

**INFORMACIÓN GENERAL DEL DOCUMENTO**

<b>Código:</b>	DG-0203/03	<b>Nombre del documento:</b>	POLÍTICA DE RIESGO OPERACIONAL
<b>Versión</b>	3	<b>Fecha de Vigencia</b>	24/10/2025
<b>Descripción del lineamiento</b>	En cumplimiento de los memorandos PD-MEN-PR-038-2025, PD-MEN-PR-058-2025 y PD-MEN-VP-001-2026 de Proindesa S.A.S., los cuales establecen las directrices para la adopción de las políticas corporativas, se adopta la POLÍTICA DE RIESGO OPERACIONAL.		

**INFORMACIÓN DE NO APLICABILIDAD POLÍTICA O LINEAMIENTO**

Numeral	Descripción	Justificación de no aplicabilidad
3.	Definiciones	Concesionaria Panamericana S.A.S. cuenta con un glosario de riesgos operacionales adecuado a las características propias de la compañía.
4.	Normatividad aplicable	La normatividad nacional relacionada en este numeral no es aplicable a Panamericana.
7.	Documentos de referencia y anexos	Se aplicarán los procedimientos y formatos propios de Panamericana.

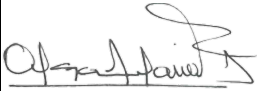
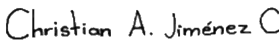
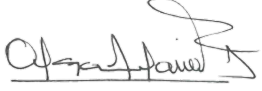
**IDENTIFICACIÓN DE CONTROLES NO APLICABLES**

Control	Numeral de ubicación	Justificación de no aplicación

**PROCESOS ALCANZADOS SOX NO APLICABLES O NORMATIVAS NO APLICABLES**

Proceso o Normativa	Justificación de no aplicación
N/A	N/A

**RESPONSABLES DE LA VALIDACIÓN**

Área de Gobierno, Riesgos y Cumplimiento		Área de Calidad, Procesos o equivalente		Área con mayor injerencia procesal	
<b>Firma:</b>		<b>Firma:</b>		<b>Firma:</b>	
<b>Nombre:</b>	OLGA LUCIA AFANADOR MARIN	<b>Nombre:</b>	CHRISTIAN ALEJANDRO JIMENEZ CORTES	<b>Nombre:</b>	OLGA LUCIA AFANADOR MARIN
<b>Cargo:</b>	COORDINADORA GRC	<b>Cargo:</b>	LIDER DE DESARROLLO ORG.	<b>Cargo:</b>	COORDINADORA GRC

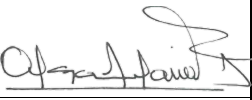
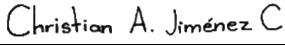
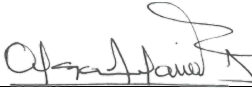
**INFORMACIÓN GENERAL DEL DOCUMENTO**

<b>Código:</b>	DG-0203/03	<b>Nombre del documento:</b>	POLÍTICA DE RIESGO OPERACIONAL
<b>Versión</b>	3	<b>Fecha de Vigencia</b>	24/10/2025
<b>Descripción del lineamiento</b>	En cumplimiento de los memorandos PD-MEN-PR-038-2025, PD-MEN-PR-058-2025 y PD-MEN-VP-001-2026 de Proindesa S.A.S., los cuales establecen las directrices para la adopción de las políticas corporativas, se adopta la POLÍTICA DE RIESGO OPERACIONAL.		
<b>Proceso(s) Alcanzado(s) con la Política</b>	Todos los procesos de Panamericana.		

**INFORMACIÓN DE EQUIVALENCIA**


Cargo relacionados en el documento	Equivalencia funcional interna	Justificación de la equivalencia
Área de Riesgo y Cumplimiento	Coordinación de Gobierno, Riesgo y Cumplimiento	Estructura organizacional aprobada para Concesionaria Panamericana.
Presidencia	Gerencia General	Estructura organizacional aprobada para Concesionaria Panamericana.
Vicepresidencias	Direcciones de área	Estructura organizacional aprobada para Concesionaria Panamericana.
Gerencia Jurídica	Dirección Jurídica	Estructura organizacional aprobada para Concesionaria Panamericana.
Vicepresidente Ejecutiva y de Sostenibilidad o Gerente Administrativo y Financiero	Gerente General	Estructura organizacional aprobada para Concesionaria Panamericana.
Auditoría Interna	Auditoría de Corficolombiana y Proindesa	Estructura organizacional aprobada para Concesionaria Panamericana.
Unidad de Riesgo Operacional	Coordinación de Gobierno, Riesgo y Cumplimiento	Estructura organizacional aprobada para Concesionaria Panamericana.
Estructura de Responsabilidad Frente a la Política en la Organización	Se homologa a la estructura organizacional de Panamericana.	Estructura organizacional aprobada para Concesionaria Panamericana.

