1. INTRODUCCIÓN

La Fundación Cataruben, en su compromiso continuo con la realización de su misión y la consecución de sus objetivos, reconoce la inherente presencia de situaciones de riesgos en el desarrollo de su valor. Estos riesgos, si no se manejan de manera adecuada, pueden tener un impacto adverso en la ejecución eficiente de sus operaciones, lo que a su vez podría repercutir en la materialización plena de los objetivos y metas que la Fundación se ha propuesto alcanzar.

En este contexto, se forja la Política de Gestión de Riesgos de la Fundación Cataruben. Esta política tiene como objetivo primordial implementar una metodología idónea que permita una administración integral y sostenible de los riesgos vinculados a los procesos fundamentales que caracterizan a Fundación Cataruben como entidad misional. Al hacerlo, se aspira a prevenir la concreción de dichos riesgos, alineando todas las acciones con los valores fundamentales que rigen y definen a nuestra organización.

La presente política se erige como un compromiso esencial de la Fundación Cataruben hacia la excelencia en la gestión y el logro efectivo de su impacto social. En las secciones siguientes, se detallarán los principios rectores y las prácticas concretas que guiarán nuestros esfuerzos en la identificación, evaluación y mitigación de los riesgos, a fin de asegurar una operación fluida y alineada con nuestra visión y valores.

2. GENERALIDADES

2.1. Objeto

Crear un conjunto de principios y herramientas que ayuden a identificar, tratar, manejar y seguir los riesgos. El propósito de estos esfuerzos es prevenir que los riesgos se conviertan en problemas reales y garantizar que los eventos que puedan impactar los objetivos estratégicos de Cataruben estén bajo control.

2.2. Alcance

La presente Política es aplicable a todas las personas y entidades relacionadas con la Fundación Cataruben, incluyendo miembros de la junta directiva, asociados, inversionistas, contratistas, proveedores, clientes, aliados, gestores del ecosistema y colaboradores. Su aplicación abarca todas las actividades desarrolladas por Cataruben.

3. TÉRMINOS Y DEFINICIONES

- **Administración de riesgos:** La cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital,

recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

- **Amenaza:** Peligro latente de que un evento físico de origen natural, o causado, o inducido por la acción humana de manera accidental, se presente con una severidad suficiente para causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes, la infraestructura, los medios de sustento, la prestación de servicios y los recursos ambientales, según Ley 1523 de 2012.

- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

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

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

- **Capacidad del riesgo:** Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

- **Compartir o transferir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.

- **Confiabilidad de la Información:** Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

- **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Control de riesgos:** La parte de administración de riesgos que involucra la implementación de políticas, estándares, procedimientos para eliminar o minimizar los riesgos adversos.

- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

- **Identificación del riesgo:** Elemento de control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo, se compone de definición de causas y consecuencias y clasificación del riesgo.

- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Integridad:** Propiedad de exactitud y completitud.

- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

- **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.

- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **Reducir el riesgo:** Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

- **Riesgo:** Representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos. En esencia es un efecto de incertidumbre sobre los objetivos.

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

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

- **Seguridad de la información:** Conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

- **Valoración:** Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo inherente). Está integrada por el análisis y la evaluación del riesgo.

- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

4. FACTORES DE RIESGOS

Con carácter general, se considera riesgo el efecto, tanto positivo como negativo, de la incertidumbre sobre la consecución de los objetivos o de las expectativas razonables de negocio. A efectos de esta política se consideran factores de riesgo, cualquier amenaza de que un evento potencial, acción u omisión, afecte negativamente a dichos objetivos o expectativas de la Fundación Cataruben.

En el desarrollo de las actividades propias de Cataruben, se identifican diversos riesgos inherentes a los procesos/ áreas en la que opera, entre los que cabe destacar:

- **Riesgo de Corrupción.** Posibilidad de que se presente un acto, sin que ello signifique que exista corrupción en la entidad. Se trata de reconocer que se pueden presentar hechos de corrupción, con el fin de determinar sus causas y de establecer sus controles.

