventos de riesgo operacional por los líderes de proceso y el responsable de la gestión de riesgo operacional de la Oficina de Planeación que hace parte del P.A. FONTUR.

    - Definición de tratamiento y plan de acción por parte de los líderes de procesos que reportan.

    - Seguimiento a planes de acción por el responsable de la gestión de riesgo operacional de la Oficina de Planeación que hace parte del P.A. FONTUR y elaboración de informes de la gestión de eventos de riesgo operacional.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

Para el desarrollo de estas etapas, los procedimientos definidos para el P.A. FONTUR deben atender lo dispuesto en los documentos establecidos por Fiducoldex y/o sus modificaciones y adiciones, dentro de los cuales se encuentran:

- **PR-GRI-001** - Procedimiento Gestión de eventos de Riesgo Operacional.
- **IT-GRI-022** - Instructivo de Administración Eventos de Riesgo Operacionales en Atalaya.
- **FT-GRI-009** - Reporte de evento.
- Circular Básica Contable y Financiera (Circular Externa 100 de 1995), Capítulo XXXI Sistema Integral de Administración de Riesgos (SIAR) de la Superintendencia Financiera de Colombia.

3.3.1 Directrices frente al reporte, registro y acciones de eventos de riesgo

Reporte de eventos de riesgo operacional

- Cualquier trabajador del P.A. FONTUR que tenga conocimiento de la materialización de un evento de riesgo operacional, debe informar al gestor de riesgo del proceso, para que este realice el reporte en la herramienta tecnológica definida por Fiducoldex para dicha gestión, propendiendo por reportarlo inmediatamente sea descubierto.

- Los trabajadores que estén involucrados en la ocurrencia del evento deben apoyar en las actividades para la recuperación si se presentaron pérdidas económicas y las que se requieran para el cierre y conclusión del evento.

- El trabajador que reporte el evento de riesgo operacional deberá informar de manera clara y detallada lo acontecido identificando que sucedió, porque sucedió, cual fue la causa raíz por la cual sucedió el evento de riesgo operacional. Es importante que la redacción queda registrada en tercera persona y que se garantice la integridad de la información.

En caso de tener inquietudes frente a cómo proceder para efectuar un reporte de evento de riesgo operacional, deberá comunicarse con la Dirección SARO – SARLAFT de Fiducoldex (correo electrónico: riesgo.operativo@fiducoldex.com.co), área que le brindará el acompañamiento y apoyo que sea requerido, por parte del trabajador.

Análisis de eventos y definición de Plan de Acción

- Cada vez que sea registrado un evento de riesgo operacional el responsable de la gestión de riesgo operacional de la Oficina de Planeación del P.A. FONTUR procederá a revisar y analizar la información reportada con el fin de verificar que sea clara y comprensible, y que contenga todos los elementos definidos. Así mismo, debe solicitar al líder y/o colaborador del proceso originador los ajustes o complementos al reporte que considere necesarios, los cuales deberán ser atendidos dentro del plazo estipulado.

- El Líder de proceso que originó el evento de riesgo, con el apoyo del gestor de riesgo, y con la participación de los líderes de los procesos afectados, deberá

formular el respectivo plan de acción que mitigue la causa raíz del evento materializado. El plan de acción debe comprender tanto las acciones correctivas como las de corrección, el cual debe formularse cumpliendo los tiempos establecidos por Fiducoldex. Estas acciones deben ser informadas por la Oficina de Planeación del P.A. FONTUR a la Dirección SARO-SARLAFT de Fiducoldex, en los medios definidos para tal fin y documentarse según lo estipulado en el PR-GRI -001 Procedimiento Gestión de eventos de Riesgo Operacional de Fiducoldex.

- En caso de incumplimiento en la formulación del plan de acción en el término provisto, la Oficina de Planeación del P.A. FONTUR hará el respectivo requerimiento al superior jerárquico inmediato del líder de proceso para que en el menor tiempo posible cumpla con la formulación del plan. En caso de no recibir respuesta notificará al Director(a) de la Oficina de Planeación del P.A. FONTUR, quien deberá hacer las gestiones respectivas, pondrá en conocimiento de la Dirección SARO – SARLAFT, quien a su vez informará al Comité de Riesgo Operacional de Fiducoldex, para que sea sustentado en esta instancia por el líder de proceso las razones del incumplimiento, para que esta determine las respectivas medidas.

- En caso de que se presente recurrencia en los eventos de riesgo operacional el líder del proceso deberá definir planes de acción más robustos, los cuales si son originados por el mismo trabajador deben comprender llamados de atención escritos, con copia a la hoja de vida.

Seguimiento a los planes de acción frente a eventos de riesgo operacional materializados

- Los líderes de proceso con el apoyo de los gestores de riesgo deben hacer seguimiento a la ejecución de los planes de acción definidos para mitigar o prevenir la ocurrencia de nuevos eventos de riesgo, hasta el cierre o conclusión del evento.

- La modificación de los planes de acción formulados para mitigar los eventos de riesgo materializados, respecto a las fechas de implementación de las actividades, solo puede solicitarse por los responsables de estos, previo a su vencimiento con la respectiva justificación razonable dando cumplimiento a los lineamientos establecidos por Fiducoldex. La Oficina de Planeación del P.A. FONTUR, escalará la solicitud a la Dirección SARO – SARLAFT y esta a su vez la presentará al Comité de Riesgo Operacional de Fiducoldex, quien podrá autorizar modificaciones a las actividades o con plazos superiores cuando se presenten variaciones en el alcance, responsables de las actividades o necesidades del P.A. FONTUR. Ninguna modificación a los planes podrá ser efectuada sin que sea autorizada por el Comité de Riesgo Operacional.

- Si como resultado de la materialización de un evento de riesgo, el líder del proceso, la Oficina de Planeación del P.A. FONTUR o la Dirección SARO – SARLAFT evidencian la necesidad de complementar la matriz de riesgo del P.A. FONTUR, se deberá informar a la Oficina de Planeación del P.A. FONTUR para coordinar con este las mesas de trabajo para la documentación del riesgo, su valoración, así

como para la identificación de los controles, actividades que no sustituyen las acciones que deban adoptarse de manera preventiva como parte del plan de acción.

Controversias en el reporte de eventos de riesgo

- Las situaciones de controversia que surjan con relación al registro de eventos de riesgo operacional deben ser canalizadas por los líderes de proceso a la Dirección SARO-SARLAFT de la Gerencia de Riesgos, a través de la Oficina de Planeación del P.A. FONTUR. Dicha Oficina tiene la responsabilidad de analizar las mismas respecto al cumplimiento de las condiciones, requisitos y características de un evento de riesgo operacional según lo estipulado en los instructivos definidos por Fiducoldex; convocar al líder del proceso que reporta y líder (es) del(los) proceso(s) involucrado(s), a la Oficina de Planeación del P.A. FONTUR y con Gerencia de Riesgos determinar si la situación reportada corresponde a un evento de RO, lo cual informará a los líderes de proceso para la definición por su parte de los planes de acción.

- El Comité de Riesgo Operacional de Fiducoldex es la instancia encargada de analizar y decidir sobre las controversias y conflictos de interés que se presenten en el proceso de implementación y recolección de información de las diferentes etapas de la gestión de riesgo operacional, especialmente en cuanto al registro de eventos de riesgo operacional.

Clasificación de eventos de riesgo operacional

Todos los eventos de riesgo operacional registrados en la herramienta de reporte y base de datos se clasifican de acuerdo con su tipo de pérdida definida por la Superintendencia Financiera de Colombia:

A. Generan pérdidas y afectan el estado de resultados del Patrimonio Autónomo.
B. No generan pérdidas y por lo tanto no afectan el estado de resultados del Patrimonio Autónomo.

Las pérdidas tipo A causadas por un evento de riesgo operacional común o por varios eventos de riesgo operacional relacionados a lo largo del tiempo corresponde a las que se contabilizan a las cuentas de riesgo operativo y generaron una pérdida económica que afecta el estado de resultados de la sociedad fiduciaria como administradora del P.A. FONTUR.

3.4 Etapas para la Gestión de Riesgo Operacional

Fiducoldex tiene alineadas las metodologías para el desarrollo de las etapas de Gestión de Riesgo Operacional con las establecidas por Bancóldex, su casa matriz y se encuentran integradas al Manual del Sistema Integral de Administración de Riesgos. En este sentido, estas metodologías también deben darse cumplimiento en los patrimonios autónomos administrados, entre los cuales se encuentra el P.A. FONTUR. De esta manera, cualquier modificación en las mismas debe surtir la revisión por parte de la

Dirección SARO-SARLAFT, la Gerencia de Riesgos y el Comité de Administración de Riesgos y la aprobación de la Junta Directiva de Fiducoldex.

A continuación, se describen los procedimientos y metodologías que deben ser aplicadas para la Gestión de Riesgo Operacional en las diferentes etapas, con alcance a los procesos del P.A. FONTUR:

3.4.1 Identificación

En esta etapa se determinan los riesgos (actuales y potenciales) inherentes a las actividades que desarrolla o planea desarrollar el P.A. FONTUR. Esta etapa debe realizarse con periodicidad anual y previamente en el caso de la implementación de nuevas actividades o modificación sobre las que están en operación y/o cambios en el plan de negocio.

A continuación, se establecen los lineamientos y procedimientos para la identificación de riesgos en los procesos del P.A. FONTUR:

- La identificación de los riesgos se fundamenta en el modelo de operación por procesos del P.A. FONTUR. De esta manera, la identificación de los riesgos operacionales se debe realizar considerando las caracterizaciones de los procesos (objetivo, alcance, actividades y salidas o productos resultantes del proceso) y sus procedimientos y documentos complementarios que se encuentran publicados en el Sistema de Gestión de Calidad del P.A. FONTUR. Lo anterior con el fin de considerar sólo aquellos riesgos que realmente le atañen y se encuentran dentro del alcance del proceso.

- Esta etapa debe desarrollarse con la participación de los líderes de proceso y de sus gestores de riesgo, coordinadas y acompañadas por el responsable de la Oficina de Planeación del P.A. FONTUR.

- En la etapa de identificación de riesgos se deben documentar tanto los riesgos operacionales, potenciales como los ocurridos, en cada uno de los procesos que conforman el P.A. FONTUR.

- En la identificación de riesgos se deben tener en consideración los eventos de riesgo materializados que fueron originados por los siguientes factores de riesgo: recurso humano, procesos, tecnología, infraestructura y factores externos. En este sentido, cuando previamente no se hubieren identificado los riesgos, se debe complementar la matriz de riesgos incluyendo los nuevos riesgos materializados.

- La identificación de riesgos debe realizarse de manera previa a la implementación o modificación de cualquier proceso del P.A. FONTUR. De esta manera, el líder del proceso y/o el gestor de riesgos deben validar, la existencia de riesgos operacionales asociados y los mecanismos de control a establecer para mitigar los mismos.

- Cualquier proyecto o desarrollo tecnológico que genere nuevas implementaciones y cambios en los aplicativos que se ejecutan para el desarrollo del P.A. FONTUR,

requerirá que se valide previamente la existencia de riesgos operacionales con el objetivo de que sean identificados previo a la salida de producción de los desarrollos o cambios a ejecutar. (Esta identificación aplica tanto para desarrollos internos como desarrollos que se realicen por parte de terceros contratados).