**RESPONSABLES DE LA VALIDACIÓN**

Área de Gobierno, Riesgos y Cumplimiento		Área de Calidad, Procesos o equivalente		Área con mayor injerencia procesal	
<b>Firma:</b>		<b>Firma:</b>		<b>Firma:</b>	
<b>Nombre:</b>	OLGA LUCIA AFANADOR MARIN	<b>Nombre:</b>	CHRISTIAN ALEJANDRO JIMENEZ CORTES	<b>Nombre:</b>	OLGA LUCIA AFANADOR MARIN
<b>Cargo:</b>	COORDINADORA GRC	<b>Cargo:</b>	LIDER DE DESARROLLO ORGANIZACIONA	<b>Cargo:</b>	COORDINADORA GRC

**TABLA DE CONTENIDO**

<b>1. OBJETIVOS.....</b>	<b>2</b>
<b>2. ALCANCE.....</b>	<b>2</b>
<b>3. DEFINICIONES .....</b>	<b>2</b>
<b>4. NORMATIVIDAD APLICABLE.....</b>	<b>3</b>
<b>5. DIRECTRICES Y LINEAMIENTOS GENERALES .....</b>	<b>4</b>
<b>6. AMBIENTE DE CONTROL.....</b>	<b>5</b>
<b>7. DOCUMENTOS DE REFERENCIA Y ANEXOS .....</b>	<b>15</b>
<b>8. CONTROL DE CAMBIOS.....</b>	<b>16</b>
<b>9. FIRMAS DE REVISIÓN Y APROBACIÓN.....</b>	<b>16</b>

	<b>POLÍTICA DE RIESGO OPERACIONAL</b>	<b>Página 2 de 16</b>
		<b>Versión: 03</b>
		<b>Fecha: 24/10/2025</b>

## 1. OBJETIVOS

### 1.1. Objetivo General

Establecer los lineamientos metodológicos, roles y responsabilidades de los actores claves para la Gestión del Sistema de Administración de Riesgo Operacional.

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

### 1.2. Objetivos Específicos

- Formular los principios y políticas generales del Riesgo Operacional.
- Impulsar a nivel institucional la cultura en materia de riesgo operacional.
- Evidenciar el deber de los órganos de administración, de control y de sus demás funcionarios, de asegurar el cumplimiento de las normas internas y externas relacionadas con la administración del riesgo operacional.
- 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 operacional.
- 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 Operacional 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 (líderes o dueños de proceso) sobre la importancia de desarrollar sus procesos con una asertiva administración de riesgos.

## 2. ALCANCE

Aplica para Proindesa, Sociedades Administradas, Concesionarias y Constructoras según les aplique (en adelante la Organización). La aplicación del presente documento es responsabilidad del Área de Riesgo y Cumplimiento, no obstante, es responsabilidad de todas las áreas y dueños de procesos de la Organización conocer, acatar y aplicar las disposiciones legales vigentes, que les sean aplicables, así como las directrices establecidas en el presente documento.

## 3. DEFINICIONES

Los términos y definiciones relacionados en este documento están detallados en el *Glosario Gestión de Riesgos F-0286*, el cual proporciona referencia estructurada de las definiciones para facilitar la comprensión y aplicación de los conceptos fundamentales al procedimiento. Los términos aplicables son:

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Alineados con el compromiso de la Organización con el cuidado del medio ambiente, este documento no deberá ser impreso. Las copias físicas son consideradas como copias no controladas.

**Código: DG-0203/03**

- Acontecimientos externos
- Alta Dirección
- Ambiente de control
- Análisis de riesgos
- Apetito de Riesgo
- Base de Eventos de Riesgo Operacional y de Alto Impacto
- Clasificación de los riesgos operacionales
- Clientes, productos y prácticas empresariales
- Control (Actividad de control)
- Control correctivo
- Control del Riesgo
- Control detectivo
- Control preventivo
- Daños a activos fijos
- Dueño o líder de proceso
- Ejecución y administración de procesos
- Entes de Control Corporativos
- Evento de pérdida
- Evento de Riesgo Operacional (ERO)
- Factores de riesgo
- Fallas tecnológicas
- Fraude externo
- Fraude interno
- Identificación de riesgos
- Impacto/severidad
- Infraestructura
- Líneas operativas
- Mapa Térmico o Mapa de Calor
- Materialización
- Matriz de riesgos (Matriz ERM)
- Medición de Riesgos
- Mitigar
- Monitoreo de riesgos
- NAS (Network Attached Storage)
- Normatividad
- Pérdida bruta
- Pérdida neta
- Pérdidas
- Perfil de riesgo
- Plan de acción correctivo
- Plan de acción preventivo
- Plan de contingencia
- Plan de continuidad del negocio
- Primera Línea
- Probabilidad/frecuencia
- Procesos
- Recurso Humano
- Relaciones laborales y seguridad laboral
- Riesgo
- Riesgo inherente
- Riesgo legal
- Riesgo Operacional (RO)
- Riesgo residual
- Segunda Línea
- Sistema de administración de riesgo operacional (SARO)
- Subproceso
- Tecnología
- Tercera Línea
- Tipos de eventos de Riesgo
- Unidad de Riesgo Operacional

