TABLA DE CONTENIDO

1 INTRODUCCIÓN

Dentro de su actividad organizacional, **PROINDESA S.A.S Y SOCIEDADES ADMINISTRADAS**[1] **,** en adelante **"LA ORGANIZACIÓN"** siempre buscará asegurar una eficiente relación entre rentabilidad y riesgo en todas las posiciones tomadas, garantizando que el nivel de riesgo asumido este acorde con los objetivos y limites definidos por **LA ORGANIZACIÓN**.

La presente Política plantea los lineamientos, metodologías y etapas requeridas para la administración del Riesgo Operativo de la actividad empresarial de **LA ORGANIZACIÓN,** para fortalecer los mecanismos de control para la minimización de los riesgos operativos a los cuales pueda estar expuesta su operación. Establece estrategias claras, supervisión de la Junta Directiva o el máximo órgano de Dirección de la Organización, así como la Alta Dirección, una fuerte cultura interna de control y de riesgo operacional, entendida como un conjunto combinado de valores, actitudes, habilidades y conductas individuales y corporativas que determinan el estilo y compromiso de esta respecto de la administración del Riesgo Operacional.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer los lineamientos metodológicos, roles y responsabilidades de los actores claves para la Gestión del Sistema de Administración de Riesgo Operativo de **PROINDESA S.A.S y sus Administradas**.

Asimismo, esta Política está dirigida a todas las contrapartes vinculadas con **LA ORGANIZACIÓN** con las cuales se establezca una relación de negocio.

2.2 OBJETIVOS ESPECÍFICOS

- Impulsar a nivel institucional la cultura en materia de riesgo operativo.
- Evidenciar el deber de los órganos de administración, de control y de sus demás colaboradores, de asegurar el cumplimiento de las normas internas y externas relacionadas con la administración del riesgo operativo.
- Permitir la prevención y resolución de conflictos de interés en la recolección de información en las diferentes etapas del SARO, especialmente para el registro de eventos de riesgo operativo.

[1] En virtud del Acuerdo de Colaboración Empresarial suscrito entre Proindesa S.A.S y estas sociedades.

- Permitir la identificación de los cambios en los controles y los perfiles de riesgo.
- Desarrollar e implementar planes de continuidad del negocio.
- Dar a conocer el modelo de gobierno del Sistema de Administración de Riesgo Operativo Corporativo a ser adoptado por **LA ORGANIZACIÓN**.
- Establecer lineamientos que permitan empoderar el compromiso y responsabilidad de la gestión del riesgo en **LA ORGANIZACIÓN**, dando especial claridad a la primera línea de defensa (líderes de proceso) sobre la importancia de desarrollar sus procesos con una asertiva administración de riesgos.

3 ALCANCE

La aplicación del presente documento es responsabilidad de la Dirección de Riesgos, no obstante, es responsabilidad de todas las áreas de **LA ORGANIZACIÓN** conocer, acatar y aplicar las disposiciones legales vigentes, que les sean aplicables, así como las directrices establecidas en el presente documento.

4 DEFINICIONES

- **Evento:** Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.
- **Eventos de pérdida:** Son aquellos incidentes que generan pérdidas por riesgo operacional a la organización.
- **Clasificación de los riesgos operacionales:** Para los efectos de la presente Política los riesgos operacionales se clasifican de la siguiente manera:

    - **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 de la entidad.

      Dentro de esta categoría se incluyen las "Actividades no autorizadas", las cuales ocurren si se cumple con las siguientes circunstancias:

        - Se ha sido cometido por una persona vinculada a LA ORGANIZACIÓN.
        - Tiene el ánimo de obtener beneficio para sí mismo o para un tercero; (aunque el beneficio no se pueda asociar directamente a una ganancia económica).

- Se ha originado como consecuencia del incumplimiento de políticas, normas y procedimientos internos de la Organización y facultades o atribuciones otorgadas.
- No sea sancionable por los órganos jurisdiccionales.