- **Riesgos Reputacionales.** Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.

- **Riesgo de Cumplimiento.** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

- **Riesgo de Seguridad de la Información.** Posibilidad de que una amenaza concreta explore una vulnerabilidad para causar una pérdida o daño en un activo de información. Suelen considerarse como una combinación de la probabilidad de

ocurrencia de un evento y sus consecuencias. Estos riesgos pueden clasificarse en pérdida de confidencialidad, pérdida de integridad y pérdida de disponibilidad.

- **Riesgos Operativos.** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
- **Riesgo Financieros.** Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
- **Riesgos Estratégicos:** Derivados de la posición estratégica de Cataruben en el entorno en que desarrolla su actividad, las relaciones con terceros, el portafolio de productos y servicios, así como la planificación y organización, y que pueden conllevar la dificultad en el cumplimiento de los objetivos definidos en su Plan Estratégico.
- **Riesgos Fiscales:** Asociados a la toma de decisiones en el ámbito tributario, ya sea por parte de Cataruben como por parte de autoridades tributarias o judiciales, que puedan conllevar un impacto negativo en los estados financieros o la reputación de La Fundación Cataruben.
- **Riesgo Gerenciales:** Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
- **Riesgos Tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

5. ASPECTOS FUNDAMENTALES PARA SU IMPLEMENTACIÓN.

Para la implementación de la presente política se deben considerar las siguientes etapas:

Etapa 1: Establecer contexto:

- Establecer el contexto tanto interno como externo en el cual se desarrollan las actividades de la organización y que condicionan positiva o negativamente el logro de los objetivos de la misma.
- Realizar análisis de la incidencia de los factores internos y externos de acuerdo con la naturaleza de cada negocio y las características propias de los procesos ejecutados y los productos y/o servicios entregados.
- Incluir en el análisis del contexto externo los factores geo políticos, legales, regulatorios, económicos, tecnológicos, socioculturales y ambientales, bien sean internacionales, nacionales o regionales, según sea el caso de análisis.
- Incluir en el análisis del contexto interno, la estructura, cultura organizacional, el cumplimiento de los planes y programas, los sistemas de información, los procesos, procedimientos, recursos humanos y/o económicos con los que dispone la empresa.

Etapa 2: Indicar Riesgos:

- Identificar los eventos que podrían afectar de forma positiva o negativa el cumplimiento o logro de los objetivos organizacionales a nivel estratégico, de procesos o de proyectos, con base en el análisis del contexto interno y externo que ha sido realizado en la etapa 1.

- Documentar la siguiente información para la identificación de riesgos:

  a. La descripción del riesgo.
  b. La identificación de causas
  c. La identificación de consecuencias.
  d. La identificación del tipo de impacto

Etapa 3. Valorar Riesgos:

- Estimar la probabilidad de ocurrencia y el impacto de sus consecuencias, con el fin de obtener información para el establecimiento del nivel de riesgo y la estrategia o plan de respuesta a implementar para su tratamiento.
- Realizar el análisis de los riesgos, utilizando como herramienta de evaluación las tablas de valoración de riesgos, las cuales adoptan formas descriptivas para representar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad).
- Evaluar los riesgos en dos fases:

  1. Riesgo inherente o sin control, considerando la naturaleza del riesgo y la evaluación del riesgo en su estado puro.
  2. Riesgo residual o controlado, considerando el grado en que se modifica el riesgo por efecto de los controles.

- Implementar estrategias de tratamiento o planes de respuesta según la valoración y el nivel del riesgo, con el fin de evitar, mitigar, transferir y/o aceptar el riesgo.
- Determinar los criterios de los niveles de apetito de riesgo, tolerancia y capacidad, para el logro de la estrategia corporativa.

Etapa 4: Definir Controles.