Los riesgos operacionales que sean identificados de los procesos del P.A. FONTUR, deben clasificarse acorde a la categorías y subcategorías definidas por la Superintendencia Financiera de Colombia.

3.4.1.1 Identificación de riesgo operacional en la formulación de programas/proyectos

Para los programas/proyectos formulados, viabilizados y aprobados por el Comité Interno de Proyectos y/o Comité Directivo, se debe adelantar la identificación de riesgos, la cual considere como mínimo los aspectos críticos a nivel técnico, administrativo y presupuestal del proyecto a desarrollar. Como resultado debe generarse la matriz de riesgos que contemple los mecanismos de control para mitigar los riesgos y gestionarse su implementación. Si en la formulación del proyecto o en la ejecución del negocio jurídico celebrado para el desarrollo de este se presentan modificaciones deberá efectuarse la actualización de la matriz de riesgos, identificando los riesgos operacionales del cambio a realizar, actividad que estará a cargo del supervisor del proyecto o líder del área donde se ejecutará el mismo.

En esta etapa se deben identificar tanto los riesgos de Lavado de Activos y Financiación del Terrorismo, Seguridad de la Información, de Fraude y Corrupción, como los Legales y los relacionados con obligaciones contractuales con las partes intervinientes.

Con relación a los negocios jurídicos en la etapa de identificación se deben analizar, considerar y documentar los riesgos desde la planeación hasta la terminación del plazo contractual, incluyendo los relacionados con la liquidación del contrato, el vencimiento de las garantías de calidad y/o la disposición final del bien contratado. Así mismo, acogiendo las recomendaciones de Colombia Compra Eficiente, se deben considerar los siguientes posibles eventos:

- Los que impidan la adjudicación y firma del contrato como resultado del Proceso de Contratación.
- Los que alteren la ejecución del contrato
- El equilibrio económico del contrato
- La eficacia del Proceso de Contratación, es decir, que el contratante pueda satisfacer la necesidad que motivó el Proceso de Contratación.
- La reputación y legitimidad del encargado de prestar el bien o servicio.

3.4.2 Medición

Metodología para la medición de los riesgos operacionales de los procesos del P.A. FONTUR.

La metodología para la evaluación de los riesgos operacionales identificados de las actividades que conforman los procesos del P.A. FONTUR, debe atender los siguientes lineamientos y metodología establecida por Fiducoldex:

- La medición de los riesgos se realizará de manera semicuantitativa, teniendo en cuenta las escalas de calificación de probabilidad e impacto definidas por Fiducoldex en el Manual del Sistema Integral de Administración de Riesgos (SIAR).

- En aquellos casos en los cuales se pueda construir estadísticas sobre procesos o actividades, estas serán tenidas en cuenta para la definición de cálculos en probabilidad, los cuales deben ser previamente compartidos a la Dirección SARO-SARLAFT de Fiducoldex para su revisión y aprobación.

- Las escalas de calificación de impacto, probabilidad y severidad serán aprobadas por la Junta Directiva de Fiducoldex, previa evaluación del Comité de Administración de Riesgos. Cuando se presenten cambios o ajustes en las mismas, la Dirección SARO-SARLAFT procederá a informarle a la Oficina de Planeación del P.A. FONTUR para que se dé aplicación a las mismas.

- Para la evaluación de los riesgos operacionales se utiliza una matriz de riesgo en una escala 5x5, que contemple los niveles definidos por Fiducoldex para evaluar la probabilidad e impacto de los riesgos identificados.

- Durante la medición de los riesgos se deben asociar los niveles de probabilidad e impacto a cada riesgo identificado, sin tener en cuenta los controles. Esta medición se conoce como calificación inherente, lo cual se efectúa con el fin de conocer el nivel de mayor exposición de los riesgos.

- El horizonte de tiempo considerado para la determinación de la probabilidad de ocurrencia es de un año, y la medición del impacto se hará en función de la evaluación de la consecuencia cuantitativa (pérdida económica) y/o cualitativa (reputacional) según los niveles establecidos en la tabla de impacto de Fiducoldex.

- En los casos en que un riesgo contemple simultáneamente varios impactos, el profesional debe escoger la calificación de mayor nivel. Sin embargo, en la descripción del riesgo es necesario nombrar los diferentes impactos a los que se encuentra expuesto el riesgo.

- La descripción del incumplimiento regulatorio se encuentra involucrada en el impacto reputacional y su materialización se ve implícita en las pérdidas económicas y/o reputacionales.

- Una vez se realice la medición de la probabilidad y el impacto para los riesgos identificados en cada uno de los procesos, se debe consolidar la información, determinando el perfil de Riesgo Inherente por procesos y del P.A. FONTUR.

3.4.2.1 Medición de los riesgos operacionales en la formulación de proyectos.

Para los proyectos formulados, viabilizados y aprobados por el comité interno y/o comité directivo, se deberá efectuar la medición de los riesgos identificados, así mismo cuando hay modificaciones a los mismos, teniendo en cuenta la probabilidad y el impacto conforme a la metodología que se defina la Dirección SARO-SARLAFT y la Oficina de Planeación del P.A. FONTUR, asociando los niveles de probabilidad e impacto de cada riesgo identificado sin tener en cuenta los controles (valoración inherente), contemplando en los casos en que se presenten varios impactos la calificación de mayor nivel. Una vez efectuada la medición de los riesgos se deberá efectuar la medición consolidada del programa/proyecto.

Para aquellos riesgos en los que el nivel de severidad sea críticos o altos, se deberá definir el respectivo tratamiento para revisión y aprobación de las instancias respectivas del P.A. FONTUR. Estos tratamientos deberán ser informados previamente a la Oficina de Planeación del P.A. FONTUR.

3.4.3 Control

En esta etapa se deben implementar las medidas que permitan reducir la probabilidad y recurrencia del impacto de los riesgos operacionales a los que puede estar expuesto el P.A. FONTUR, para lo cual se deben cumplir los siguientes lineamientos frente al diseño e implementación de los controles:

- Estas medidas o controles deben estar debidamente documentadas y ser conocidas por todos los líderes de proceso y sus áreas de trabajo. Así mismo, deben ser difundidas al interior del P.A. FONTUR.

- La Oficina de Planeación del P.A. FONTUR encargada de la Gestión de Calidad debe velar por que se realice una adecuada documentación de los controles que tengan implementados los procesos, la revisión, creación o actualización de manuales, procedimientos y demás documentos que hagan parte del Sistema de Gestión de Calidad del P.A. FONTUR.

- Los líderes de los procesos del P.A. FONTUR tienen la responsabilidad de capacitar e instruir a los miembros de su equipo de trabajo sobre la aplicación de los controles nuevos o existentes.

- Se debe realizar por parte de los líderes de proceso la identificación de los controles preventivos o correctivos que se encuentren implementados en sus procesos, con el propósito de valorar la protección que estos ofrecen y determinar la necesidad de implementar nuevos controles o modificar los existentes.

- En el diseño de nuevos controles se debe realizar el análisis de los costos y beneficios de su implementación.

- En caso de que la implementación de un nuevo control conlleve la destinación de recursos, el líder de proceso que realiza la propuesta debe adelantar las gestiones para solicitar la asignación de los recursos del P.A. FONTUR.

- Fundamentado en el principio de autocontrol, la responsabilidad de la implementación y ejecución de los controles es de todos los trabajadores del P.A. FONTUR. En este sentido, cada trabajador, independientemente de su nivel jerárquico dentro del P.A. FONTUR debe desarrollar y evaluar su trabajo, detectar desviaciones y efectuar correctivos, de tal manera que la ejecución de los procesos, actividades y tareas bajo su responsabilidad procuren el logro de los objetivos institucionales.

- La Oficina de Auditoría Interna del P.A. FONTUR, en desarrollo de los procesos de auditoría interna debe verificar la implementación, cumplimiento y eficacia de los controles que se definan para los procesos que conforman el P.A. FONTUR. El resultado de estas evaluaciones debe ser remitido a la Gerencia de Riesgos de Fiducoldex.

- La metodología para la valoración de los controles que se identifican para prevenir o mitigar la materialización de un riesgo operacional de un proceso del P.A. FONTUR, corresponderá a la definida por Fiducoldex la cual se encuentra documentada en el PT-GRI-005 Protocolo Metodología de Evaluación de Riesgo Operacional, que hace parte del Sistema Integral de Administración de Riesgos (SIAR).

- Se debe vigilar que se implementen las medidas de control sobre cada uno de los riesgos operacionales identificados y se establezcan las medidas que permitan asegurar la continuidad del negocio.

3.4.3.1 Calificación de la eficiencia del diseño de los controles

En la etapa de control se debe validar que se han tomado las medidas necesarias para controlar el riesgo inherente, con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso del riesgo evaluado se materialice.

La descripción y documentación de los controles se debe realizar atendiendo los criterios establecidos en la metodología definida por Fiducoldex, dentro de la cual también se encuentra definida la calificación de la eficacia de los controles. Estas actividades se adelantarán con los gestores de riesgo, y deben contar con la aprobación de los líderes de proceso.

Otra fuente para validar la efectividad de los controles será el registro de eventos de riesgo operacional y las recomendaciones, instrucciones, hallazgos, oportunidades de mejora y demás que sean informadas por entes de vigilancia y control, así como la Dirección de Auditoría Interna del P.A. FONTUR.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

3.4.3.2 Determinación del Nivel de Riesgo Residual

Una vez realizada la calificación de la eficacia de los controles diseñados para mitigar cada uno de los riesgos de los procesos que conforman el P.A. FONTUR, se debe determinar el nivel de reducción que estos tienen respecto a su probabilidad o impacto, a fin de determinar el perfil de riesgo residual, conforme a la metodología establecida por Fiducoldex. Esta actividad se realizará por el responsable de la gestión de riesgo operacional de la Oficina de Planeación del P.A. FONTUR, quien debe remitir el perfil de riesgo residual para aprobación por parte de los líderes de los procesos que conforman el P.A. FONTUR.

Conforme al nivel de severidad que se obtenga en los procesos, se definirán las acciones a seguir y la instancia responsable de definir estas acciones, de acuerdo con la siguiente tabla:

Tabla 1. Niveles de severidad

Nivel de severidad	Acción por seguir:
Crítica	El Líder de proceso deberá definir un tratamiento con la validación del Gerente General del P.A. FONTUR, el cual debe ser presentado a la Junta Directiva de Fiducoldex para su aprobación, con previo análisis del Comité de Administración de Riesgos.
Alta	El Líder de proceso deberá definir un tratamiento, el cual debe ser presentado y aprobado por el Comité de Riesgo operacional, con previa validación del Gerente General del P.A. FONTUR.
Media	El Líder de proceso debe definir el tratamiento del riesgo y las acciones necesarias para administrarlo.
Baja	Se administra con procedimientos rutinarios. El Líder de proceso define si se requiere ajustar o implementar controles adicionales.

Fuente: Gerencia de Riesgos Fiducoldex

La consolidación del perfil de riesgo del P.A. FONTUR a nivel inherente y residual se realizará por la Oficina de Planeación del P.A. FONTUR y sus resultados los debe remitir a la Dirección SARO-SARLAFT para su revisión y presentación al Comité de Riesgo Operacional de Fiducoldex. Posteriormente se entregarán al Ministerio de Comercio, Industria y Turismo.