Ejemplos de eventos:

- Actividad no Autorizada / Empleado desleal/Empleado Infractor
- Actividad orientada a subvaluar precios (Deliberado)
- Actividades criminales
- Colusión (Pacto Ilícito entre dos o más personas)
- Desfalco / Peculado
- Destrucción de activos
- Falseamientos contables
- Falsificaciones
- Fallas intencionales o datos errados de manera intencional.
- Fraude crediticio
- Fraudes empleados / malicia (criminal)
- Fraude por programación
- Fraudes con cheques (Falsificación / adulteración)
- Fraudes con otros documentos de control (Falsificación / adulteración)
- Hurto de información (con pérdida monetaria)
- Hurto y fraude
- Ignorar / pasar por alto procedimientos (Deliberado)
- Infidelidad de funcionarios
- Malversación de fondos
- Negociación con firmas comisionistas por fuera de la bolsa
- Pautas incorrectas (Deliberado)
- Pautas riesgosas
- Pérdida de posición (intencional)
- Robo -Físico
- Robo -Propiedad intelectual
- Sobornos
- Sustracciones (Hurto/robo)
- Tipo de transacciones no autorizadas
- Tomar posesión de cuentas / personalización de cuentas
- Transacciones no reportadas (intencional)
- Violación a derechos de confianza

- Violación a las normas ambientales
- Violación de límites (atribuciones)
- Violaciones de responsabilidad (uso inadecuado de datos confidenciales)
- Violaciones en la seguridad de TI

- **Fraude Externo:** Actos, realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes, en los que se encuentra implicado un tercero ajeno a la entidad.

  Ejemplos de eventos:

  - Amenaza de bomba
  - Asalto a mano armada
  - Asonada
  - Contrabando
  - Cuentas fraudulentas abiertas por clientes
  - Chantaje / Amenaza
  - Destrucción de activos
  - Documentos no apropiadamente elaborados
  - Errores en garantías (Deliberado)
  - Estafa
  - Evasión (voluntaria)
  - Extorsión
  - Falsificaciones
  - Fallas de contabilización o datos errados
  - Financiación del terrorismo
  - Fraude crediticio
  - Fraudes con tarjetas
  - Hostigamiento / Acoso
  - Huelga
  - Hurto y fraude
  - Incendio premeditado
  - Incumplimientos y evasiones de tipo fiscal y legal Infidelidad
  - Interpretación errada de leyes
  - Lavado de dinero
  - Lavado de dinero (Deliberado)
  - Pánico financiero
  - Perjuicios por hacking a los sistemas de información

- Pobre asesoría / soporte (incluso en inversiones/valores)
- Procesos de acuerdo de pago errado o inadecuado
- Propuestas inadecuadas de proyectos / planes
- Revolver / Confundir información (Churning)
- Robos
- Sabotaje a la reputación (Deliberado)
- Sabotajes
- Secuestro
- Suplantación de personas
- Tergiversación de leyes
- Terrorismo
- Terrorismo / bombas / guerra
- Violaciones a la seguridad de los Sistemas
- Violaciones en la seguridad de TI

- **Relaciones laborales y seguridad laboral:** 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.

Ejemplos de eventos:

- Actividades sindicales por fuera de la ley
- Ambiente de seguridad
- Ausencia de personal entrenado y adecuado
- Ausencia o pérdida de personal clave
- Compensación a trabajadores
- Contrataciones Inadecuadas
- Cualquier obligación derivada de un reclamo en general
- Destrucción maliciosa de activos
- Discriminación / igualdad oportunidades
- Discriminación laboral
- Incumplimientos de las leyes de seguridad y salud
- Incumplimientos de las relaciones laborales

- **Clientes, productos y 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 de la entidad como consecuencia de desastres naturales, actos de terrorismo, vandalismo u otros acontecimientos.

- **Fallas tecnológicas:** Hechos o cambios originados por fallas del hardware, software, telecomunicaciones o servicios públicos que puedan afectar, además de la operación interna de la entidad, la prestación del servicio a los clientes.

- **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.

- **Factores de Riesgo**: Se entiende por factores de riesgo las 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.

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

- **Internos**

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

    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 la entidad una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo.

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

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

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

- **Externos:** Son situaciones asociadas a la fuerza de la naturaleza u ocasionadas por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

- **Manual de Riesgo Operacional:** Es el documento contentivo de todas las políticas, objetivos, estructura organizacional, estrategias, los procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento del SARO.
- **Pérdida Bruta:** Se entiende una pérdida antes de recuperaciones de cualquier tipo.
- **Pérdida Neta:** Se entiende la 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.
- **Pérdidas:** Cuantificación económica de la ocurrencia de un evento de riesgo operacional, así como los gastos derivados de su atención.
- **Perfil de Riesgo:** Resultado consolidado de la medición permanente de los riesgos a los que se ve expuesta la entidad.
- **Plan de Contingencia**: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.
- **Plan de Continuidad del Negocio:** Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.
- **Riesgo inherente:** Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- **Riesgo legal:** Es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales.

  El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones. Aplica a todas las actividades e incluye a terceros que actúen en representación de la entidad respecto de los procesos y/o actividades tercerizadas.