#### **4. NORMATIVIDAD APLICABLE**

##### **4.1. Regulación Nacional Aplicable:**

- Capítulo XXIII - Circular Básica Contable y Financiera (CE 100/95) Superintendencia Financiera de Colombia.
- Circular Básica Jurídica 029 de 2014, Superintendencia Financiera de Colombia.
- Circular Básica Jurídica 025 de 2020, Superintendencia Financiera de Colombia

#### **4.2. Regulación Internacional Aplicable:**

- Acuerdo de Basilea II
- Norma ISO 31000:2018

#### **5. DIRECTRICES Y LINEAMIENTOS GENERALES**

- 5.1.** La gestión del riesgo forma parte integral de las responsabilidades de la Alta Dirección, lo que se traduce en una fuerte cultura de control, el conocimiento de los riesgos y el propio estilo de administración.
- 5.2.** La Alta Dirección, a todos los niveles, es responsable de gestionar, controlar, y mitigar los riesgos operacionales en sus áreas de responsabilidad.
- 5.3.** El control del Riesgo Operacional, de forma independiente a la propia gestión, tiene por objeto facilitar la identificación, evaluación, el seguimiento del grado de gestión, la mitigación, y en su caso la medición de los riesgos Operacionales, utilizando para ello herramientas cualitativas y cuantitativas de diferente naturaleza.
- 5.4.** La administración del Riesgo Operacional estará a cargo del Área de Riesgo y Cumplimiento, debido a la necesaria segregación de funciones y a la especialización que se requiere para ejecutarlas.
- 5.5.** Todos los funcionarios de la Organización están en la obligación de participar en las diferentes etapas del SARO, particularmente en la recolección de la información.
- 5.6.** Es de obligatorio cumplimiento por parte de todos los funcionarios de la Organización, todas las políticas, procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento del Sistema de Administración del Riesgo Operacional (SARO).
- 5.7.** Las funciones y responsabilidades que se relacionan con la gestión y control del Riesgo Operacional deben ser entendidas por la Alta Dirección y por todos los niveles, y deben incluirse dentro de los objetivos individuales que forman parte de la evaluación anual de desempeño.
- 5.8.** Todos los funcionarios deben conocer los riesgos operacionales de su responsabilidad; así mismo, su eficacia en la gestión y control de estos riesgos debe formar parte de la evaluación de desempeño anual.
- 5.9.** Todos los funcionarios deben reportar al Área de Riesgo y Cumplimiento (Unidad de Riesgo Operacional) los eventos de riesgo que resulten en su actividad laboral o los que se presenten en su área de trabajo. Los mecanismos para realizar este reporte estarán a cargo del Área de Riesgo y Cumplimiento.
- 5.10.** Todos los procesos y procedimientos aplicables a la gestión de riesgo operacional deben estar referenciados en el contenido de la presente política la cual constituye un marco general para la ejecución de actividades. La documentación detallada de dichos procesos deberá consultarse en los documentos específicos, los cuales se encuentran disponibles para la consulta de todos los funcionarios.
- 5.11.** La implementación del Plan de Continuidad de Negocio es imprescindible, de forma que se puedan llevar a cabo todos los procesos operacionales en caso de situaciones extremas. Dicho plan debe contar con las pruebas necesarias para confirmar su eficacia y eficiencia.

- 5.12. Deben existir herramientas cualitativas y cuantitativas que permitirán identificar, medir, controlar y monitorear los riesgos Operacionales.
- 5.13. La divulgación de la información forma parte esencial en el sistema de Administración de Riesgo Operacional, por lo tanto, el Área de Riesgo y Cumplimiento será la encargada de establecer funciones, responsabilidades y el medio adecuado por los cuales se dará a conocer toda la información que resulte en la gestión.