3.4.3.3 Tratamiento de riesgos

A partir del nivel de riesgo residual consolidado del P.A. FONTUR, se debe realizar la evaluación de este frente al nivel de riesgo admisible aprobado por la Junta Directiva de Fiducoldex, con el propósito de establecer las medidas de tratamiento que se requieran, entre las que se puede encontrar reducir o trasferir los riesgos. Para esto se debe tener en consideración los siguientes lineamientos:

- El nivel de severidad residual de riesgo admisible para FIDUCOLDEX S.A. aprobado por la Junta Directiva es:" Media". Cuando el nivel de riesgo residual supere el nivel admisible, los líderes de los procesos del P.A. FONTUR con el apoyo de los gestores de riesgo establecerán, los planes de tratamiento para mitigar los riesgos.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

- En ningún caso el líder de proceso del P.A. FONTUR podrá asumir riesgos que se encuentren ubicados en la zona de severidad "Alta" o "Crítica", para los cuales deberá formular e implementar planes de tratamiento para mitigarlos y escalarlos a las instancias correspondiente.

- En la formulación de planes de tratamiento se debe realizar el análisis de los costos (si conlleva) y beneficios de su implementación.

- En caso de que la implementación de un plan de tratamiento conlleve la destinación de recursos por parte del P.A. FONTUR, el líder de proceso que realiza la propuesta debe validar el mismo, con su superior jerárquico y adelantar las gestiones correspondientes para la asignación del presupuesto requerido.

- En caso de que la propuesta de tratamiento corresponda a una transferencia de riesgos mediante la contratación de un seguro, esta debe ser presentada a las instancias de aprobación internas establecidas del P.A. FONTUR para su análisis y validación de disponibilidad de recursos.

- La modificación de planes de tratamiento solo puede solicitarse por los responsables de los mismos con una justificación razonable a la Oficina de Planeación del P.A. FONTUR quien a su vez informará a la Dirección SARO – SARLAFT dentro de los tiempos establecidos en cumplimiento a la directrices impartidas por Fiducoldex para la gestión de riesgos, con el fin de que sea presentada la solicitud al Comité de Riesgo Operacional y/o instancias internas establecidas, quienes podrán autorizar las modificaciones a las actividades o con plazos superiores cuando se presenten variaciones en el alcance, responsables de las actividades o necesidades del P.A. FONTUR.

3.4.3.4 Identificación de controles y formulación de planes de tratamiento en la formulación de programas/proyectos.

Para los programas/proyectos formulados, viabilizados y aprobados por el Comité Interno de Proyectos y/o Comité Directivo, se debe adelantar la identificación de los controles que contribuyan a mitigar los riesgos del programa/proyecto, los cuales se midieron previamente a nivel inherente (sin controles). Para la definición de los controles se deben aplicar los lineamientos establecidos en el numeral 3.2.3. Posteriormente se debe generar el nivel de riesgo residual.

Para aquellos riesgos en los que el nivel de severidad residual sea crítico o alto, se deberá definir el respectivo tratamiento por el responsable del proyecto, para revisión y aprobación de las instancias respectivas del P.A. FONTUR. Estos tratamientos deberán ser informados a la Oficina de Planeación del P.A. FONTUR, quien efectuará el respectivo seguimiento.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

Tabla 2. Niveles de severidad

Nivel de severidad	Acción por seguir:
Crítica	El Líder de proceso deberá definir un tratamiento con la validación del Gerente General del P.A. FONTUR, el cual debe ser presentado a la Junta Directiva de Fiducoldex para su aprobación, con previo análisis del Comité de Administración de Riesgos.
Alta	El Líder de proceso deberá definir un tratamiento, el cual debe ser presentado y aprobado por el Comité de Riesgo operacional, con previa validación del Gerente General del P.A. FONTUR.
Media	El Líder de proceso debe definir el tratamiento del riesgo y las acciones necesarias para administrarlo.
Baja	Se administra con procedimientos rutinarios. El Líder de proceso define si se requiere ajustar o implementar controles adicionales.

Fuente: Gerencia de Riesgos Fiducoldex

El plan de tratamiento debe incluir como mínimo: acciones a ejecutar, responsables, fechas de inicio y fecha de terminación, recursos requeridos, soportes o evidencias. Estas medidas a implementar deben permitir reducir la probabilidad de ocurrencia y el impacto de los riesgos operacionales identificados. Medidas que deben ser difundidas para conocimiento de todos los partícipes del tratamiento.

Para la implementación o ejecución del plan de tratamiento o controles se debe asegurar que se cuente con los recursos necesarios para el cumplimiento oportuno de las acciones, para lo cual el líder del proyecto debe realizar la validación para la asignación de los mismos con su superior inmediato, quien a su vez debe escalar la presentación y aprobación a la instancia respectiva.

Así mismo, es importante es hacer una correcta asignación y tratamiento de los riesgos identificados en los procesos de contratación, teniendo en cuenta los lineamientos definidos en el Manual para la identificación y cobertura del riesgo en los procesos de contratación de Colombia Compra Eficiente.

3.4.4 Monitoreo

En la etapa de monitoreo se busca verificar y hacer seguimiento a la gestión del riesgo operacional dentro de la cual se confirmará la efectividad del cumplimiento frente a los lineamientos, procedimientos y metodologías definidos, así como hacer seguimiento a los perfiles de riesgo y a las exposiciones a pérdidas del P.A. FONTUR. En esta etapa se adelantará:

- La verificación del funcionamiento de los controles mediante monitoreos muestrales, de forma semestral con el fin de validar la eficacia y efectividad en la ejecución de los controles establecidos, la cual permitirá retroalimentar y actualizar la valoración de los controles y del perfil de riesgo residual. Estos monitoreos serán adelantados por la Oficina de Planeación del P.A. FONTUR quien a su vez remitirá a través del director (a) de la Oficina el respectivo informe a la Gerencia General del P.A. FONTUR y a la Dirección SARO – SARLAFT quien presentará lo correspondiente al Comité de Riesgo Operacional de Fiducoldex. En los casos que se requiera se invitará al director(a) de la Oficina de Planeación del P.A. FONTUR a explicar estos resultados.

- El seguimiento periódico para monitorear que los riesgos residuales se encuentren en los niveles de aceptación establecidos y aprobados por la Junta Directiva.

- El seguimiento al mapa de riesgo operacional realizado por los líderes o gestores de riesgo de los procesos, quienes deberán informar cualquier modificación o inclusión que se requiera de nuevos riesgos y controles sobre los procesos a su cargo para proceder con la actualización de la matriz de riesgos.

- El seguimiento a los eventos de riesgo operacional que se presentaron para el P.A. FONTUR, considerando que cada vez que se materialice un riesgo operacional conforme a la metodología establecida por Fiducoldex, se deberá afectar la calificación del riesgo dentro de la matriz de riesgo operacional y el mapa de calor.

- El análisis de los resultados de las auditorías que adelante la Dirección de Auditoria del P.A. FONTUR, así como de los informes proferidos por la Contraloría General de la República (CGR), los cuales podrán fundamentar una modificación a la valoración de los controles. Así mismo, considerando que los hallazgos de la CGR repercuten en el fenecimiento de la cuenta fiscal del Ministerio de Comercio, Industria y turismo, se deberá asegurar que en el monitoreo de controles se priorice la verificación de las medidas establecidas en el Patrimonio para controlar la ejecución presupuestal y contractual de los recursos públicos transferidos al P.A. FONTUR.

3.4.4.1 Monitoreo de controles en la formulación de programas/proyectos

Respecto a los riesgos identificados para los programas/proyectos formulados, viabilizados y aprobados por el Comité Interno de Proyectos y/o Comité Directivo se debe efectuar un monitoreo periódico, a través de una verificación de la efectividad de los controles y el seguimiento a los planes de tratamiento definidos, con el fin de evaluar o establecer si es necesario ajustarlos o robustecerlos, de acuerdo con las circunstancias actuales del proyecto, así como actualizar la valoración de los riesgos teniendo en cuenta los eventos de riesgo operacional materializados.

El monitoreo puede ser efectuado mediante seguimientos y revisión de muestreos aleatorios de controles para lo cual se podrá solicitar a los líderes de proyecto o supervisores los soportes de su ejecución, o adelantar verificaciones en sitio.

3.5 Divulgación y Capacitación

La Oficina de Planeación del P.A. FONTUR será la responsable de adelantar las capacitaciones, sensibilizaciones y socializaciones requeridas para la gestión del riesgo operacional en el P.A. FONTUR, en coordinación con la Dirección SARO-SARLAFT y atendiendo las directrices que para este efecto le emita la Gerencia de Riesgos de la Fiduciaria. Estas actividades atienden la normatividad vigente y tienen por objeto divulgar los lineamientos, procedimientos, metodologías, planes de trabajo y resultados de la gestión de riesgo operacional, por lo cual se deberá promover por la Dirección de

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

Talento Humano y la Oficina de Planeación la asistencia de todos los trabajadores del P.A. FONTUR independiente de su nivel jerárquico. Así mismo, se deben generar y conservar los reportes de cumplimiento de estas actividades, los cuales deberán ser entregados a la Dirección SARO-SARLAFT de la Fiduciaria, los cuales estarán a disposición del Ministerio de Comercio, Industria y Turismo y de los entes de vigilancia y control que se requieran.

3.6 Reportes y presentación de informes

La Oficina de Planeación del P.A. FONTUR, quien tendrá a cargo la gestión de riesgo operacional preparará y remitirá a la Dirección SARO - SARLAFT de Fiducoldex y al Ministerio de Comercio, Industria y Turismo los siguientes reportes:

- Reporte de eventos de riesgo operacional del P.A. FONTUR. el cual detalla el número y valor de eventos materializados, clasificación de eventos (tipo A y tipo B), estado de formulación y cumplimiento de planes de acción para mitigación de ERO y solicitudes de modificación de los mismos presentadas (Trimestral).
- Estado de avance del cronograma para la actualización de las matrices de riesgo operacional de los procesos del P.A. FONTUR (Trimestral).
- Informe de Monitoreo de controles a los procesos del P.A. FONTUR (Semestral).
- El reporte de la actualización del perfil de riesgo operacional inherente y residual de los procesos del P.A. FONTUR (Anual).
- Reporte de cumplimiento de actividades de capacitación, sensibilización y socialización de la gestión de riesgo operacional, incluyendo el porcentaje de cobertura en los trabajadores (Anual).

No obstante, la Dirección SARO-SARLAFT de Fiducoldex podrá requerir en cualquier momento los reportes y/o soportes a lugar de la gestión de riesgo operacional que se ejecute en el Patrimonio Autónomo FONTUR con el fin de atender los requerimientos de los entes de vigilancia y control, por lo cual la Oficina de Planeación del P.A. FONTUR debe atender de forma oportuna las solicitudes y asegurar la calidad de la información entregada.