- **Riesgo Operacional (RO):** Es la posibilidad de que la entidad 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 Residual:** Nivel resultante del riesgo después de aplicar los controles.
- **Sistema de Administración de Riesgo Operacional (SARO):** Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operacional, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operacional.
- **Tipos de Eventos de Riesgo:** Se clasifican en tres:

  - ✓ **Evento Tipo A:** Son los eventos que generan pérdida y afectan el estado de resultados.

  - ✓ **Evento Tipo B:** Son los eventos que generan pérdida y no afectan el estado de resultados.

  - ✓ **Evento Tipo C:** Son los eventos que no generan pérdidas y, por lo tanto, no afectan el estado de resultados de **LA ORGANIZACIÓN**.

5 MARCO DE REFERENCIA DE EVALUACIÓN DEL RIESGO OPERATIVO

El proceso de evaluación de la Alta dirección requiere que se utilice un *"Marco de control interno generalmente aceptado"*, que define los elementos que se espera estén presentes y funcionando en un sistema de control interno efectivo. En la evaluación de la efectividad, se evalúa si el control interno incluye políticas, procedimientos y actividades para cubrir los elementos que el marco de referencia describe.

Para el efecto, **LA ORGANIZACIÓN** adoptó por disposición de Grupo AVAL y Corficolombiana el COSO (Committee on Sponsoring Organizations of the Treadway Commission) como Marco de Control Interno para su evaluación, por considerar que el mismo es una buena práctica, mundialmente reconocida y se ajusta a tales requerimientos.

6 PRINCIPIOS

LA ORGANIZACIÓN acoge como suyos los siguientes principios sobre los cuales fundamenta y estructura su Sistema de Administración del Riesgo Operativo. Tales Principios son expresiones de la Alta Dirección para una presentación y valoración justa y transparente del

Riesgo Operativo, permitiendo la adecuada identificación de los controles a nivel de procesos para mitigar razonablemente los riesgos operativos identificados.

- **Adoptar y mantener una sólida cultura del riesgo operativo**

LA ORGANIZACIÓN propenderá por el establecimiento de una sólida cultura de gestión de riesgos operativos, apoyándose en directrices apropiadas para el buen comportamiento profesional y responsable de todos los colaboradores de la Compañía. En este sentido, es responsabilidad de la Administración de **LA ORGANIZACIÓN**, a través de la Dirección de Riesgos, el asegurar que exista una fuerte cultura de gestión del riesgo operativo.

- **Implementar y mantener un "Marco de Gestión del Riesgo Operativo**

El marco elegido para la gestión del riesgo es COSO 2013 el cual fue seleccionado por Grupo AVAL por una variedad de factores, incluyendo su naturaleza, magnitud, general aceptación por parte de los órganos de regulación tanto nacionales como internacionales.

- **Supervisión del modelo de riesgo operativo por parte de la Junta Directiva o quien haga sus veces y/o Comité de Auditoría.**

La Junta Directiva o quien haga sus veces y/o el Comité de Auditoría deben establecer, aprobar y revisar periódicamente el "Marco de Gestión del Riesgo Operativo". Así mismo, deben supervisar a la Administración para asegurar que las políticas, procesos y sistemas de información se aplican eficazmente en todos los niveles de decisión de **LA ORGANIZACIÓN**.

- **Determinación del apetito de riesgo operativo, del nivel de tolerancia y la capacidad de riesgo.**

La Junta Directiva o quien haga sus veces en **LA ORGANIZACIÓN** define el apetito de riesgo, el nivel de tolerancia y la capacidad máxima al riesgo, considerando para el efecto la naturaleza de sus operaciones; así como los niveles de riesgo operativo que está dispuesta a asumir en cada uno de los mismos. La Junta Directiva o quien haga sus veces en **LA ORGANIZACIÓN** debe aprobar el apetito de riesgo, el nivel de tolerancia y la capacidad máxima al riesgo tomando como referencia un porcentaje estimado sobre la utilidad neta, capital social o ingresos.

- **Compromisos de la Administración**

La Administración de **LA ORGANIZACIÓN** cuenta con una estructura de gestión del riesgo operativo clara y eficaz con líneas de responsabilidad bien definidas, transparentes y

coherentes, asignadas a la Dirección de Riesgos, siendo esta responsable de su implementación de forma consistente y de mantener en toda **LA ORGANIZACIÓN** políticas, procesos y sistemas para su gestión, que sean acordes con el apetito por el riesgo y los niveles de tolerancia asumidos.