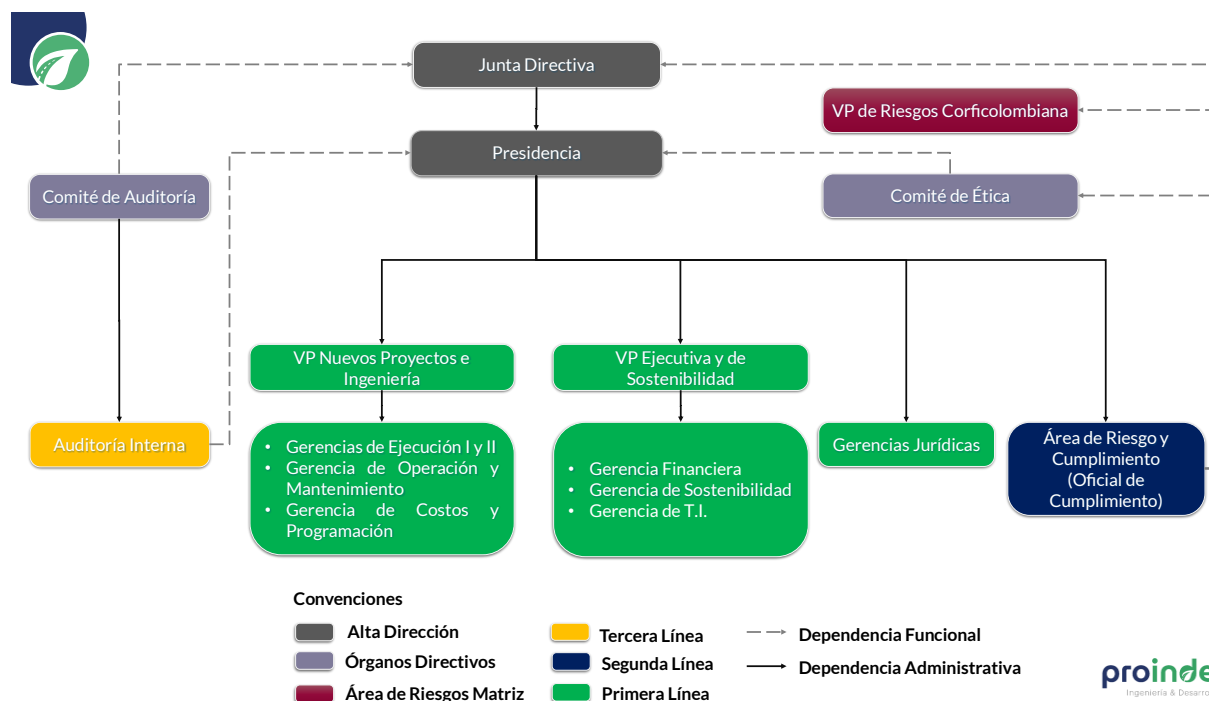
## 6. AMBIENTE DE CONTROL

### 6.1. Declaración de Compromiso

La Organización, está comprometida con la adopción de la presente política con base en el fortalecimiento de la cultura de riesgo operacional en todos sus niveles, promoviendo así la implementación de un sistema de gestión que apoye en la consecución de sus objetivos.

Por lo anterior, todas las áreas de la Organización son responsables de aplicar los criterios definidos en esta política, así como, informar y/o reportar oportunamente los eventos operacionales y de alto impacto de los que pueda llegar a tener conocimiento.

### 6.2. Estructura de Responsabilidad Frente a la Política en la Organización



La administración de los riesgos operacionales de la Organización involucra a los diferentes procesos y/o áreas, y a cada una se le asignan responsabilidades diferentes, tal como se describe a continuación:

- **Junta Directiva o Asamblea de Accionistas<sup>Δ</sup>**

Como ente máximo de control su función principal es aprobar políticas y límites que permitan una adecuada gestión de riesgos operacionales. Está en la obligación de conocer los resultados obtenidos y los riesgos asumidos en la operación de la Organización.

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

- ✓ Establecer las políticas relativas al SARO, así como su revisión y actualización periódica.
- ✓ 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.
- ✓ 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.

- **Vicepresidente Ejecutiva y de Sostenibilidad o Gerente Administrativo y Financiero<sup>Δ</sup>**

Tiene la responsabilidad de la gestión de riesgo operacional asumida por la Organización, para lo cual se ocupará de:

- ✓ Diseñar y someter a aprobación de la Junta Directiva o quien haga sus veces en la Organización, la Política de Riesgo de Riesgos Operacional y sus actualizaciones.
- ✓ Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva o quien haga sus veces en la Organización.
- ✓ 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 – (Área de Riesgo y Cumplimiento).
- ✓ 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 Organización.
- ✓ Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por la Junta Directiva o quien haga sus veces en la Organización.
- ✓ Velar por la correcta aplicación de los controles del riesgo inherente, identificado y medido.
- ✓ Verificar los informes que recibe del Área de Riesgo y Cumplimiento.

<sup>Δ</sup> O quien haga sus veces según la estructura organizacional en cada concesión y constructora

- ✓ Velar porque las etapas y elementos del SARO se implementen de acuerdo con lo definido en el presente documento.
- ✓ 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.
- ✓ Presentar el informe periódico preparado por el Área de Riesgo y Cumplimiento, semestralmente a la Junta Directiva o quien haga sus veces en la Organización, sobre la evolución y aspectos relevantes del SARO, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.