3.7 Indicadores

Como parte de la Gestión de Riesgo Operacional del P.A. FONTUR fueron establecidos los siguientes indicadores:

Tabla 3. Indicadores establecidos para la Gestión de Riesgo Operacional

Indicador	Descripción	Fórmula	Meta anual
Efectividad en la ejecución de los controles	Verifica la efectividad en la ejecución de los controles. **Control efectivo:** corresponde a los controles que se ejecutan acorde a las características dentro de su diseño. **Periodicidad:** Semestral.	(Controles efectivos/Total de controles de la muestra a verificar) *100	90%
Cumplimiento en la actualización de las matrices de riesgo operacional	Corresponde al cumplimiento en la actualización de las matrices de riesgo operacional por proceso acorde a la metodología aprobada. **Periodicidad:** Trimestral.	(Matrices de riesgos actualizadas/matrices de riesgo programadas al corte)	100%

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

Indicador	Descripción	Fórmula	Meta anual
Ejecución de los planes de acción	Corresponde a la medición de la ejecución de los planes de acción resultado de la materialización de eventos de riesgo operacional. **Periodicidad:** Trimestral.	(Actividades de los planes de acción ejecutados oportunamente/Total de actividades programas a cumplir al corte) *100	100%
Cumplimiento en el reporte de eventos de riesgo	Corresponde al cumplimiento en el reporte de los eventos de riesgo cuando se presentan hallazgos o se materialice un riesgo operacional. **Periodicidad:** Trimestral.	(Eventos de riesgo registrados/Eventos de riesgo informados) *100	100%

3.8 Documentación relacionada

La Gestión de Riesgo Operacional del P.A. FONTUR se soportará en la siguiente documentación que hace parte del Sistema Integral de Administración de Riesgos de Fiducoldex y/o en los documentos que los sustituyan o complementen:

- **PT-GRI -004** - Protocolo de metodología Autoevaluación de Riesgos y Controles.
- **PT-GRI-005** - Protocolo Metodología de Evaluación de Riesgo Operacional.
- **PT-GRI -006** - Perfil de Riesgo operacional.
- **PR-GRI -001** - Procedimiento Gestión de eventos de Riesgo Operacional.
- **IT-GRI-022** - Instructivo de Administración Eventos de Riesgo Operacionales en Atalaya.
- **FT-GRI-009** - Reporte de eventos.

4 CAPÍTULO IV – GESTIÓN DEL RIESGO DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO (LAFT)

4.1 Lineamientos y procedimientos para la gestión del Riesgo LAFT

- En el P.A. FONTUR se debe dar cumplimiento a las políticas, procedimientos, metodologías, modelos, funciones y responsabilidades establecidos por Fiducoldex, en el Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo, implementado en su carácter de entidad vigilada y en cumplimiento de lo definido en la Parte I – Título IV – Capítulo IV de la Circular Básica Jurídica, emitida por la Superintendencia Financiera de Colombia.

- Este sistema, tiene por objetivo de reducir la posibilidad que Fiducoldex y sus patrimonios administrados puedan ser un instrumento para el ocultamiento o legalización de bienes producto de conductas delictivas o de aquellos que estuvieren asociados a la materialización de ilícitos, también tiene por objeto mitigar el riesgo de pérdida o daño que se puede obtener con los riesgos asociados (Legal, reputacional, de contagio y operacional).

- Para Fiducoldex es imperativo anteponer la observancia de los principios éticos y el cumplimiento de las políticas y los procedimientos SARLAFT al logro de las metas comerciales. Por lo anterior, no se podrá iniciar en el P.A. FONTUR, ningún tipo de relación contractual o legal, si no se ha cumplido con el proceso de vinculación establecido, dando adecuado cumplimiento al conocimiento del cliente. Lo anterior es extensivo para trabajadores y proveedores.

- Para mitigar la exposición a riesgos asociados a LA/FT, previo a contraer cualquier tipo de vínculo con un cliente o contraparte, se deben realizar las consultas y cruces de información en la herramienta del proveedor de listas de la Fiduciaria. Así mismo, también deben consultar a los terceros relacionados al cliente o contraparte tales como: Accionistas, Representantes Legales, Revisores Fiscales, miembros de Junta Directiva, Contadores, Oficiales de Cumplimiento, Administradores, entre otros, y los relacionados en la información con la que se cuente.

- El proceso de conocimiento del cliente, el cual es extensivo a los proveedores y terceros no clientes, acorde con la normatividad vigente, así como la verificación en listas podrá ser adelantado por la Dirección de Servicios Administrativos del P.A. FONTUR, una vez se haya definido e implementado el respectivo procedimiento. En este caso, esta área será responsable de ejecutar el proceso de verificación documental SARLAFT de todos aquellos terceros que pretendan establecer una relación comercial o contractual con el P.A. FONTUR. Así mismo será responsable de comunicar e informar oportunamente a la Dirección SARO-SARLAFT de Fiducoldex los alertamientos presentados en el desarrollo de este proceso y en la actualización periódica de la información de los clientes; así como los intentos de vinculación que se presenten. La Dirección SARO-SARLAFT adelantará los procesos de monitoreo para asegurar que se dé cumplimiento al procedimiento, lineamientos y controles establecidos.

- En cumplimiento de los requerimientos del SARLAFT impartidos por la Superintendencia Financiera de Colombia, Fiducoldex estableció una metodología de evaluación con el fin de determinar la posibilidad de ocurrencia del riesgo de LA/FT frente a cada uno de los factores de riesgo (cliente, producto, canal y jurisdicción). Por lo tanto, la Fiduciaria y sus negocios administrados deberán abstenerse de vincular clientes o contrapartes para operaciones directas cuya actividad económica principal o secundaria (ingresos representativos dentro del total) sea valorada como nivel de riesgo de LA/FT "Muy alto".

- Adicionalmente, no se podrá continuar con el proceso que se esté llevando con el cliente o contraparte si la jurisdicción internacional corresponde a un nivel de riesgo LA/FT "Muy alto".

- En el P.A. FONTUR se deben incorporar en los contratos e instrumentos que celebre, cláusulas de prevención de riesgos de LA/FT, que faculten la finalización de los contratos u ordenes de servicio cuando el cliente, contraparte y terceros o alguna de sus partes relacionadas están registradas en alguna de las listas vinculantes por parte de las autoridades competentes.

- Los documentos relacionados a la Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo deberán mantenerse actualizados y publicados en el aplicativo del Sistema de Gestión de Calidad disponible, para consulta y conocimiento de los empleados de la Fiduciaria y del P.A. FONTUR.

4.2 Alcance

El P.A. FONTUR administrado por Fiducoldex debe aplicar el SARLAFT en todas las operaciones que realice, ya sean en moneda nacional o extranjera e indistintamente el tipo de transacciones que se lleven a cabo. Así mismo, las políticas y directrices establecidas en el presente documento aplican para la vinculación de personas naturales y jurídicas en el marco de los negocios jurídicos que adelante el P.A. FONTUR local e internacionalmente, incluyendo sus beneficiarios finales y otros vinculados de acuerdo con los procedimientos definidos en le SARLAFT.

4.3 Etapas para la gestión del riesgo LAFT

4.3.1 Identificación

La identificación de los riesgos LAFT y sus respectivas causas se desarrolla en forma paralela a la revisión de los riesgos operacionales de los procesos ejecutados en el P.A. FONTUR, con la finalidad de identificar aquellas situaciones que generen exposición a la materialización del riesgo LA/FT. Este ejercicio debe realizarse mínimo una vez en el año y estará liderado por la Dirección SARO-SARLAFT de la Fiduciaria, con la participación de los líderes de proceso del P.A. FONTUR, para lo cual, coordinará con la Oficina de Planeación del P.A. FONTUR, su participación en las mesas de trabajo y será responsable de consolidar y administrar esta información.

Estas causas serán incluidas en la matriz de riesgo metodológica de SARLAFT, administrada por la Dirección SARO – SARLAFT de la Fiduciaria.

4.3.2 Medición

La medición del Riesgo LAFT será liderada por la Dirección SARO-SARLAFT con la participación de los lideres de proceso del P.A. FONTUR, conforme a la metodología establecida por Fiducoldex, la cual comprende las tablas de clasificación de impacto y probabilidad aprobadas por la Junta Directiva. Para la etapa de medición, se deben considerar los lineamientos establecidos en el numeral 3.4.2.

4.3.3 Control

En esta etapa se definen e implementan los mecanismos que permitan mitigar la probabilidad y el impacto a las causas LA/FT identificadas. Dentro de los procesos del P.A. FONTUR, es importante garantizar que se cumplan con los siguientes lineamientos:

- Los controles deben ser definidos por los líderes de proceso, siguiendo las recomendaciones entregadas por la Dirección SARO – SARLAFT en cuanto a su estructuración y características.

- Los líderes deben garantizar la implementación, documentación y ejecución de los mecanismos de control en sus procesos y notificar sus posibles desviaciones.

- Los líderes de los procesos del P.A. FONTUR tienen la responsabilidad de capacitar e instruir a los miembros de su equipo de trabajo sobre la aplicación de los controles nuevos o existentes.

- Se debe garantizar que los controles implementados mitiguen el riesgo inherente identificado previamente.

- La metodología para la valoración de los controles definidos para cada causa asociada con el riesgo LAFT del P.A. FONTUR, tanto en su diseño como en su aplicación, corresponderá a la definida por Fiducoldex la cual se encuentra documentada en el PT-GRI -007 Protocolo Metodológico para gestionar los Riesgos de LAFT.

Una vez realizada la calificación de la eficacia de los controles diseñados para mitigar cada una de las causas asociadas con el riesgo LAFT, se debe determinar el nivel de reducción que estos tienen respecto a su probabilidad o impacto, a fin de determinar la calificación residual del riesgo, conforme a la metodología establecida por Fiducoldex. Esta actividad estará a cargo por la Dirección SARO-SARLAFT, quien a su vez realizará la consolidación de la matriz de riesgo LAFT y administrará la respectiva información.

Realizada la actualización de las causas y controles asociadas al riesgo LAFT, la Dirección SARO-SARLAFT remitirá esta información, para validación por parte de los líderes del proceso del P.A. FONTUR, para su posterior consolidación de la matriz metodológica SARLAFT, cuya aprobación la realizará el Oficial de cumplimiento de Fiducoldex. La

actualización de la matriz de riesgos LAFT de Fiducoldex, será presentada por el Oficial de Cumplimiento al CAR y la Junta Directiva, en el marco de los informes trimestrales.

Tratamiento de Riesgos LAFT y sus Causas

A partir del nivel de riesgo residual de las causas asociadas con el riesgo LAFT identificadas en el P.A. FONTUR, se debe realizar la evaluación de este frente al nivel de riesgo admisible aprobado por la Junta Directiva de Fiducoldex, con el propósito de establecer las medidas de tratamiento que se requieran, entre las que se puede encontrar reducir o trasferir el riesgo. Para esto se debe tener en consideración los siguientes lineamientos:

- El nivel de severidad residual de riesgo admisible para FIDUCOLDEX S.A. aprobado por la Junta Directiva es:" Media". Cuando el nivel de riesgo residual supere el nivel admisible, los líderes de los procesos del P.A. FONTUR establecerán los planes de tratamiento para mitigar los riesgos

- En ningún caso el líder de proceso del P.A. FONTUR podrá asumir riesgos que se encuentren ubicados en la zona de severidad "Alta" o "Crítica", para los cuales deberá formular e implementar planes de tratamiento para mitigarlos y escalarlos a las instancias correspondiente.

    - En este caso, el Oficial de Cumplimiento de Fiducoldex procederá a informar la Oficina de Planeación del P.A. FONTUR para coordinar las mesas de trabajo con los líderes de procesos que se requieran.

- En la formulación de planes de tratamiento se debe realizar el análisis de los costos (si conlleva) y beneficios de su implementación.