- **Identificación, evaluación y control de riesgos operativos**

LA ORGANIZACIÓN asegura la identificación y evaluación del riesgo operativo que se encuentra presente en todos sus procesos (mapa de procesos).

Los riesgos se identificarán y evaluarán a nivel de proceso, los cuales tienen implícitas actividades, que consideran los siguientes puntos:

- Establecer un proceso para identificar y evaluar los riesgos susceptibles de materialización.
- Los procedimientos de evaluación de riesgos requieren, entre otras cosas, la obtención de una comprensión detallada del negocio y su entorno, así como de su sistema de Control Interno. De igual manera, dichos procedimientos deben permitir determinar la probabilidad de ocurrencia y el impacto de los potenciales eventos, así como los hallazgos por incumplimientos de los diferentes factores de riesgo.
- Establecer un enfoque de arriba hacia abajo. En otras palabras, no debe colocarse un énfasis indebido en la gestión de las pruebas de revisión de controles y otros controles de detección, sin considerar si se están abordando adecuadamente los riesgos con eventual impacto material en la cuenta contable asociada al proceso crítico.
- La metodología requiere, entre otros:

  ✓ Un seguimiento permanente para confirmar que no se han presentado cambios significativos en los procesos. La responsabilidad primaria recae sobre la primera línea de defensa (dueños de procesos).

  ✓ En general este es un compromiso permanente de todos los responsables o dueños de los procesos quienes deben informar a la Dirección de Riesgos de cambios significativos en los procesos que puedan afectar la evaluación de riesgos existente y su perfil.

  ✓ La primera línea de defensa debe garantizar coherencia entre lo documentado y como operan realmente los controles.

  ✓ Reforzar el entendimiento de los riesgos a través de:

- Las pruebas de controles realizadas por la tercera línea de defensa
- El monitoreo continúo realizada por la primera línea de defensa
- El seguimiento a los eventos de riesgo operativo realizado por la segunda línea de defensa.

Por lo tanto, la consideración principal en la evaluación adelantada por la tercera línea de defensa sobre el nivel de precisión está dada en función de si los controles están diseñados y operando para prevenir o detectar oportunamente errores básicos que podrían causar la no detección de un riesgo con potenciales efectos en los estados financieros y/o en la reputación de **LA ORGANIZACIÓN**:

- ✓ En la implementación del enfoque de control, el énfasis debe colocarse en los controles preventivos antes que en la gestión de controles detectivos.
- ✓ Para determinar la suficiencia del esquema de control, se debe considerar si los controles en forma individual o en combinación, son capaces de gestionar los riesgos.

- **Gestión de riesgos frente a la dinámica del negocio**

LA ORGANIZACIÓN se encarga de asegurar que hay un proceso de aprobación que evalúa plenamente el riesgo operativo para todos los nuevos procesos, actividades y/o sistemas que se implementen.

- **Seguimiento**

La ORGANIZACIÓN ha implementado un proceso para monitorear regularmente los perfiles de riesgo operativo y las exposiciones a pérdidas importantes.

- **Control y mitigación**

LA ORGANIZACIÓN cuenta con un "ambiente de control" que contempla un análisis de riesgos y un adecuado establecimiento de actividades de control estructurado mediante políticas, procesos, sistemas y controles internos adecuados.

- **Flexibilidad empresarial y continuidad**

La **ORGANIZACIÓN** define su plan de continuidad que le permitirá asegurar la capacidad de operar ante impactos materiales y/o reputacionales que afecten la disponibilidad de los procesos críticos del negocio y/o ante eventos que pongan en entredicho el giro ordinario de sus negocios.

7 RESPONSABLES DE LA IMPLEMENTACIÓN, DESARROLLO Y MONITOREO

La **ORGANIZACIÓN** estructura las funciones y responsabilidades en general frente a todos los riesgos, siguiendo el esquema de las tres líneas de defensa, esto es, considerando (i) la gestión por línea de negocio, (ii) la gestión de la Dirección de Riesgos, y (iii) la gestión de quien haga revisiones independientes de la administración.

7.1 PRIMERA LÍNEA DE DEFENSA

La primera línea de defensa la constituyen los procesos misionales y de apoyo que gestionan directa e indirectamente el negocio de **LA ORGANIZACIÓN**.