- **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 o líderes de procesos quienes actuarán bajo el rol de la Primera Línea asumen responsabilidades sobre la gestión sobre los riesgos operacionales de los procesos a su cargo como gestores del negocio. 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 operacional.
- ✓ Gestionar los riesgos operacionales de los procesos a cargo, de acuerdo con la metodología definida en el documento P-0217 Procedimiento para la identificación, Medición, Control y Monitoreo de los Riesgos Operacionales.
- ✓ Implementar medidas correctivas para mitigar o eliminar riesgos operacionales.
- ✓ Gestionar los planes de acción establecidos a partir del registro de eventos y resultados del monitoreo del perfil de riesgos del proceso.
- ✓ Proporcionar toda la información necesaria frente a los eventos de riesgo operacionales identificados.
- ✓ Recibir la Información periódica elaborada por el área de Riesgo y Cumplimiento para su seguimiento, análisis, y toma de decisiones.
- ✓ Participar en el desarrollo de proyectos de su respectiva área que impliquen Riesgo Operacional.
- ✓ Fomentar la cultura de administración del riesgo al interior de sus equipos de trabajo.

- **Área de Riesgo y Cumplimiento (Unidad de Riesgo Operacional)**

Como parte de la segunda línea, tiene entre sus responsabilidades lo siguiente:

- ✓ Diseñar y realizar seguimiento al cumplimiento de la Política de Riesgo Operacional.
- ✓ Definir los instrumentos, metodologías y procedimientos tendientes a que la Organización 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 operacionales.

- ✓ Ejecutar la implementación de los lineamientos corporativos que en materia de Riesgos operacionales emita la 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 y de Alto impacto.
- ✓ Coordinar la recolección de la información para alimentar el registro de eventos de riesgo operacional y de alto impacto y velar porque el registro cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida.
- ✓ Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los riesgos operacionales medidos.
- ✓ Establecer y monitorear el perfil de riesgo operacional 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 operacionales.
- ✓ Desarrollar los modelos de medición del riesgo operacional.
- ✓ Implementar los programas definidos de capacitación en SARO para todos los funcionarios de la Organización.
- ✓ Evaluar los informes que presente la Auditoría referentes a SARO.
- ✓ Apoyar a los dueños o líderes de procesos en la identificación, medición, monitoreo y control de los sus riesgos operacionales.
- ✓ 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 y en general el desempeño del sistema.
- ✓ Recomendar a los dueños o líderes 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.

- **Oficial de Riesgo Operacional**

Persona designada del área de Riesgo y Cumplimiento con el propósito de cumplir con la siguiente responsabilidad:

- ✓ Registrar eventos de riesgo operacional que se presenten en los procesos del área de Riesgo y Cumplimiento e informar al Líder de Riesgo y Cumplimiento<sup>A</sup> para su conocimiento, análisis y toma de decisiones.

<sup>A</sup> O quien haga sus veces según la estructura organizacional en cada concesión y constructora

- **Auditoría Interna**

La Auditoría Interna, quien actúa bajo el rol de la Tercera Línea, es un área independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de la Organización. Ayuda a la Organización a cumplir sus objetivos aportando en un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

Sin perjuicio de las funciones asignadas en otras disposiciones a la Auditoría Interna, o quien ejerza el control interno, ésta deberá 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, deberá informar los resultados de la evaluación del Área de Riesgo y Cumplimiento y al Representante Legal de la Organización.

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.

Debe brindar servicios de aseguramiento que comprenden la evaluación objetiva de las evidencias, efectuada para proporcionar una opinión o conclusión independiente respecto de un proceso, sistema u otro asunto. La naturaleza y el alcance del trabajo de aseguramiento están determinados por el auditor interno

No son funciones de la Auditoría:


- Establecer el apetito de riesgo.
- Imponer procesos de gestión de riesgo operacional.
- Manejar el aseguramiento sobre los riesgos.
- Tomar decisiones en respuesta a los riesgos.
- Implementar respuestas a riesgos a favor de administración

### **6.3. 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, esto es, considerando:

- (i) La gestión por cada línea de negocio
- (ii) La gestión de Área de Riesgo y Cumplimiento,
- (iii) La gestión de quien haga revisiones independientes de la administración<sup>1</sup>.

<sup>1</sup> Nuevo Código País: Medida o. 29: Monitoreo de la Arquitectura de Control. "Leveraging CO O Across the Three Lines of offense", 7 de Julio de 2015, COSO en colaboración con el Instituto de Auditores Internos, publicó este documento, Usando/aprovechando COSO a través de tres líneas ; documento que presenta cómo las responsabilidades y funciones relacionadas a la administración y control de riesgos pueden ser asignadas y coordinadas, con el fin de minimizar los vacíos controles y la duplicación de actividades y responsabilidades dentro de una Organización para el cumplimiento de los objetivos establecidos

	<b>POLÍTICA DE RIESGO OPERACIONAL</b>	Página 10 de 16
		Versión: 03
		Fecha: 24/10/2025

#### 6.4. Estrategia en la Gestión de Riesgo Operacional

Para un desarrollo continuo y una gestión apropiada del Sistema de Administración de Riesgo Operacional, la Organización ha definido un modelo el cual tiene como objetivo dar a conocer las metodologías y herramientas de gestión SARO para el fortalecimiento y logro de un sistema de administración de riesgo sostenible.