- En caso de que la implementación de un plan de tratamiento conlleve la destinación de recursos por parte del P.A. FONTUR, el líder de proceso que realiza la propuesta debe validar el mismo, con su superior jerárquico y adelantar las gestiones correspondientes para la asignación del presupuesto requerido.

En caso de que la propuesta de tratamiento corresponda a una transferencia de riesgos mediante la contratación de un seguro, esta debe ser presentada a las instancias de aprobación internas establecidas del P.A. FONTUR para su análisis y validación de disponibilidad de recursos.

4.3.4 Monitoreo

En la etapa de monitoreo se busca verificar, supervisar y hacer seguimiento a la administración del riesgo LAFT dentro de la cual se confirma la efectividad del cumplimiento frente a los lineamientos, procedimientos y metodologías definidos por Fiducoldex.

El monitoreo se ejecutará por parte de la Dirección SARO-SARLAFT de Fiducoldex, realizando la actualización de la matriz metodológica de SARLAFT mediante la revisión de los procesos del P.A. FONTUR; así como, a través del testeo de los controles, el cual

comprenderá la revisión de los soportes documentales que requiera a los líderes de proceso del P.A. FONTUR y/o a través de la realización de pruebas de recorrido que permitan identificar su correcta ejecución.

4.4 Conocimiento de contratistas derivados y sus beneficiarios finales

De acuerdo con lo establecido en el numeral 8.2.4 del Manual SARLAFT de Fiducoldex, aplicable a la Sociedad Fiduciaria y a todos sus negocios administrados, se debe dar cumplimiento a lo dispuesto en el PR-GAD-019 Procedimiento de Vinculación y/o Actualización para Proveedores y Contratistas que pretendan tener relación contractual con el PA FONTUR.

Las áreas del P.A. FONTUR, una vez sean seleccionados los contratistas, de acuerdo con los criterios y procedimientos que se establezcan en el Manual de Contratación del P.A. FONTUR, deben solicitar la vinculación y/o actualización de estos, según corresponda, a la Coordinación Administrativa de Suministros y Adquisiciones de Fiducoldex, quien realizará la gestión de conocimiento con el apoyo del funcionario de la Unidad de Gestión de FONTUR que sea designado.

Todos los contratistas deberán diligenciar y firmar el formato FT-GAD-015, entregar los soportes definidos en el Procedimiento PR-GAD-19, garantizando la completitud y consistencia de la información. En el caso de personas jurídicas adicionalmente deberán proporcionar la información de sus beneficiarios finales, mediante el diligenciamiento del formulario Formato FT-GAD-069.

La Coordinación Administrativa de Suministros y Adquisiciones de Fiducoldex, a través del personal de la Unidad Misional de FONTUR designado para esta gestión, verificará el formulario de tal forma que esté diligenciado de manera completa, esté firmado y la información sea consistente con la documentación entregada. En caso de evidenciar novedades las dará a conocer al área solicitante, para que apoye las gestiones para la corrección o complemento por el proveedor o contratista derivado que haya a lugar. De persistir inconsistencias notificará al área solicitante sobre la imposibilidad de continuar con la vinculación, así mismo, reportará al Equipo de Cumplimiento SARLAFT esta alerta presentada en el proceso de vinculación.

La Coordinación Administrativa de Suministros y Adquisiciones de Fiducoldex, a través del personal de la Unidad Misional de FONTUR designado para esta gestión, realizará la consulta en las listas vinculantes para Colombia y en las restrictivas disponibles por Fiducoldex a los contratistas, así como a sus beneficiarios finales, y también a las personas relacionadas en los documentos suministrados. De encontrar alguna coincidencia relacionada con temas de LA/FT o delitos contra la administración pública, se aplicará lo definido en el numeral 6.3 del Manual SARLAFT - POLÍTICAS SOBRE CONSULTAS EN LISTAS VINCULANTES PARA COLOMBIA Y LISTAS RESTRICTIVAS. Todas las novedades que se presenten en la vinculación de contratistas que no sean subsanadas, deberán ser puestas en conocimiento del Equipo de Cumplimiento SARLAFT para su validación y concepto con el Oficial de Cumplimiento.

Es importante mencionar que además estas consultas en listas se deben realizarse para todos las personas con las cuales se pretenda tener una relación contractual tales como proponentes y sus relacionados.

De esta manera debe darse aplicación a la política de consulta en listas del Manual SARLAFT que establece "*Abstenerse de vincular clientes, proveedores o contratistas derivados que se encuentren reportados o incluidos en listas vinculantes para Colombia, en la lista de la Office Foreign Assets Control (OFAC) o las listas que determine el Consejo de Seguridad Nacional de Colombia; así mismo, si están sancionados o condenados judicial o administrativamente por actividades relacionadas con LA/FT.*"

4.5 Divulgación y Capacitación

El plan de capacitación será definido por la Dirección SARO – SARLAFT de la Gerencia de Riesgos de la Fiduciaria y actualizado de acuerdo con las necesidades identificadas, dando cumplimiento a la normatividad vigente, estará compuesto por las capacitaciones de inducción, que serán dictadas a los empleados nuevos de planta y temporales del P.A. FONTUR y las capacitaciones anuales de fortalecimiento de conocimientos, que podrá manejar temas diferentes y esenciales para la administración del riesgo de LAFT.

4.6 Reportes y presentación de informes

4.6.1 Operaciones inusuales

Los empleados del P.A. FONTUR, como responsables de la gestión operativa de los procesos y programas a su cargo, deberán reportar de forma oportuna cualquier hecho o situación inusual o sospechosa que haga suponer que puede estarse presentando un intento de lavado de activos o financiación del terrorismo a través del Patrimonio Autónomo, dicho reporte deberá ser remitido a la Dirección SARO – SARLAFT a través del correo electrónico cumplimientolaft@fiducoldex.com.co y demás mecanismos definidos por ésta.

4.7 Documentación relacionada

Dentro del SARLAFT de Fiducoldex se encuentran documentados los procedimientos, metodologías y formatos aplicados a la gestión del riesgo de Lavado de Activos y Financiación del Terrorismo, de los cuales específicamente serán aplicables al P.A. FONTUR los siguientes:

- **MA-GRI-001** - Manual SARLAFT.
- **PR-GAD-010** - Procedimiento de Debida Diligencia para la Vinculación o Actualización de los Proveedores.
- **PR-GAD-019** - Procedimiento de vinculación y/o actualización para proveedores y contratistas derivados para Fiducoldex y sus negocios administrados.
- **PT-GRI -007** - Protocolo Metodológico para gestionar los Riesgos de LAFT.
- **PT-GRI -004** - Protocolo de metodología Autoevaluación de Riesgos y Controles.
- Circular Básica Contable y Financiera (Circular Externa 100 de 1995), Capítulo XXXI Sistema Integral de Administración de Riesgos (SIAR) de la Superintendencia Financiera de Colombia.

5 CAPÍTULO V – GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

5.1 Lineamientos y procedimientos para la gestión de seguridad de la información y ciberseguridad

El presente documento establece y define los siguientes lineamientos que deben cumplir los trabajadores, proveedores y entidades que tengan relación con el P.A. FONTUR, con respecto a la Gestión de la Seguridad de la Información y Ciberseguridad:

- En el P.A. FONTUR se debe dar cumplimiento a la política, lineamientos y directrices establecidas por Fiducoldex en su Sistema de Gestión de la Seguridad de Información (SGSI), con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información de la entidad y del P.A. FONTUR, para garantizar la operatividad de sus procesos , preserva la buena imagen de la Fiduciaria y dar cumplimiento a las obligaciones contractuales establecidas con el Ministerio de Comercio, Industria y Turismo en el marco del contrato 413-2023.

- Se deben identificar, medir, controlar y monitorear los posibles riesgos de seguridad de la información y ciberseguridad asociados a gestión del P.A. FONTUR y de sus activos de información.

- Es necesario establecer las medidas de seguridad de la información y ciberseguridad para mitigar los riesgos de seguridad identificados y las necesarias para dar cumplimiento a los requerimientos normativos de la SFC y otras entidades reguladoras, así como a los acuerdos con terceros vigentes relacionados a la seguridad de la información y ciberseguridad.

- Se deben reportar, detectar gestionar y hacer seguimiento a los incidentes de seguridad de la información y ciberseguridad que puedan afectar o atenten contra la confidencialidad, disponibilidad e integridad de la información.

Es prioritario motivar, capacitar y concientizar permanentemente a los trabajadores y terceros sobre la responsabilidad de hacer uso de información que pertenezca al P.A. FONTUR y a Fiducoldex.

5.2 Gestión de usuarios

Administración de Accesos de Usuarios y Perfiles

La administración de usuarios y perfiles consiste en la atención de las solicitudes que realicen los líderes de proceso del P.A. FONTUR para la creación, modificación y eliminación de los accesos en las diferentes aplicaciones, las cuales deben estar plenamente justificadas atendiendo las necesidades del P.A. FONTUR y siguiendo el procedimiento que para este efecto se definan.

Por su parte, la Dirección de Seguridad de la Información y Continuidad de Negocio debe establecer y mantener actualizada una matriz en la que se especifiquen los diferentes perfiles de usuario y las funcionalidades asignadas de los aplicativos, así mismo, debe

llevar un control de los usuarios a los cuales les han sido asignados estos perfiles. En la asignación de los accesos a los aplicativos y a sus funcionalidades se debe verificar que no se presente incompatibilidad respecto a las funciones a realizar.

Control de acceso

- La administración de controles de acceso al sistema debe estar separadas de otros deberes incompatibles. Algunos ejemplos de dichos deberes incluyen la operación de sistemas, el soporte técnico, el desarrollo de sistemas y la utilización como parte de la operación.

- Las solicitudes para la creación, modificación y eliminación del código de acceso del usuario a los sistemas deben:

    - Documentarse.
    - Ser autorizadas por el jefe del usuario y, si fuera necesario, por otras áreas de negocio responsables de la información del negocio o sistema en cuestión.
    - Retenerse por un mínimo de 6 meses.

- Los códigos de acceso son de uso personal e intransferible y se deben proteger de forma confidencial. Los trabajadores son responsables de todas las actividades llevadas a cabo con su código de acceso.

- No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por la Dirección de Seguridad de la Información y Continuidad del Negocio de Fiducoldex S.A.

- Los códigos de acceso al sistema deben ser revisados al menos cada seis meses.

- El acceso a la red por parte de terceros es restrictivo y permisible únicamente mediante suscripción del acuerdo de seguridad de la información (acuerdo de confidencialidad) y aceptación de la política de seguridad de la información.

- El sistema debe desplegar un aviso (“log-on banner”), antes de conceder el acceso, que advierta que únicamente los usuarios autorizados pueden acceder al sistema y que el acceso no autorizado podría considerarse como un acto delictivo.

- Las contraseñas deben ser distribuidas a los usuarios del sistema a través de medios seguros.

- Los códigos de acceso al sistema deben cancelarse cuando ya no sean necesarias.

- Se deben inactivar, preferiblemente de manera automática, las cuentas que no presentan actividad después de un período de tiempo (están exceptas los códigos utilizados como cuentas de conexión).

- Se deben inactivar los códigos de usuarios de los trabajadores que presentan cualquier tipo de ausentismo (vacaciones, licencias, incapacidades, etc.) por un período superior o igual a cinco (5) días hábiles.