Esto significa que el gobierno del riesgo operativo reconoce que la gestión de la primera línea de negocio es la responsable de identificar, evaluar, gestionar y controlar los riesgos asociados a los procesos. Esta línea debe conocer y aplicar las políticas y procedimientos, así como disponer de los recursos suficientes para realizar eficazmente estas tareas. Para tal efecto, **LA ORGANIZACIÓN**:

- Específica y documenta claramente las políticas, procedimientos, riesgos y controles y los comunica a los colaboradores correspondientes, a través de la Dirección de Riesgos.

- Realiza la promoción del principio del autocontrol, asegurando que se tengan implementados y documentados en los procedimientos los controles para mitigar los riesgos a los que se encuentren expuestos.

- Incluye una descripción clara de las obligaciones de los colaboradores y de las instrucciones que deben seguir para cumplirlas.

- Dispone de políticas y procesos adecuados para seleccionar a su personal, presente y futuro, a fin de garantizar unos elevados principios éticos y profesionales, los cuales son reforzados a través de planes y programas de capacitación de modo que los colaboradores estén adecuadamente capacitados para aplicar las políticas y procedimientos de Riesgo Operativo.

Para tal fin, **LA ORGANIZACIÓN**, adapta la programación y contenido de la capacitación para el personal de las distintas áreas de acuerdo con las necesidades y riesgos de esta. Las necesidades de formación podrán variar dependiendo de las funciones de los colaboradores y de las responsabilidades de los distintos cargos.

7.2 SEGUNDA LÍNEA DE DEFENSA

La segunda línea de defensa asigna responsabilidades a la Dirección de Riesgos como la responsable de hacer un seguimiento continuo del cumplimiento de todas las obligaciones en materia de Riesgo Operativo de **LA ORGANIZACIÓN**. Esto implica hacer una verificación por muestreo del cumplimiento de la normatividad y un seguimiento a los informes de gestión (eventos) de manera que pueda comunicarlas a Alta dirección o a la Junta Directiva o quien haga sus veces y/o al Comité de Auditoría. Para el efecto, debe cuestionar a las áreas de negocio utilizando adecuadas herramientas de gestión del riesgo y realizando actividades de medición de este.

Los cumplimientos de los objetivos del negocio no deben oponerse en absoluto al eficaz desempeño de las atribuciones anteriormente mencionadas de la Dirección de Riesgos. Así mismo, para evitar discusiones sobre su independencia y permitir juicios ecuánimes y facilitar un asesoramiento imparcial a la Alta dirección de **LA ORGANIZACIÓN**, la Dirección de Riesgos no debe, por ejemplo, asumir competencias en los procesos misionales ni de apoyo del negocio, ni en el contexto de protección de datos o en la función de Auditoría Interna.

Ante cualquier conflicto entre los procesos de negocio y las atribuciones del Director de Riesgos, existen procedimientos que garantizan que los asuntos relacionados con el riesgo operativo reciban una consideración objetiva al más alto nivel.

7.3 TERCERA LÍNEA DE DEFENSA

La tercera línea de defensa juega un papel importante al evaluar de forma independiente la gestión y los controles del riesgo operativo, así como los procesos y sistemas de **LA ORGANIZACIÓN**, rindiendo cuentas a la Junta Directiva o quien haga sus veces y/o Comité de Auditoría, mediante evaluaciones periódicas de la eficacia del cumplimiento de las políticas y procedimientos de SARO.

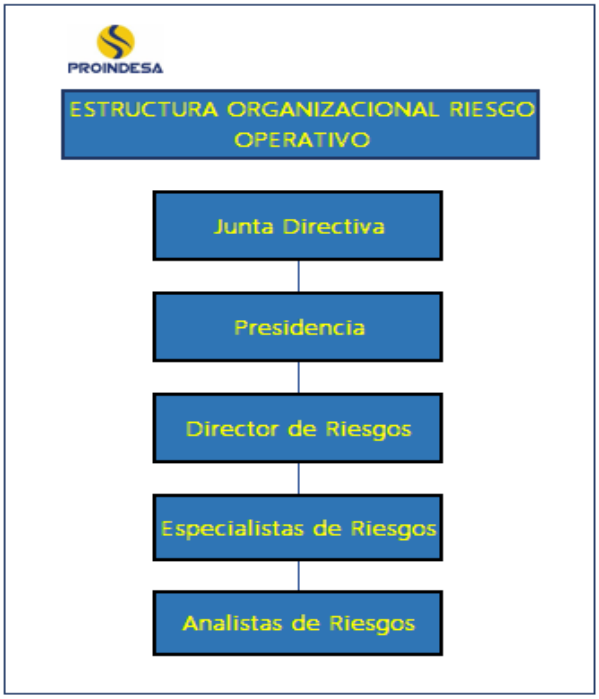
Las Auditorías Internas o externas realizan estas revisiones, ya que no participan en el desarrollo, implementación y operación de la estructura riesgo/control.