La metodología establecida por la Organización para la administración del Riesgo Operacional el cual se fundamenta en un proceso de cuatro etapas: *Identificación, Medición, Control y Monitoreo*, las cuales, a su vez, deben cumplir con unos pasos para su debida implementación. En el Anexo No 1. Modelo de Gestión de Riesgo Operacional se definen los lineamientos metodológicos y en el documento *Procedimiento para la identificación, Medición, Control y Monitoreo de los Riesgos Operacionales P-0217*, se encuentran las actividades a realizar para la adecuada ejecución de cada una de las etapas.

Este proceso se actualiza por lo menos una vez al año o cuando circunstancias especiales ocurran, como, por ejemplo, un cambio en las condiciones del mercado que impacten a la Organización, el lanzamiento de un nuevo servicio o línea de negocio o cuando se presente una reestructuración organizacional en procesos y cargos.

##### 6.4.1. Identificación de Riesgos

La identificación de los riesgos se realiza con base en los siguientes factores: Entorno, personas, procesos, infraestructura y tecnología. Consiste en reconocer y determinar las causas (factores de riesgo) y riesgos inherentes a los procesos de la organización (mapa de procesos), es decir, el riesgo puro sin el efecto del control, que impedirían la consecución de los objetivos propios del negocio. (para mayor detalle ver *P-0217 Procedimiento para la identificación, Medición, Control y Monitoreo de los Riesgos Operacionales*).


##### 6.4.2. Medición de Riesgos

- **Medición del Riesgo Operacional Inherente**

El riesgo inherente mide el impacto/severidad 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 o Líderes de Procesos con el acompañamiento del equipo del Área de Riesgo y Cumplimiento. (para mayor detalle ver *P-0217 Procedimiento para la identificación, Medición, Control y Monitoreo de los Riesgos Operacionales*).

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Alineados con el compromiso de la Organización con el cuidado del medio ambiente, este documento no deberá ser impreso. Las copias físicas son consideradas como copias no controladas.	<b>Código: DG-0203/03</b>
--	---------------------------

	<b>POLÍTICA DE RIESGO OPERACIONAL</b>	Página 11 de 16
		Versión: 03
		Fecha: 24/10/2025

- **Medición del Riesgo Operacional 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 o sesiones de entendimiento a través de los medios determinados (comunicación vía mail o reuniones físicas o virtuales), en los que participan los Dueños o Líderes de Proceso (responsables de los riesgos y controles) o funcionarios que éstos deleguen con el soporte del Área de Riesgo y Cumplimiento, así como otros expertos con el nivel técnico y conocimiento adecuado de ser requerido.

La estimación del riesgo residual se realiza en términos de Probabilidad/frecuencia e Impacto/severidad, del mismo modo que el riesgo inherente. (para mayor detalle ver *Procedimiento para la identificación, Medición, Control y Monitoreo de los Riesgos Operacionales P-0217*).

#### 6.4.3. Control de Riesgos


La Organización establece para cada uno de los riesgos definidos en la etapa de identificación, actividades de control encaminadas a identificar, prevenir y mitigar su impacto en caso de materialización.

Las actividades de control pueden ser preventivas, de detección, correctivas, manuales, dependientes de TI o automáticas; e incluyen un rango de actividades diversas, dentro de las que se incluyen: aprobaciones, autorizaciones, segregación de funciones, verificaciones, reconciliaciones, revisiones de desempeño, perfiles de usuario y controles de acceso, controles físicos, entre otros, éstos pueden ser identificadas en el propio proceso de gestión del Riesgo Operacional (a través del análisis de la base de eventos de riesgo operacional y de alto impacto, de los Indicadores y del ejercicio del Área de Riesgo y Cumplimiento), pero también pueden ser identificadas en procesos de control internos (revisiones de auditoría interna) o externos ejercidos por la Contraloría de Corficolombiana, Revisoría Fiscal o cualquier Ente de control Corporativo.

Los dueños o líderes de proceso deben documentar apropiadamente y para cada uno de los procesos o áreas de negocio, las diferentes actividades de control. Así se asegura que cada uno de los riesgos definidos durante las etapas de identificación y medición se encuentren gestionados. Dicha documentación se hace a través de matrices de riesgo y controles.

Las actividades de control diseñadas para mitigar los riesgos operacionales son evaluadas, tanto en su diseño como en su operatividad, de acuerdo con la metodología establecida por Casa Matriz. (para mayor detalle ver *Procedimiento para la identificación, Medición, Control y Monitoreo de los Riesgos Operacionales P-0217*).

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Alineados con el compromiso de la Organización con el cuidado del medio ambiente, este documento no deberá ser impreso. Las copias físicas son consideradas como copias no controladas.	<b>Código: DG-0203/03</b>
--	---------------------------

	<b>POLÍTICA DE RIESGO OPERACIONAL</b>	Página 12 de 16
		Versión: 03
		Fecha: 24/10/2025

#### 6.4.4. Monitoreo de Riesgos

El Área de Riesgo y Cumplimiento como responsable de velar que se ejecute adecuadamente el sistema de Riesgo Operacional, debe realizar una revisión, como mínimo anual de los objetivos y componentes de la presente Política o lineamientos relacionados, además de un monitoreo continuo de revisión de riesgos identificados y de la suficiencia, idoneidad y efectividad de los controles asociados.