- Definir los controles o medidas que mantienen o modifican un riesgo, como acciones, planes de respuesta, políticas, procedimientos, entre otros, que apoyan el aseguramiento de las estrategias de tratamiento a los riesgos.
- Identificar las causas que puedan ocasionar la materialización del riesgo.
- Definir si los controles identificados contribuyen a maximizar la probabilidad y consecuencias de potenciales sucesos positivos o disminuir la probabilidad e impacto en el evento de materialización del riesgo o si disminuye o elimina alguna de las posibles causas del riesgo.
- Definir acciones de control posibles de realizar en términos de tiempos y costos.

Etapa 5: Implementar controles.

- Evaluar los controles implementados teniendo en cuenta su ejecución y la eficacia en el diseño.
- Evaluar el riesgo controlado teniendo en cuenta el tipo de control, es decir, si actúa sobre la probabilidad o el impacto.
- Reportar la materialización de riesgos identificada.

Etapa 6: Realizar Monitoreo y Revisión.

- Garantizar que las acciones se estén llevando a cabo y para evaluar la efectividad en su implementación.
- Garantizar que se identifican, evalúan, controlan y mitigan los riesgos, así como el monitoreo y revisión para evaluar la eficacia de los controles implementados.
- Hacer seguimiento periódico a la implementación de los controles y los resultados de la gestión de riesgos.
- Evaluar los riesgos y controles, con el fin de asegurar su manejo y gestión adecuada, así como sugerir y/o aplicar oportunamente los ajustes y correcciones que sean necesarios.
- Realizar seguimiento a la gestión integral de riesgos y brindar recomendaciones para su mejoramiento continuo a través de instancias superiores como el Comité de Presidencia y el Comité de Auditoría y Riesgos.

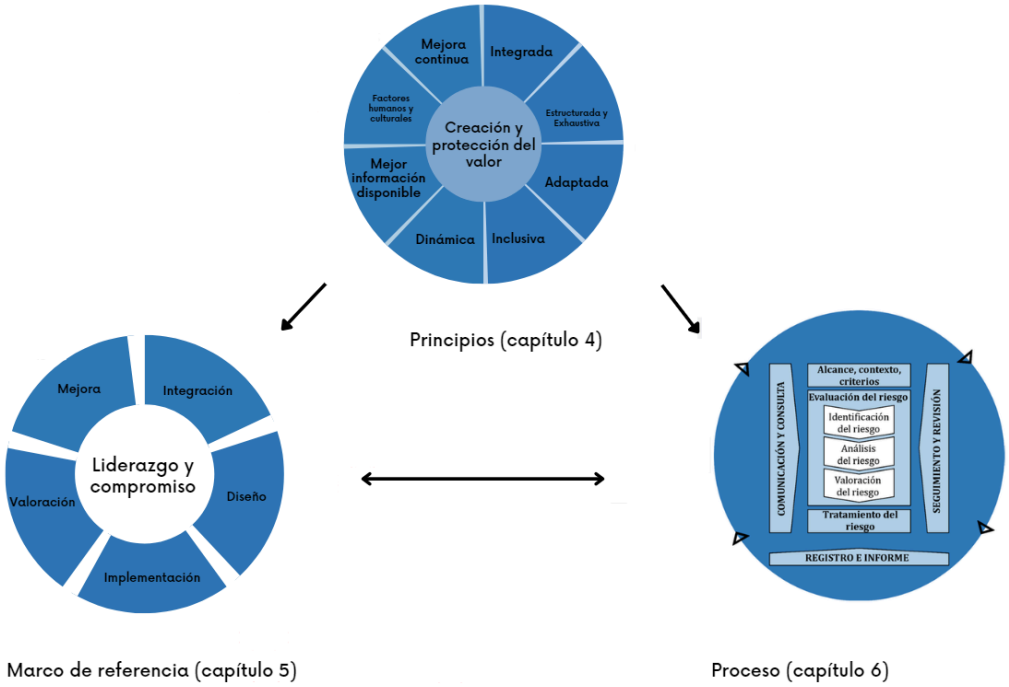
Etapa 7: Comunicación y Consulta.