- Cualquier uso de contraseñas compartidas u otras credenciales es excepcional y específicamente autorizado por la Secretaria General del P.A. FONTUR. Se debe asignar responsabilidad específica para revisar y mantener las contraseñas compartidas.

- Las novedades relacionadas con códigos de usuarios deben quedar registradas en el log de auditoría.

- Se deben utilizar mecanismos automatizados para apoyar el monitoreo sobre las acciones de creación, modificación, desactivación y eliminación de los códigos de usuarios y si es del caso, utilizar la notificación a los usuarios en la medida que se requiera.

5.3 Gestión de incidentes de Seguridad de la Información y Ciberseguridad

El objetivo principal de este capítulo de gestión de incidentes de seguridad de la información y ciberseguridad es contar con un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información y ciberseguridad, para poder desarrollar los siguientes objetivos:

- Definir roles y responsabilidades, como eje puntual para evaluar los riesgos y que se permita mantener la operación, la continuidad y la disponibilidad de los servicios críticos del P.A. FONTUR.

- Gestionar los eventos de seguridad de la información y ciberseguridad desde su detección, con el fin de identificar si se requiere clasificarlos como incidentes de seguridad de la información y/o ciberseguridad.

- Minimizar los impactos adversos de los incidentes en el P.A. FONTUR y sus operaciones, mediante la utilización de las salvaguardas establecidas en el desarrollo de este manual.

- Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y ciberseguridad y validar su gestión para evitar la repetición de estos eventos. Con lo anterior, se reduce la ocurrencia de futuros incidentes, mejora la implementación y el uso de las salvaguardas y mejora el esquema global de la gestión de incidentes de seguridad de la información.

- Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información y ciberseguridad, a través de una base de conocimiento y registro de incidentes basada en la bitácora de incidentes, según el procedimiento de gestión de incidentes de seguridad de la información y ciberseguridad.

- Definir los lineamientos para el procedimiento formal de reporte y escalamiento de los incidentes de seguridad de la información.

Metodología

Para lograr los anteriores objetivos, en la gestión de incidentes de seguridad de la información y ciberseguridad se seguirán las siguientes etapas de manera cíclica:

Gráfica 1. Ciclo de vida para la respuesta a Incidentes de seguridad de la información, según el NIST (Instituto Nacional de Estándares y Tecnología de los Estados Unidos)

Fuente: NIST (Instituto Nacional de Estándares y Tecnología de los Estados Unidos)

- Planificación y preparación para la gestión del Incidente
- Detección y análisis.
- Contención, erradicación y recuperación.
- Actividades Post-Incidente.

La Dirección de Seguridad de la Información y PCN de Fiducoldex definirá el procedimiento para la gestión de incidentes y apoyará las actividades para la atención de estos; así mismo, manejará las relaciones con entes internos y externos. Por otra, la Oficina de Planeación, en articulación con la Oficina de Tecnología, estará a cargo de:

- **Detectar Incidentes de Seguridad:** monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información a través del soporte de (los) proveedor(es) que adelante(n) el monitoreo de seguridad y ciberseguridad.

- **Atender los Incidentes de Seguridad:** recibir y resolver los incidentes de seguridad de acuerdo con los procedimientos establecidos.

- **Recolectar y Analizar la Evidencia Digital:** toma, preservación, documentación y análisis de evidencia cuando sea requerida.

- **Efectuar anuncios de Seguridad:** debe mantener informados a los trabajadores, contratistas o terceros sobre las nuevas vulnerabilidades,

actualizaciones a las plataformas y recomendaciones de seguridad informática, a través de algún medio de comunicación (Web, Intranet, Correo).

- **Realizar análisis de Seguridad Informática:** debe coordinar y gestionar l las verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.

5.4 Evaluación de nivel de madurez de Seguridad de la Información (ISO 27001) y Ciberseguridad (NIST)

Alineado al Sistema de Gestión de Seguridad de la Información implementado en Fiducoldex, se evaluará el nivel de madurez en el P.A. FONTUR respecto a los dominios de control y controles que están en el alcance de la Herramienta de Diagnóstico de Seguridad de Gobierno Digital.

A partir de los resultados de esta evaluación se debe **formular e implementar un plan de trabajo** para mejorar el nivel de madurez del SGSI. Los resultados serán consolidados por la Oficina de Planeación del P.A. FONTUR y analizados con la Dirección de Seguridad de la Información y PCN de la Fiduciaria. A su vez serán presentados a la Secretaria General y la Gerente General del P.A. FONTUR.

Posterior al seguimiento de los planes de trabajo, se debe realizar una **nueva evaluación del SGSI** para verificar las mejoras implementadas.

5.5 Etapas para la gestión de riesgos de seguridad de información y ciberseguridad

La gestión de los riesgos de seguridad y ciberseguridad de la información será coordinada por la Oficina de Planeación del P.A. FONTUR, atendiendo las directrices y metodologías que defina la Dirección de Seguridad de la Información y PCN y la Dirección SARO-SARLAFT de Fiducoldex.

5.5.1 Identificación

En la etapa de identificación se determinan los riesgos (actuales y potenciales) de seguridad y ciberseguridad de la información inherentes a las actividades que desarrolla o planea desarrollar el P.A. FONTUR y asociados a los activos de información del patrimonio.

Esta etapa debe realizarse con una periodicidad anual y previamente en el caso de la implementación de nuevas actividades o de la modificación sobre las que están en operación y/o cambios en el plan de negocio, en la forma de operación de los procesos del Patrimonio, así como con la implementación de nuevas soluciones tecnológicas o servicios en nube para procesos misionales o de gestión contable y financiera, acorde con lo dispuesto por la Superintendencia Financiera de Colombia.

Para la realización de esta etapa se deberá contar con la participación de los líderes de proceso con la coordinación y acompañamiento de la Oficina de Planeación del P.A. FONTUR, y se tendrán en cuenta los lineamientos establecidos en el numeral 3.3.1 del presente Manual.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

Así mismo, se tendrán en cuenta los resultados de la Identificación, Clasificación y Valoración de los Activos de Información, a través de la cual se establecerá el grado de criticidad de los activos, información que retroalimentará la identificación y medición de los riesgos de seguridad, ciberseguridad y privacidad de la información. Para esto, la Oficina de Planeación del P.A. FONTUR definirá el respectivo procedimiento y acompañará a los líderes de proceso en estos ejercicios.

5.5.2 Medición

En la medición de los riesgos de Seguridad y ciberseguridad de la Información del P.A. FONTUR, se cuantifica y/o evalúa la exposición a nivel inherente, mediante la calificación de la probabilidad y del impacto en caso de materializarse. Esta medición se realizará por los líderes de proceso con la coordinación y acompañamiento de la Oficina de Planeación del P.A. FONTUR, aplicando la metodología establecida por Fiducoldex, cuyos lineamientos se describen en el numeral 3.4.2.

5.5.3 Control

En esta etapa se establecen los mecanismos tendientes a mitigar y/o minimizar la posibilidad de ocurrencia e impacto de la materialización de los riesgos inherentes a las actividades que desarrolla el P.A. FONTUR.

Para la identificación, documentación y valoración de los controles se seguirá los lineamientos establecidos en el numeral 3.4.3. Esta etapa será liderada por la Oficina de Planeación del P.A. FONTUR y se requiere la participación de los líderes de proceso.

5.5.4 Monitoreo

En esta etapa se deberá realizar un seguimiento permanente y efectivo a las fuentes de riesgo, al perfil de riesgo y, a la efectividad de los controles implementados y al posible impacto de la materialización de los riesgos. Respecto a la efectividad de los controles se adelantarán monitoreos muestrales por parte de la Oficina de Planeación del P.A. FONTUR con el fin de verificar que estos se ejecuten según se encuentran definidos.

5.5.4.1 Análisis y remediación de vulnerabilidades y Pruebas de Ethical Hacking

Por otra parte, y con el propósito de monitorear el estado de las amenazas y ciber amenazas de seguridad de la información se gestionará por parte de la Dirección de Seguridad de la Información y PCN de Fiducoldex, a través de los servicios que contrate la Fiduciaria, pruebas de vulnerabilidad trimestrales y de Ethical hacking anual para los sistemas del P.A. FONTUR.

Los resultados de estos análisis deberán ser remitidos a la Oficina de Tecnología quien, con el apoyo del(los) profesional(es) que determine, debe realizar la formulación del plan de acción con el propósito de remediar estas vulnerabilidades. Así mismo, estos resultados podrán originar ajustes en el perfil de riesgos de seguridad y ciberseguridad de la información del P.A. FONTUR, sobre lo cual se deben reportar a la Dirección de Seguridad de la Información y PCN y de SARO-SARLAFT de la Fiduciaria.

5.6 Divulgación y Capacitación

El programa de sensibilización y capacitación tiene como objetivo asegurar que los trabajadores comprendan y conozcan los lineamientos y procedimientos de seguridad y ciberseguridad de la información y adopten el Modelo de Seguridad de la Información y Ciberseguridad aplicado por Fiducoldex para la protección de los activos de información del P.A. FONTUR.

La Oficina de Planeación del P.A. FONTUR será responsable de gestionar y/o ejecutar el programa de sensibilización y capacitación, el cual comprende:

- **Inducción de ingreso:** Todos los nuevos trabajadores del P.A. FONTUR recibirán capacitación sobre seguridad de la información y ciberseguridad como parte de su proceso de inducción.

- **Reinducciones anuales:** Todos los trabajadores del P.A. FONTUR recibirán capacitación anual sobre seguridad de la información y ciberseguridad.

- **Capacitación específica:** Se ofrecerá capacitación específica a los grupos de interés o procesos del P.A. FONTUR que acorde con sus funciones que lo requieran.

- **Divulgación de piezas de sensibilización:** se realizará publicación periódica mediante correo electrónico y pantallas con los aspectos relevantes de seguridad de la información, ciberseguridad en el P.A. FONTUR.

La efectividad del programa se evaluará mediante:

- **Evaluaciones de eficacia:** Se evaluará el nivel de conocimiento y comprensión de la información provista en las capacitaciones realizadas.

- **Cobertura de las actividades de capacitación:** Se analizarán los datos de participación en las sesiones de inducción y capacitación.

5.7 Reportes y presentación de informes

La Oficina de Planeación del P.A. FONTUR, quien tendrá a cargo la gestión de seguridad y ciberseguridad de la Información preparará y remitirá a la Dirección de Seguridad de la Información y PCN de Fiducoldex y al Ministerio de Comercio, Industria y Turismo los siguientes reportes:

- Estado de avance del cronograma y actividades para la gestión de seguridad y ciberseguridad de la información del P.A. FONTUR (Semestral).
- Informe de la Gestión de vulnerabilidades (Semestral).
- Reporte de incidentes de seguridad y ciberseguridad de la Información (Semestral).
- Reporte de cumplimiento de actividades de capacitación, sensibilización y socialización de la gestión de seguridad y ciberseguridad de la información, incluyendo el porcentaje de cobertura en los trabajadores (Anual).