En todo caso, cada funcionario de la Organización es responsable de asegurar el cumplimiento de los controles a su cargo y de los estándares establecidos en esta política, así como, de reportar los eventos conocidos y/o identificados, a través de los canales dispuestos para el efecto el Formato *Reporte de Eventos de Riesgo Operacional y de Alto Impacto F-0251*.

Para el cumplimiento de esta etapa, 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 (Matriz ERM), que el riesgo residual se encuentra dentro de los niveles de aceptación establecidos por la entidad.
- Actualizar las calificaciones de Riesgo Residual y Riesgo Inherente a partir del comportamiento de los eventos de riesgo operacional en un periodo de un año.


Revisión del diseño y ejecución de los controles a partir de un criterio estadístico y técnico, establecido desde la Unidad de Riesgo Operacional. (para mayor detalle ver *Procedimiento para la identificación, Medición, Control y Monitoreo de los Riesgos Operacionales P-0217* y el documento *Evaluación, Diseño y Ejecución de Controles de Riesgo Operacional P-0216*).

#### 6.5. Gestión de Eventos de Riesgo Operacional y de Alto Impacto

El Área de Riesgo y Cumplimiento es la responsable de establecer, mantener actualizado y custodiar el registro de eventos de riesgo operacional y de alto impacto en la Organización. Este registro es un inventario de los eventos que implican la materialización de un riesgo en la Organización y llevará cuenta de todos los eventos que impliquen los siguientes tipos:

- **Tipo A:** Generan pérdidas y afectan el estado de resultados de la Organización.
- **Tipo B:** No generan pérdidas y por lo tanto no afectan el estado de resultados de la Organización

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Alineados con el compromiso de la Organización con el cuidado del medio ambiente, este documento no deberá ser impreso. Las copias físicas son consideradas como copias no controladas.	<b>Código: DG-0203/03</b>
--	---------------------------

	<b>POLÍTICA DE RIESGO OPERACIONAL</b>	Página 13 de 16
		Versión: 03
		Fecha: 24/10/2025

## 6.6. Información y Comunicación

### 6.6.1. Repositorio de Información

Para evidenciar la gestión realizada por la Organización con respecto al desarrollo y cumplimiento de la Política de Riesgo Operacional, se cuenta con un repositorio de información que permite soportar los elementos del SARO, así como, herramientas que permiten hacer una gestión de los riesgos identificados y los controles implementados, además, de llevar un control estadístico de todos los eventos de riesgo operacional y de alto impacto reportados y gestionados. Con lo anterior, se garantiza la disponibilidad, oportunidad y confiabilidad de la información relacionada con los EROS gestionados.

### 6.6.2. Capacitación y Entrenamiento

Con el fin de desarrollar una cultura hacia el Riesgo Operacional, la Organización ha definido las siguientes estrategias enfocadas hacia los funcionarios y áreas internas:

- **Funcionarios Antiguos**

Los funcionarios antiguos se capacitan por lo menos una vez al año en aspectos fundamentales de Riesgo Operacional definidos por el Área de Riesgo y Cumplimiento. Estas capacitaciones se desarrollan de manera presencial o no presencial según la disponibilidad de recursos y medios seleccionados para la comunicación, en la cual se expondrán los aspectos generales concernientes al sistema de Administración de Riesgo Operacional y la evolución de la Organización en su implementación.

- **Funcionarios Nuevos**

Los funcionarios nuevos se capacitan al momento de ingresar a la Organización, estas capacitaciones se desarrollan de forma continua, virtual o presencial según la disponibilidad de recursos y medios para la comunicación, en la cual se expondrá de manera general la Gestión liderada por el Área de Riesgo y Cumplimiento y los aspectos fundamentales frente a la administración y gestión del SARO y serán evaluados de manera física o digital para confirmar y retroalimentar los conocimientos que adquirieron.

- **Terceros Involucrados en Actividades de Negocio**

Al momento de establecerse vínculo con terceros que participen en el desarrollo de Actividades propias de la Organización, se definirán sus responsabilidades y funciones dentro del Sistema de Administración de Riesgo Operacional a través del conocimiento y aceptación de Políticas Corporativas e inclusión de cláusulas de Riesgo operacional cuando aplique.

Así mismo, conscientes de que una comunicación efectiva es un elemento fundamental para la implementación, interiorización, mantenimiento y sostenibilidad del SARO, el Área de Riesgo y Cumplimiento de la Organización, diseña campañas de socialización de mensajes que refuerzan la importancia del reporte de eventos de riesgo operacional y de alto impacto. Esto permite promover y afianzar la cultura de Riesgo Operacional en la Organización. Estas campañas internas, pueden contener y sin limitarse a comunicaciones escritas, correos electrónicos, mensajes a través de piezas comunicativas, material de apoyo, entre otros.