8 ESTRUCTURA ORGANIZACIONAL

Con el objetivo de asignar funciones y responsabilidades en relación con el Sistema de Administración de Riesgo Operacional, PROINDESA S.A.S establece los siguientes mecanismos:

8.1. Organigrama de Riesgo Operacional

El siguiente es el organigrama que representa las diferentes áreas que tienen responsabilidad con el Sistema de Administración de Riesgo Operacional en **LA ORGANIZACIÓN**.



La administración de riesgos operativos de **LA ORGANIZACIÓN** involucra a los diferentes procesos y/o áreas de la Compañía y a cada una se le asignan responsabilidades diferentes:

- **Junta Directiva o quien haga sus veces**

Las responsabilidades de éste, respecto a la aplicación de SARO son:

- ✓ Establecer las políticas relativas al SARO, así como su revisión y actualización periódica.
- ✓ Aprobar el Manual de Riesgo Operacional y sus actualizaciones.

- ✓ Hacer seguimiento y pronunciarse sobre el perfil de riesgo operacional de la entidad, así como de la cuantificación de los requerimientos de capital por dicho riesgo.
- ✓ Establecer las medidas relativas al perfil de riesgo operacional, teniendo en cuenta el nivel de tolerancia al riesgo de la entidad, fijado por la misma Junta Directiva o quien haga sus veces en la ORGANIZACION.
- ✓ Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente el Representante Legal.
- ✓ Pronunciarse sobre la evaluación periódica del SARO, que realicen los órganos de control.
- ✓ Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SARO.
- ✓ Aprobación de los planes de contingencia y de continuidad de negocio.

- **Representante Legal**

Se ocupará de:

- ✓ Someter a aprobación de la Junta Directiva o quien haga sus veces, la Política de Riesgo y el Manual de Riesgos Operativo.
- ✓ Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva o quien hagas sus veces.
- ✓ Adelantar el seguimiento permanente de las etapas y elementos constitutivos del SARO.
- ✓ Designar el área o cargo que actuará como responsable de la implementación y seguimiento del SARO – (Unidad de Riesgo Operacional).
- ✓ Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural que la administración de este riesgo implica para la entidad.
- ✓ Velar por la correcta aplicación de los controles del riesgo inherente, identificado y medido.
- ✓ Recibir y evaluar los informes que recibe de la Dirección de Riesgos.
- ✓ Velar porque se implementen los procedimientos para la adecuada administración del riesgo operacional a que se vea expuesta la entidad en desarrollo de su actividad.

✓ Presentación de informes periódicos, como mínimo semestralmente, a la Junta Directiva o quien haga sus veces, sobre la evaluación y aspectos relevantes del SARO, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable. Velar porque el registro de eventos de riesgo operacional cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida.

- **Dirección de Riesgos**

Tendrá entre sus funciones:

- ✓ Diseñar e implementación de la Política y el Manual de Riesgo Operativo.
- ✓ Definir los instrumentos, métodos y procedimientos tendientes a que la ORGANIZACION administre efectivamente sus riesgos operacionales, en concordancia con los lineamientos, etapas y elementos previstos en esta Política.
- ✓ Proponer nuevas y mejoras a políticas o procedimientos que permitan una gestión y control adecuado de los riesgos operativos.
- ✓ Ejecutar la implementación de los lineamientos corporativos que en materia de Riesgos Operativos emita su casa matriz y Grupo AVAL.
- ✓ Desarrollar e implementar el sistema de reportes, internos y externos, del riesgo operacional de la organización.
- ✓ Administrar el registro de eventos de riesgo operacional.
- ✓ Coordinar la recolección de la información para alimentar el registro de eventos de riesgo operacional.
- ✓ Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los riesgos operacionales medidos.
- ✓ Establecer y monitorear el perfil de riesgo operativo de la ORGANIZACIÓN e informarlo al órgano correspondiente.
- ✓ Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con el SARO y proponer sus correspondientes actualizaciones y modificaciones.
- ✓ Asegurar que los procedimientos contemplen una adecuada administración, gestión y control de los riesgos operativos.
- ✓ Desarrollar los modelos de medición del riesgo operacional.
- ✓ Implementar Programas de capacitación en SARO para todos los colaboradores de PROINDESA S.A.S