5.8 Documentación relacionada

- Estándar ISO/IEC 27001 (Sistemas de Gestión de Seguridad de la Información).
- Estándar ISO/IEC 27032 (Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad)
- Estándar ISO/IEC 31000 (Gestión de Riesgos - Principios y Directrices)

6 CAPÍTULO VI – GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La gestión de continuidad de negocio busca definir e implementar la estrategia de Continuidad del Negocio que permita recuperar y restaurar en el P.A. FONTUR las funciones críticas, parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

6.1 Lineamientos y procedimientos para la gestión de continuidad del negocio

La gestión de la continuidad de negocio se centra en la mitigación del impacto de un evento disruptivo, es decir, tiene un enfoque correctivo sobre los incidentes que se presenten, definiendo previamente un plan de acción que soporte la administración de la crisis para que el P.A. FONTUR continúe prestando sus servicios en los tiempos establecidos y las obligaciones contraídas por Fiducoldex con el Ministerio de Comercio, Industria y Turismo puedan ser ejecutadas en las condiciones establecidas.

6.2 Análisis BIA según estructura de procesos del P.A. FONTUR

La definición de la estrategia para la continuidad del negocio del P.A. FONTUR se apoya en el Análisis de Impacto al Negocio – BIA (Business Impact Analysis), el cual se desarrolla con el fin de identificar la criticidad y priorización de los diferentes procesos P.A. FONTUR mediante la identificación de los impactos cuantitativos y cualitativos, que lo afectarían en caso de presentarse un incidente perjudicial.

El Análisis de Impacto de Negocio se debe desarrollar anualmente de acuerdo con la metodología definida por la Fiduciaria en el MA-GRI-012 Manual de Continuidad del Negocio y el Formato BIA (FT-GRI-017 Análisis de Impacto en el Negocio BIA). Para esto la Oficina de Planeación debe programar y desarrollar las sesiones con los líderes de proceso del P.A., FONTUR y analizar y consolidar los resultados.

6.3 Definición y aprobación estrategia de continuidad del P.A. FONTUR

La estrategia para la continuidad del negocio se debe fundamentar en los resultados del análisis de impacto al negocio (BIA) y en la evaluación de riesgos, contemplando el antes, durante y después de una interrupción para las funciones criticas / prioritarias frente a un incidente desastre o una interrupción mayor.

La formulación de esta estrategia debe contemplar los planes y procedimientos para garantizar la continuidad del negocio recuperando las actividades prioritarias dentro del periodo de tiempo identificado y la capacidad acordada. Esta debe ser propuesta por la Dirección de Seguridad de la Información y PCN de Fiducoldex, con la participación de la Oficina de Tecnología y la Dirección de Servicios Administrativos del P.A. FONTUR, quienes deben apoyar en la definición de las especificaciones técnicas de los recursos tecnológicos y administrativos requeridos para su implementación, así como en la determinación de los respectivos costos.

Esta estrategia debe ser revisada por la Secretaria General y aprobada la Gerencia General del P.A. FONTUR.

Los recursos requeridos para la implementación y mantenimiento de la estrategia de continuidad de negocio deben ser incorporados en el presupuesto anual de gastos del P.A. FONTUR.

6.4 Definición y ejecución del plan de pruebas del PCN P.A. FONTUR

Con periodicidad anual se debe definir un plan de pruebas para validar el nivel de alistamiento y verificar la funcionalidad de la estrategia implementada, ante un evento disruptivo de acuerdo con la estrategia establecida para dar continuidad del negocio. Este plan debe formularse en conjunto por la Oficina de Planeación del P.A. FONTUR y la Dirección de Seguridad de la Información y PCN de Fiducoldex, con la participación de la Oficina de Tecnología y la Dirección de Servicios Administrativos del P.A. FONTUR.

Es obligatorio que la Oficina de Planeación del P.A. FONTUR coordine la ejecución de las pruebas, según la planeación definida, con la intervención de las áreas anteriormente mencionadas y los líderes de los procesos críticos del P.A. FONTUR. Así mismo, debe consolidar y presentar los resultados a la Dirección de Seguridad de la Información y PCN de Fiducoldex, Secretaría General y Gerencia General del P.A. FONTUR. Así mismo, debe elaborar los informes respectivos para poner en conocimiento del Ministerio de Comercio, Industria y Turismo el estado de la estrategia de continuidad.

6.5 Evaluación del nivel de madurez de Continuidad del Negocio (ISO 22301)

Con el propósito de fortalecer la Gestión de Continuidad de Negocio en el P.A. FONTUR, se realizará la evaluación del nivel de madurez aplicando el modelo de evaluación de controles implementado por Fiducoldex, el cual sigue el estándar ISO 22301.

A partir de los resultados, se formulará el respectivo plan de trabajo para reducir las brechas identificadas. Los resultados serán consolidados por la Oficina de Planeación del P.A. FONTUR y analizados con la Dirección de Seguridad de la Información y PCN de la Fiduciaria. A su vez serán presentados a la Secretaría General y la Gerencia General del P.A. FONTUR.

6.6 Etapas para la gestión de riesgos de continuidad del negocio

6.6.1 Identificación

En la etapa de identificación se documentan los riesgos de continuidad de negocio actuales y potenciales, que podrían afectan la prestación de los servicios y actividades del P.A. FONTUR, considerando los diferentes eventos disruptivos. Será desarrollada por el Dirección de Seguridad de la Información y PCN con la participación de los líderes de proceso y con el apoyo del responsable de la gestión de riesgo operacional de la Oficina de Planeación del P.A. FONTUR, para lo cual se deben tener en cuenta los lineamientos establecidos en el numeral 3.4.1 del presente Manual.

Para realizar este análisis en el P.A. FONTUR, se considerarán los resultados del BIA, en el que se identifican las actividades, procesos críticos y recursos necesarios.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

6.6.2 Medición

En la etapa de medición se evalúa la probabilidad e impacto de los riesgos de continuidad de negocio que afecten la prestación de los servicios misionales del P.A. FONTUR. La medición se debe realizar mediante metodologías definidas por Fiducoldex para la gestión de riesgo operacional y documentadas en el Manual SIAR y sus documentos asociados y se deben seguir los lineamientos expuestos en el numeral 3.4.2.

En esta etapa se requiere la participación de los líderes de proceso del patrimonio con el apoyo del responsable de la gestión de riesgo operacional de la Oficina de Planeación del P.A. FONTUR.

6.6.3 Control

En esta etapa se establecen mecanismos de control para mitigar y minimizar la probabilidad e impacto de los riesgos de continuidad de negocio que afectan a las actividades misionales del P.A. FONTUR.

Los mecanismos de control pueden incluir:

- **Planes de respuesta a incidentes:** Estos planes definen las acciones que se deben tomar en caso de un evento disruptivo.
- **Controles preventivos:** Estos controles se implementan para evitar que ocurran eventos disruptivos.
- **Controles de detección:** Estos controles se utilizan para identificar eventos disruptivos en caso de que ocurran.
- **Controles de recuperación:** Estos controles se utilizan para restaurar las operaciones a la normalidad después de un evento disruptivo.

La selección de los mecanismos de control se basará en la siguiente información:

- La probabilidad de que ocurra un riesgo.
- El impacto potencial del riesgo.
- El costo de implementar el mecanismo de control.

En esta etapa se requiere la participación de los líderes de proceso y será liderada por la gestión de riesgo operacional de la Oficina de Planeación del P.A. FONTUR.

6.6.4 Monitoreo

En la etapa de monitoreo se contempla la definición y ejecución del plan de pruebas de continuidad de negocio como mecanismo de verificación de la efectividad de la estrategia de continuidad implementada, cuya ejecución permitirá a la vez familiarizar a los trabajadores encargados de su implementación. Así mismo, contempla la verificación de

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

los controles definidos para mitigar los riesgos, las cuales permitirán retroalimentar y actualizar el perfil de riesgos de continuidad del P.A. FONTUR.

6.7 Divulgación y capacitación

El programa de sensibilización y capacitación tiene como objetivo asegurar que los trabajadores del P.A. FONTUR comprendan los lineamientos, procedimientos y estrategias para la Continuidad del Negocio.

La Oficina de Planeación del P.A. FONTUR será responsable de la ejecución del programa el cual comprenderá:

- **Inducción de ingreso:** Todos los nuevos trabajadores del P.A. FONTUR recibirán capacitación sobre el Plan de Continuidad del Negocio como parte de su proceso de inducción.

- **Reinducciones anuales:** Todos los trabajadores del P.A. FONTUR recibirán capacitación anual sobre el Plan de Continuidad del Negocio.

- **Capacitación específica:** Se ofrecerá capacitación específica a los grupos de interés y/o procesos que lo requieran.

- **Divulgación de piezas de sensibilización:** se realizará publicación periódica mediante correo electrónico y pantallas con los aspectos relevantes del plan de continuidad de negocio implementado en el P.A. FONTUR.

La efectividad del programa se evaluará mediante:

- **Evaluaciones de desempeño:** Se evaluará el nivel de conocimiento y comprensión de la información provista en las capacitaciones y el desempeño de los participantes en simulacros de eventos disruptivos.

- **Cobertura de las actividades de capacitación:** Se analizará la participación en las actividades de inducción y capacitación.

6.8 Reportes y presentación de informes

La Oficina de Planeación del P.A. FONTUR, quien tendrá a cargo la gestión de continuidad de negocio preparará y remitirá a la Dirección de Seguridad de la Información y PCN de Fiducoldex y al Ministerio de Comercio, Industria y Turismo los siguientes reportes:

- Estado de avance del cronograma y de las actividades para la gestión de continuidad del negocio del P.A. FONTUR (Semestral), incluyendo lo relacionado con la planeación, implementación y pruebas de la estrategia de continuidad.
- Reporte de cumplimiento de actividades de capacitación, sensibilización y socialización de la gestión de continuidad del negocio, incluyendo el porcentaje de cobertura en los trabajadores (Anual).

6.9 Documentación relacionada

- Estándar ISO/IEC 22301 (Sistema de Gestión de la Continuidad de Negocio).
- Estándar ISO/IEC 31000 (Gestión de Riesgos - Principios y Directrices)

7 CAPÍTULO VII – PROTECCIÓN DE DATOS

7.1 Lineamientos y procedimientos para la protección de datos

La gestión de la protección de datos se centra en proteger la información, cumplir con las normas, minimizar los riesgos, ser transparente, respetar los derechos de los titulares de los datos, implementar una buena gobernanza de datos y crear una cultura de seguridad.

7.2 Política de tratamiento de datos del P.A. FONTUR

El P.A. FONTUR cuenta con una Política de Tratamiento de Datos Personales, la cual se encuentra implementada, aprobada y publicada en la página web del P.A. FONTUR. Su revisión y actualización estará a cargo de la Secretaría General y la aprobación del Gerente General del P.A. FONTUR. A su vez, el P.A. FONTUR cuenta con el apoyo jurídico del administrador, la sociedad Fiduciaria Colombiana de Comercio Exterior S.A. – Fiducoldex.

7.2.1 Clasificación de la información

En el P.A. FONTUR se establecen los lineamientos para la gestión de la información y para el tratamiento adecuado de los activos de información, tanto interna como externamente, los cuales se fundamentan en la Ley 1712 de 2014 *(Ley de Transparencia y del Derecho de Acceso a la Información Pública)* y en la Ley 1581 de 2012 *(Ley de Protección de Datos Personales).*

Su objetivo es garantizar que la información del P.A. FONTUR se gestione de manera adecuada, segura y transparente, protegiendo los derechos de los titulares de la información y cumpliendo con las normas legales vigentes. Estos lineamientos aplican a toda la información, en cualquier formato, que sea generada, recopilada, almacenada, procesada o transmitida por el P.A. FONTUR, incluyendo:

- Información pública
- Información reservada
- Información clasificada
- Datos personales

A su vez, los lineamientos se basan en los siguientes principios:

- **Legalidad:** La gestión de la información debe ser lícita, veraz y transparente.
- **Consentimiento:** El tratamiento de datos personales debe contar con el consentimiento libre, previo e informado del titular.
- **Finalidad:** La información debe ser recolectada y tratada para una finalidad específica y explícita.