### 6.6.3. Estrategia de Divulgación

La divulgación de la información concerniente al sistema de Riesgo operacional es responsabilidad de cada área de la estructura de Riesgo Operacional, para eso se realizan las siguientes estrategias de acuerdo con el nivel de responsabilidad.

#### a) Representante Legal

- Informar semestralmente a la Junta Directiva sobre la evolución y aspectos relevantes de la gestión de riesgo operacional.
- Comunicar en el Informe de Gestión, al cierre de cada ejercicio contable, sobre la gestión adelantada en materia de administración de riesgo operacional.
- Suministrar al público la información necesaria con el fin de que el mercado pueda evaluar las estrategias de gestión del riesgo operacional adoptadas.
- Señalar en las notas a los estados financieros las causas que originaron los eventos de riesgo operacional, revelados en cuentas de orden o registrados en el estado de resultados cuando aplique.

#### b) Área de Riesgo y Cumplimiento (Unidad de Riesgo Operacional)

- Suministrar a la Alta Dirección los reportes de seguimiento a toda la gestión del riesgo operacional en forma clara y oportuna. La periodicidad de los informes será mínimo semestral.
- Cumplir con la imparcialidad en la generación de informes, garantizando la transparencia de la información.
- Informar a las unidades de negocio sobre el seguimiento realizado en la gestión de riesgos operacional en cada una de sus áreas.
- Realizar los informes regulatorios correspondientes a la gestión de riesgos operacional.

#### c) Auditoría Interna y Entes de Control Corporativos

- Informar los resultados de la evaluación de los elementos del SARO con el fin de determinar las deficiencias y sus posibles soluciones.
- Realizar informes periódicos al Representante Legal sobre el registro de eventos de riesgo operacional y de alto impacto.

- Comunicar los resultados del reporte elaborado al cierre de cada ejercicio contable, en el que informe acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el SARO.
- A su vez, debe poner en conocimiento del Representante Legal los incumplimientos del SARO, sin perjuicio de la obligación de informar sobre ellos a la Junta Directiva u órgano que haga sus veces.

En línea con lo anterior, la divulgación incluye:

- La Política de Riesgo Operacional socializada a todos los funcionarios de la Organización cada vez que se actualice.
- Se garantiza que el mapa de riesgos operacionales de cada proceso sea de fácil acceso y de conocimiento de los funcionarios de la Organización que tienen responsabilidades sobre la aplicación de los controles.
- Las matrices de Riesgo Operacional se actualizan cada vez que existan riesgos asociados a cambios o nuevos procesos, o programas de tecnología, o en los controles definidos.
- La copia de las matrices de riesgo operacional, se almacenan en el servidor NAS de la Organización y se encuentran disponibles para los Entes de Control Corporativos internos y externos, cuando estos lo requieran.

## 7. DOCUMENTOS DE REFERENCIA Y ANEXOS

- DG-0226 Matriz ERM
- P-0216 Evaluación, Diseño y Ejecución de Controles de Riesgo Operacional
- P-0217 Procedimiento para la identificación, Medición, Control y Monitoreo de los Riesgos Operacionales
- I-0212 Instructivo para el Registro, Control y Seguimiento de Eventos de Riesgo Operacional y de Alto Impacto
- F-0203 Contexto externo e interno de la organización
- F-0251 Formato Registro de Eventos de Riesgo Operacional y de Alto Impacto (ERO+AI)
- F-0286 Glosario Gestión de Riesgos
- Anexo No 1. Modelo de Gestión de Riesgo Operacional
- Anexo No 2. Lista de eventos de riesgo operacional según Basilea III

## 8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	01/08/2017	<ul style="list-style-type: none"><li>• Creación del documento</li></ul>
2	03/ 11/2020	<ul style="list-style-type: none"><li>• Actualización de lineamientos basados en la normatividad del Grupo Aval y Corficolombiana.</li><li>• Incorporación de la estructura organizacional de la Administración de Riesgo Operativo.</li><li>• Revisión general del documento.</li></ul>
3	24/10/2025	<ul style="list-style-type: none"><li>• Se realiza actualización del documento basado en las instrucciones impartidas por Casa Matriz.</li><li>• Se elimina la descripción de las definiciones del documento y se referencia el documento <i>Glosario Gestión de Riesgos F-0286</i></li><li>• Relación de la normatividad aplicable al documento. Adicionalmente se incorporan las Líneas Operativas y Tipología de Eventos según Basilea III.</li><li>• Se incluye la declaración de compromiso frente al SARO.</li><li>• Se realiza actualización de los esquemas de la metodología del SARO y su Estructura Organizacional.</li><li>• Se ajustan las áreas y responsables conforme a los cambios en el Organigrama de Proindesa.</li></ul>

## 9. FIRMAS DE REVISIÓN Y APROBACIÓN

El documento original está firmado y controlado por Proindesa S.A.S.