- ✓ Evaluar los informes que presente la Auditoría referentes a SARO.
- ✓ Apoyar a los dueños de procesos en la identificación, evaluación, monitoreo y control de los sus riesgos operativos.
- ✓ Realizar seguimiento a los controles adoptados para mitigar el riesgo inherente, con el objetivo de evaluar su efectividad.
- ✓ Reportar semestralmente al Representante Legal de la ORGANIZACIÓN la evolución del riesgo, los controles implementados y el monitoreo que se realice sobre el mismo.
- ✓ Recomendar a los dueños de proceso la conveniencia o necesidad de modificar los procedimientos y controles o bien la implementación de otros nuevos, con el fin de mejorar el nivel de control de los riesgos identificados.
- ✓ Garantizar la integridad, confiabilidad, cumplimiento, disponibilidad, eficiencia, efectividad y confidencialidad en el registro de eventos de riesgo operativo.

- **Auditoría Interna**

Sin perjuicio de las funciones asignadas en otras disposiciones a la Auditoría Interna, o quien ejerza el control interno, ésta debe evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SARO con el fin de determinar las deficiencias y sus posibles soluciones. Así mismo, debe informar los resultados de la evaluación a la Dirección de Riesgos de PROINDESA S.A.S y al Representante Legal de la ORGANIZACIÓN

También debe realizar una revisión periódica del registro de eventos de riesgo operacional e informar al Representante Legal de la ORGANIZACIÓN sobre el cumplimiento de las condiciones señaladas en el registro de eventos del riesgo operacional.

- **Responsabilidades generales de todas las áreas**

Dentro de la estructura organizacional y responsabilidades definidas para una adecuada gestión de SARO, es importante considerar el hecho de que los eventos de riesgo pueden afectar a todas las áreas de la ORGANIZACIÓN, por lo que los dueños de procesos asumen responsabilidades sobre la gestión sobre los riesgos operativos de los procesos a su cargo. Asimismo, tendrán las siguientes responsabilidades:

- ✓ Conocer y cumplir las políticas y procedimientos correspondientes a su operativa, y concretamente las relativas a la gestión y control del riesgo operativo.
- ✓ Identificar todos los riesgos operativos, de acuerdo con la metodología definida.
- ✓ Implementar de medidas correctivas para mitigar o eliminar riesgos operativos.
- ✓ Proporcionar toda la información necesaria frente a los eventos de riesgo operativos identificados.
- ✓ Fomentar la cultura de administración del riesgo al interior de sus equipos de trabajo.

9 ESTRATEGIA EN LA GESTIÓN DEL RIESGOS OPERATIVO

9.1 IDENTIFICACIÓN

La identificación de los riesgos se realiza con base en los siguientes factores: Entorno, personas, procesos y tecnología.

Consiste en reconocer y determinar las causas (factores de riesgo) y riesgos inherentes a los procesos de **LA ORGANIZACIÓN**, es decir, el riesgo puro sin el efecto del control, que impedirían la consecución de los objetivos propios del negocio.

9.2 MEDICIÓN O EVALUACIÓN

9.2.1 Evaluación del riesgo inherente

El riesgo inherente mide el impacto sin tener en cuenta los controles existentes u otros factores mitigantes. El análisis del riesgo inherente facilita el análisis de los diferentes controles existentes e identifica riesgos potenciales que podrían convertirse en reales si el control establecido falla o es eliminado.

La evaluación del riesgo inherente es realizada por los Dueños de Procesos con el acompañamiento del equipo de la Dirección de Riesgos.

9.2.2 Evaluación del riesgo residual

El riesgo residual es aquel riesgo que existe una vez considerados todos los controles y otros factores de mitigación implementados. El riesgo residual se evalúa en términos cuantitativos y cualitativos.

Este proceso se realiza a través de talleres en los que participan los Dueños de Proceso (responsables de los riesgos y controles) con la colaboración de la Dirección de Riesgos, así como otros expertos con el nivel técnico y conocimiento adecuado de ser requerido.

La estimación del riesgo residual se realiza en términos de frecuencia y severidad, del mismo modo que el riesgo inherente.

9.3 ACEPTACIÓN / MITIGACIÓN DEL RIESGO

La Junta Directiva, debe determinar si el nivel de riesgo es adecuado o si es necesario mitigarlo por medio de controles o acciones adicionales. La decisión de mitigar el riesgo se basará en la estrategia de **LA ORGANIZACIÓN**, el apetito de riesgo y el análisis coste/beneficio. Si se decide que el riesgo se debe mitigar, implicará la creación de un plan de acción.