- Garantizar que los responsables de la gestión, así como sus partes interesadas participen en la identificación y control de riesgos, analizan la situación en cada momento, comprenden y toman las mejores decisiones de actuación.

6. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO.

La gestión del riesgo en los procesos de la Fundación Cataruben, se basará en las directrices establecidas en la Norma Técnica Colombiana ISO 31010, en la cual se deben contemplar los principios, el marco de referencia y el proceso, conforme a la siguiente ilustración. Estos componentes podrían existir previamente en toda o parte de la organización, sin embargo, podría ser necesario adaptarlos o mejorarlos para que la gestión del riesgo sea eficiente, eficaz y coherente.

Figura 1: Metodología para la gestión del riesgo



Fuente: ISO 31010:2020

7. ESTRATEGIA PARA EL TRATAMIENTO DE LOS RIESGOS.

EVITAR. Cuando los escenarios de riesgo identificados se consideran demasiado EXTREMOS O ALTOS se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.

ACEPTAR. Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo BAJO.

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

COMPARTIR: Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionar, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia.

NOTA: Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

8. ÓRGANOS VINCULADOS A LA FUNCIÓN, CONTROL Y GESTIÓN DEL RIESGO.

Se establece una estructura de control para la gestión organizacional que determina los parámetros necesarios para la autogestión, la autorregulación y el autocontrol. Uno de los elementos fundamentales de esta estructura es el esquema de responsabilidades integrado por cuatro líneas de defensa, el cual proporciona una manera efectiva para mejorar las comunicaciones en la gestión de los riesgos y los controles mediante la aclaración de las funciones y deberes relacionados. A continuación se explica la aplicación de los roles y responsabilidades del esquema de líneas de defensa para la Fundación Cataruben.

8.1. Línea estratégica.

8.1.1. Asamblea General de asociados: Evalúa y aprueba la Política de Gestión de Riesgos y las responsabilidades para la gestión de los riesgos.

8.1.2. Comité de control interno del riesgo: Analiza los riesgos y amenazas de la Organización. Adicionalmente, define las líneas de reporte en temas claves para la toma de decisiones.

8.2. Primera línea de defensa.

8.2.1. Gerente General:

- Reporta al Comité de control interno del Riesgo y a Asamblea General de Asociados sobre los cambios relevantes en el perfil de riesgos estratégicos, el estado de avance de los planes de mitigación y en general el estado de implementación del Sistema de Gestión Integral en Riesgos.
- Identificar, evaluar, controlar y mitigar los riesgos a través de direccionamiento estratégico y plantea acciones correctivas de acuerdo con el nivel tolerable que defina.

8.2.2. Líderes de procesos, proyectos y equipos.

- Identificar, evaluar, controlar y mitigar los riesgos a través del autocontrol.
- Mantener efectivamente los controles internos y los controles del día a día.
- Conocer y apropiar las políticas, procedimientos, manuales, protocolos, entre otras herramientas para el autocontrol en los puestos de trabajo
- Identificar los riesgos de los procesos, programas y proyectos a su cargo, establecer los controles, hacer el seguimiento acorde con el diseño de los controles para evitar su materialización.
- Informar las materializaciones de los riesgos al Sistema de Gestión Integral (tercera línea de defensa).

8.3. Segunda línea de defensa.

8.3.1. Proceso Jurídico, Gerente Tics y Responsable de temas transversales para toda la entidad.

- Asegurar que los controles y procesos de gestión del riesgo de la primera línea de defensa sean apropiados y funcionen correctamente.
- Supervisar la implementación de prácticas eficaces para la gestión de los riesgos y para el diseño e implementación de controles.
- Evaluar y efectuar seguimiento a los controles aplicados por la 1ª línea de defensa.
- Realizar asesoría a la 1ª línea de defensa en la identificación de riesgos , el establecimiento de controles efectivos y la implementación de planes de tratamiento a los riesgos.
- Establecer los mecanismos para la autoevaluación sobre la gestión de los riesgos (seguimiento a través de herramientas objetivas, consolidación de informes de gestión).