- **Proporcionalidad:** La información recolectada debe ser proporcional al fin para el cual se solicita.

- **Seguridad:** La información debe ser protegida contra el uso indebido, acceso no autorizado, pérdida, destrucción o daño.

- **Acceso:** Los titulares de la información tienen derecho a acceder a la misma, conocerla, actualizarla y rectificarla.

- **Cancelación:** Los titulares de la información tienen derecho a solicitar la cancelación de esta cuando no se haya obtenido su autorización o cuando no se cumplan los requisitos legales para su tratamiento.

A continuación, se presenta las medidas que se deben tomar en el P.A. FONTUR, para garantizar un adecuado tratamiento de la información y el derecho de acceso a la misma por los ciudadanos:

- Implementar una política de gestión de la información.
- Clasificar la información de acuerdo con los niveles de reserva establecidos en la Ley 1712 de 2014.
- Establecer mecanismos para el control de acceso a la información.
- Capacitar a los empleados en materia de gestión de la información.
- Implementar medidas de seguridad para proteger la información.

7.3 Inscripción y/o actualización en el Registro Nacional de Bases de Datos (RNBD) de la Superintendencia de Industria y Comercio (SIC)

El Registro Nacional de Bases de Datos (RNBD) es un sistema administrado por la Superintendencia de Industria y Comercio (SIC) de Colombia, donde se inscriben todas las bases de datos que traten información personal de personas naturales o jurídicas en el territorio nacional.

De esta manera, en el P.A. FONTUR se debe dar cumplimiento al proceso de inscripción o actualización de Bases de Datos Personales en el (RNBD), a través del portal web de la SIC. Lo anterior atendiendo las guías, directrices y plazos establecidos por esa Superintendencia. Esta actividad será desarrollada por la Unidad de Gestión del el P.A. FONTUR, en coordinación con la Dirección de Seguridad de la Información y PCN de Fiducoldex, de acuerdo con el procedimiento que se establezca para tal fin.

Adicionalmente, se debe actualizar la información de los reclamos presentados por los Titulares.

7.4 Incidentes de protección de datos

De la misma manera, una vez finalizada la inscripción de la base de datos en el Registro Nacional de Bases de Datos (RNBD), se deben reportar como novedades los incidentes de seguridad que afecten la base de datos personales, dentro del plazo establecido por la SIC y cumpliendo los soportes y gestiones realizadas para el análisis, contención y atención del mismo.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

Un incidente de seguridad se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable del tratamiento o por su encargado.

7.5 Etapas para la gestión de riesgos de protección de datos

7.5.1 Identificación

Esta etapa se desarrollará atendiendo las actividades y responsabilidades establecidas en el numeral 5.3.1. del Presente Manual. En la etapa de identificación se realizará el inventario de activos de información, el cual permitirá:

- Identificar claramente las características de los activos de un proceso.
- Clasificarlos de acuerdo con su nivel de criticidad.
- Determinar aquellos que requieren mayor protección.

El responsable de realizar el inventario es el cada líder de proceso del P.A. FONTUR, quien contará con la asesoría del Profesional de Seguridad de la Información y Continuidad de Negocio del P.A. FONTUR.

7.5.2 Medición

En esta etapa se evalúa la probabilidad e impacto de los riesgos de protección de datos mediante las metodologías cualitativas y/o cuantitativas para la gestión de riesgo operacional definidas por Fiducoldex y documentadas en el Manual SIAR y sus documentos asociados.

En la etapa de medición, adicionalmente se realiza la clasificación de activos de información, la cual define los niveles de protección para la integridad, disponibilidad y confidencialidad de cada activo, y determina:

- Cómo se deben tratar los activos de información dentro del P.A. FONTUR.
- Las medidas que se deben tomar para garantizar un tratamiento adecuado, tanto al interior como al exterior de esta.

En el caso de que los activos de información se empleen datos personales, se debe indicar si se trata de información privada, semiprivada (artículo 3 de la Ley 1266 de 2008), de datos sensibles (artículo 5 de la Ley 1581 de 2012) o de información pública.

Es importante determinar el tipo de dato personal para:

- Aplicar las medidas de protección adecuadas
- Garantizar el cumplimiento de la normativa legal vigente
- Respetar los derechos de los titulares de los datos

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

7.5.3 Control

En la etapa de control se deben implementar los siguientes lineamientos y medidas de control para el manejo de la información reservada o clasificada:

Envío externo:

- La información reservada o clasificada debe ser protegida adecuadamente al enviarla de forma externa.

Conocimiento y responsabilidad:

- Todos los empleados y terceros deben conocer la política de tratamiento de la información.
- Todos los empleados y terceros deben firmar una cláusula de confidencialidad que garantice la protección y no divulgación de la información que manejan por motivos de trabajo.

Acceso:

- La información clasificada como reservada, restringida o confidencial debe estar fuera del alcance de personas no autorizadas.

Impresión:

- La impresión de documentos con información reservada o clasificada es responsabilidad del trabajador que la genera.
- El trabajador debe recoger la impresión personalmente de forma inmediata.

Divulgación:

- La divulgación de información reservada o clasificada solo debe realizarse:
  - Por necesidad de conocerla por motivos de trabajo.
  - Con autorización del propietario, caso por caso.
  - Amparada por un acuerdo de no divulgación firmado.

Restricción de acceso a documentos automatizados:

- Cifrar la información y facilitar solo al personal autorizado los mecanismos para descifrarla.

7.5.4 Monitoreo

El monitoreo de activos de información es el proceso de recopilar y analizar datos para identificar, clasificar y proteger los activos de información del P.A. FONTUR. Esto implica realizar un seguimiento continuo de los activos de información para identificar cualquier cambio en su estado o riesgo.

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co

El monitoreo de los activos de información se puede realizar utilizando una variedad de herramientas y técnicas, que incluyen:

- **Análisis de registros:** Esto implica revisar los registros del sistema para identificar actividades sospechosas o acceso no autorizado a activos de información.
- **Análisis de vulnerabilidades:** Esto implica escanear sistemas y redes para identificar vulnerabilidades que podrían ser explotadas por atacantes.
- **Pruebas de penetración:** Esto implica simular ataques a sistemas y redes para identificar y evaluar las vulnerabilidades de seguridad.
- **Monitoreo de redes:** Esto implica monitorear el tráfico de la red para identificar actividades inusuales o sospechosas.

7.6 Divulgación y capacitación

El programa de sensibilización y capacitación tiene como objetivo asegurar que los trabajadores del P.A. FONTUR comprendan y adopten la protección de Datos Personales, según lineamiento de la Ley 1581 de 2012. La Oficina de Planeación del P.A. FONTUR será responsable de la ejecución del programa, el cual se desarrollará bajos los mismos mecanismos establecidos en el numeral 5.7.

DOCUMENTOS Y FORMATOS ASOCIADOS		
CÓDIGO	**NOMBRE**	**RUTA DE CONSULTA Y DESCARGA**
PL-GRI-013 (Fiducoldex)	Política de Seguridad de la Información de la Gestión de Continuidad de Negocio	Fiducoldex S.A.
V05 (Fiducoldex)	Política de Tratamiento de Datos Personales P.A. FONTUR	Fiducoldex S.A.
PR-GAD-010 (Fiducoldex)	Procedimiento de Debida Diligencia para la Vinculación o Actualización de los Proveedores	Fiducoldex S.A.
PR-GRI-001 (Fiducoldex)	Procedimiento Gestión de eventos de Riesgo Operacional	Fiducoldex S.A.
MA-GRI-001 (Fiducoldex)	Manual SARLAFT de Fiducoldex	Fiducoldex S.A.
MA-GRI-011 (Fiducoldex)	Manual de Seguridad de la Información de Fiducoldex	Fiducoldex S.A.
PT-GRI -004 (Fiducoldex)	Protocolo de metodología Autoevaluación de Riesgos y Controles	Fiducoldex S.A.
PT-GRI-005 (Fiducoldex)	Protocolo Metodología de Evaluación de Riesgo Operacional	Fiducoldex S.A.
PT-GRI -007 (Fiducoldex)	Protocolo Metodológico para gestionar los Riesgos de LAFT	Fiducoldex S.A.
IT-GRI-022 (Fiducoldex)	Instructivo de Administración Eventos de Riesgo Operacionales en Atalaya	Fiducoldex S.A.
PT-GRI -006 (Fiducoldex)	Perfil de Riesgo operacional	Fiducoldex S.A.
P-GCA-002	Procedimiento Administración de Riesgos Operacionales en los Procesos del SGC	Administración de Riesgos Operacionales en los Procesos del SGC

G-GCA-002	Guía para la Administración de Riesgos Operacionales en los Procesos del Sistema de Gestión de Calidad	Guía para la Administración de Riesgos Operacionales en los Procesos el SGC
P-GCA-003	Procedimiento Gestión de Riesgos Materializados	Gestión de Riesgos Materializados

ANEXOS	
NÚMERO	**NOMBRE**
-	Esta versión no contiene anexos

CONTROL DE CAMBIOS		
FECHA	**VERSIÓN**	**DESCRIPCIÓN DEL CAMBIO**
04/02/2025	01	Creación del documento
20/06/2025	02	El ajuste se realiza con el propósito de precisar las áreas responsables en la detección y atención de los incidentes de seguridad de la información del P.A. FONTUR. Para ello, se plantea la inclusión de la Oficina de Tecnología como responsable de este proceso, en articulación con la Oficina de Planeación.
02/01/2026	03	Actualización en el marco del cumplimiento del Otrosí No. 6 al Contrato Fiduciario 413 de 2023, se actualizan cargos, acorde con la estructura aprobada en el Manual Operativo y se actualiza la sección 4.4 fortaleciendo los lineamientos de SARLAFT

RÓTULO DE APROBACIONES INTERNO		
REVISÓ	**REVISÓ**	**REVISÓ**
Víctor Manuel Supelano Mendoza	**Jeison Medina Valdez**	**Mary Jazmín Vergel Cardozo**
Directora SARO SARLAFT de Fiducoldex S.A.	Director de Seguridad de la Información, CI, PCN y Protección de Datos de Fiducoldex S.A.	Gerente de Riesgos Fiducoldex S.A.

Sección exclusiva para el manejo de manuales del Contrato de Fiducia Mercantil:

RÓTULO DE APROBACIONES EXTERNO	
REVISÓ 1ra versión	**APROBÓ**
Sesión Comité Fiduciario realizada el 20 de mayo de 2024	Fideicomitente - Ministerio de Comercio, Industria y Turismo
Acta 4 de 2024	Oficio No. 2-2025-041990 radicado el 30 de diciembre de 2025

Calle 28 # 13 A 24 Edificio Museo Parque Central
Piso 6 Torre B Bogotá D.C.- Colombia
Pbx: 601 747 0909
www.fontur.com.co