9.4 TRATAMIENTO: ACCIONES CORRECTIVAS / MEDIDAS MITIGADORAS

Las Acciones Correctivas / Medidas Mitigadoras pueden ser identificadas en el propio proceso de gestión del Riesgo Operativo (a través del análisis de la base de eventos, de los Indicadores y del ejercicio de la Dirección de Riesgos, pero también pueden ser identificadas en procesos de control externos ejercidos por la Contraloría de Corficolombiana, Revisoría Fiscal o cualquier Ente de control.

Las acciones de mitigación son responsabilidad de cada área de **LA ORGANIZACIÓN** quienes de ser requerido cuentan con el acompañamiento de la Dirección de Riesgos**,** la implantación de las acciones debe obedecer, a un criterio de costo-beneficio y estar en consonancia con el perfil de riesgo establecido por **LA ORGANIZACIÓN**.

Una vez efectuada esta evaluación obtenemos la cobertura del riesgo que se obtiene con el control. Lo anterior ayudará a determinar la valoración final del riesgo teniendo en cuenta el efecto de los controles (riesgo residual) y el paso a seguir con dicho nivel de riesgo.

Con el fin de disminuir la probabilidad de ocurrencia y el impacto del riesgo en caso de materializarse, se busca en esta etapa definir los controles y las medidas de prevención, teniendo en cuenta las diferentes alternativas de tratamiento existentes y desarrollando los siguientes aspectos:

- Establecer metodología para definir medidas de control
- Implementar las medidas de control
- Determinar las medidas que aseguren la continuidad del negocio
- Determinar perfil de riesgo residual individual y consolidado

9.5 MONITOREO

El monitoreo comprende la realización de un proceso continuo de revisión es esencial para una gestión de riesgos proactiva, reevaluando los riesgos y monitoreando la situación de los tratamientos y controles implementados, para lo cual se deben desarrollar los siguientes aspectos:

- Desarrollar proceso de seguimiento efectivo.
- Establecer indicadores descriptivos y/o prospectivos
- Validar que los controles sean efectivos conforme a la definición de efectividad.
- Validar en las matrices de riesgos, que el riesgo residual se encuentra dentro de los niveles de aceptación establecidos por la entidad.

10 CAPACITACIÓN

Cada colaborador de **LA ORGANIZACION** debe concientizarse del riesgo operativo presente en sus actividades y empezar a administrarlo iniciando por las funciones que desempeña y así fortalecer una cultura de gestión de riesgos.

Esta cultura organizacional, se encuentra soportada en la observancia la Política de Riesgo Operativo, el Código de Buen Gobierno, la Política Anticorrupción, Manual SAGRLAFT, Política de Seguridad de la Información y Ciberseguridad, así como la aplicación de Código de Ética y Conducta y la adecuada ejecución de los procedimientos dispuestos por **LA ORGANIZACIÓN** y las capacitaciones de riesgo operativo que brinde la Dirección de Riesgos.

10.1 DIVULGACIÓN

En línea con lo anterior, la divulgación debe incluir:

- La Política de Riesgo Operativo deben ser socializados a todos los colaboradores de **LA ORGANIZACIÓN**.
- Se debe garantizar que el mapa de riesgos operativos de cada proceso sea de fácil acceso y de conocimiento de los colaboradores de **LA ORGANIZACIÓN** que tienen responsabilidades sobre la aplicación de los controles.
- Los mapas de Riesgo Operativo se deben actualizar cada vez que existan riesgos asociados a cambios o nuevos procesos, o programas de tecnología, o en los controles definidos.

- La copia de los mapas de riesgos debe reposar en el servidor NAS de **LA ORGANIZACIÓN** y deben encontrarse disponibles para los órganos de control y vigilancia internos y externos cuando estos lo requieran.

11 CONTROLDE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	01/08/2017	- Creación del documento
2	03/ 11/2020	- Actualización de lineamientos basados en la normatividad del Grupo Aval y Corficolombiana. - Incorporación de la estructura organizacional de la Administración de Riesgo Operativo. - Revisión general del documento.

12 FIRMAS DE REVISIÓN Y APROBACIÓN

Elaborador por:	Revisado por:	Aprobado por:
FIRMADO EN ORIGINAL	**FIRMADO EN ORIGINAL**	**FIRMADO EN ORIGINAL**
ASISTENTE DE PROCESOS	**DIRECTOR DE RIESGOS**	**VICEPRESIDENTE FINANCIERA Y ADMINISTRATIVA**
Lilian Alexandra Arriero	Margarita Ramírez	Vanessa Garay Guzmán