8.4. Tercera línea de defensa.

8.4.1. Sistema de Gestión Integral.

- Monitorear y revisar de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgo.
- Realizar orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con los responsables de temas transversales.
- Realizar monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.
- Realizar asesoría proactiva y estratégica a la Alta Dirección y a los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos.
- Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.
- Informar los hallazgos sobre la gestión de riesgo y proporcionar recomendaciones de forma independiente.

9. DECLARACIONES.

Para asegurar el desarrollo de esta política, La Fundación Cataruben, establece los siguientes compromisos:

- Incorporar la gestión integral de riesgos en todos los procesos de la organización.
- Adoptar una metodología para la identificación, medición, tratamiento y monitoreo de los riesgos, que siga los lineamientos de las mejores prácticas establecidas.
- Identificar los riesgos relevantes, atendiendo a su posible impacto sobre los objetivos, el gobierno corporativo, la sostenibilidad y la continuidad de operaciones, teniendo en cuenta el contexto de Cataruben.

- Realizar con una periodicidad mínima anual una actualización de las matrices de riesgos, teniendo en cuenta las distintas fuentes de riesgo, sus eventos, causas y las situaciones que los generan.
- Monitorear en el Comité de Gestión de Riesgos el estado de los riesgos más importantes de la compañía, así como sus planes de mitigación y eventos materializados significativos.
- Realizar periódicamente análisis del entorno interno y externo que permita identificar generadores y tendencias que pueden potenciar la materialización de riesgos con impacto sobre el negocio.
- Revisar las escalas de valoración definidas con una periodicidad mínima anual, con base en los eventos materializados y los objetivos de la compañía que afecten los niveles de tolerancia al riesgo.
- Monitorear la evolución de los riesgos identificados en la compañía y el avance de los planes de acción implementados para su mitigación.
- Definir esquemas claros de reporte hacia la Asamblea General de Asociados y la alta dirección sobre el desempeño de la gestión de riesgos.
- Validar continuamente la idoneidad y eficacia del desempeño del Sistema de Gestión Integral de Riesgos, con base en las mejores prácticas sobre esta materia.
- Fomentar una cultura de gestión de riesgos con el fin de generar conciencia de autocontrol y responsabilidad frente al riesgo.
- Garantizar la independencia del área encargada de administrar el Sistema de Gestión Integral de Riesgos de las áreas de negocio que generan y gestionan los riesgos.
- Proveer los recursos requeridos por el Sistema de Gestión Integral de Riesgos para lograr su adecuada implementación y óptimo funcionamiento en la compañía.
- Implementar mecanismos y canales de información que permitan realizar una evaluación y comunicación periódica y transparente de los resultados del seguimiento a la gestión de riesgos.
- Implementar los planes de continuidad del negocio para mitigar el impacto de la materialización de los riesgos de Cataruben.

10. VIGENCIA, INTERPRETACIÓN Y MODIFICACIÓN DE LA POLÍTICA

La presente Política es aprobada por parte de la Asamblea General de Asociados de Cataruben, a través de Acta No. 48 del 27 de octubre de 2023 y reemplaza cualquier acuerdo, declaración, política, reglamento, afirmación, información y entendimiento previo sobre el objeto de la presente Política, bien sea escrita o verbal.

Control del Documento

Actualizó	Revisó	Aprobó
Ludy Pérez Líder Jurídico	**Marinela Camargo** Líder Control Operativo	**María Fernanda Wilches** Gerente General **Asamblea General**

Descripción cambio Versión
Versión 01. Elaboración (14/07/2021) Versión 02. Se realizó actualización en los riesgos que se van a detectar, se agregó los aspectos fundamentales para su implementación, actualización de la metodología para la gestión del riesgo de acuerdo a la normatividad actual, y los órganos vinculados a la fundación que ejercerán el control y gestión del riesgo en las línea estratégicas y líneas de defensas (26/08/2023).