

POLÍTICA SARO

Código: GRC-DG-03

Versión: 08

CONTENIDO

1	OBJETIVOS.....	2
1.1	OBJETIVO GENERAL	2
1.2	OBJETIVOS ESPECÍFICOS	2
2	ALCANCE	2
3	DECLARACIÓN DE COMPROMISO	2
4	POLÍTICAS PARA LA ADMINISTRACIÓN DEL RIESGO OPERATIVO	3
4.1	POLÍTICA DE GOVERNABILIDAD	3
4.2	POLÍTICA DE INDEPENDENCIA	3
4.3	POLÍTICA DE GESTIÓN.....	3
4.4	POLÍTICA DE CONTINUIDAD DE NEGOCIO	3
5	RESPONSABILIDADES	4
5.1	MODELO DE LAS TRES LÍNEAS	4
5.2	ROLES Y RESPONSABILIDADES	4
6	POLÍTICAS DE OPERACIÓN	8
6.1	POLÍTICA DE RIESGO OPERATIVO	8
6.2	MARCO DE REFERENCIA DE EVALUACIÓN DEL RIESGO OPERATIVO	9
6.3	ETAPAS DEL MODELO	9
6.4	REGISTRO DE EVENTOS DE RIESGO OPERATIVO	17
6.5	PLAN DE CONTINUIDAD	18
6.6	ACTUALIZACIÓN	18
6.7	CAPACITACIÓN	19
7	DOCUMENTO DE APROBACIÓN.....	19
8	DOCUMENTOS RELACIONADOS.....	20
9	FORMATOS RELACIONADOS	20
10	CONTROL DE CAMBIOS	21

ESTE DOCUMENTO ES PROPIEDAD DE PISA. LAS PERSONAS QUE TENGAN ACCESO A ÉL SON RESPONSABLES DE SU CUSTODIA Y CONSERVACIÓN. NO PODRÁ SER REPRODUCIDO TOTAL NI PARCIALMENTE, NI ENTREGADO A TERCEROS, SIN LA AUTORIZACIÓN DEL RESPONSABLE DE PROCESOS. CUALQUIER COPIA IMPRESA DE ESTE DOCUMENTO SE CONSIDERA COPIA NO CONTROLADA.

* * *

Esta Política fue aprobada inicialmente por la Junta Directiva mediante el acta N° 410 del 18 de febrero del 2025 y emitida el 25 de marzo de 2025.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Establecer los lineamientos metodológicos, roles y responsabilidades de los actores claves para la gestión del Sistema de Administración del Riesgo Operativo¹ (en adelante SARO) de Proyectos de Infraestructura S.A.S. (en adelante PISA).

1.2 OBJETIVOS ESPECÍFICOS

- Definir el modelo de gobierno del Sistema de Administración del Riesgo Operativo y los lineamientos generales para identificar, medir, controlar y monitorear la gestión de riesgos.
- Monitorear la gestión y tratamiento de los riesgos², buscando su alineación con el apetito de riesgo³ operativo definido por PISA, con el fin de alertar ante eventuales anomalías.
- Establecer lineamientos que permitan empoderar el compromiso y responsabilidad de la gestión del riesgo en PISA, dando especial claridad a la primera línea sobre la importancia de desarrollar sus procesos con una asertiva administración de riesgos.
- Establecer la metodología para el seguimiento del estado de los eventos⁴ de riesgo operativo⁵ con mayor probabilidad⁶ de ocurrencia e impacto⁷ que permita adoptar acciones de mitigación o planes de acción por parte de PISA.
- Propender por la adopción de tecnologías y sistemas necesarios para la adecuada administración del riesgo operativo.

2 ALCANCE⁸

Esta política establece las directrices y principios generales que PISA debe cumplir para la gestión del riesgo operativo.

La gestión de los riesgos operativos de PISA es responsabilidad de los órganos de gobierno y control. Es por ello que todos los colaboradores deben conocer, acatar y aplicar las directrices establecidas en el presente documento, así como las disposiciones legales vigentes que le sean aplicables y los lineamientos que Corficolombiana, en calidad de entidad matriz emita al respecto.

3 DECLARACIÓN DE COMPROMISO

PISA está comprometida con la adopción de la presente política con base en el fortalecimiento de la cultura de riesgo operativo en todos los niveles de la compañía, promoviendo así la implementación de un sistema de gestión que apoye a PISA en el logro de sus objetivos. Por lo tanto, los colaboradores de PISA son responsables de aplicar los criterios definidos en esta política y por ajustar sus actuaciones de acuerdo con los valores corporativos y lineamientos establecidos. De igual forma son responsables de reportar oportunamente los eventos de riesgo de alto impacto de los que pueda llegar a tener conocimiento.

¹ Sistema de Administración del Riesgo Operativo (SARO): conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales la compañía identifica, mide, controla y monitorea el riesgo operativo.

² Riesgo: la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad.

³ Apetito de Riesgo: nivel de riesgo que la compañía está dispuesta a aceptar o asumir, con el fin de lograr sus objetivos estratégicos y su plan de negocio.

⁴ Evento: Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.

⁵ Riesgo Operativo: es la posibilidad de que la compañía 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.

⁶ Probabilidad: Es la posibilidad que un riesgo se materialice. Para determinar la probabilidad se puede utilizar el análisis cualitativo o cuantitativo.

⁷ Impacto: Es la pérdida (monetaria o no monetaria) generada por la materialización de un riesgo, que puede ser medida de manera cualitativa o cuantitativa.

⁸ Alcance: de acuerdo con lo establecido en el otrosí No. 5 del contrato de prestación de servicios suscrito entre PISA y CCFC, y a las instrucciones dadas por las Juntas Directivas de cada compañía, la presente política es aplicable a Concesiones CCFC S.A.S. en lo que le aplique o le llegare a aplicar de conformidad con la estructura y naturaleza de los procesos y/o actividades desarrolladas por CCFC.

4 POLÍTICAS PARA LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

PISA ha definido las siguientes políticas, las cuales fundamentan y estructuran el SARO de tal forma que se dé una valoración y presentación objetiva y transparente del riesgo operativo: POLÍTICA ESTRATÉGICA

La gestión de los riesgos operativos en PISA debe estar orientada a la creación y el fortalecimiento de una cultura de riesgos, mediante la capacitación y concientización de todos los colaboradores de PISA. Estas actividades buscan que los colaboradores conozcan el proceso de identificación, medición, control y monitoreo de los riesgos que se pueden presentar en el desarrollo de actividades propias de los procesos.

En este sentido, es responsabilidad de la administración de PISA asegurar que exista una fuerte cultura de gestión del riesgo operativo.

4.1 POLÍTICA DE GOBERNABILIDAD

PISA debe contar con órganos de administración, gobierno y de control con funciones definidas en el SARO, que evidencien su rol y las responsabilidades específicas en cada una de las etapas del sistema, asegurando su cumplimiento y alineación con los objetivos del mismo.

4.2 POLÍTICA DE INDEPENDENCIA

La administración de PISA debe establecer una estructura de gestión del riesgo operativo, aprobada por la Junta Directiva, independiente, clara, con jerarquía y autoridad suficiente en toda la compañía para el desarrollo efectivo de sus funciones, eficaz y suficiente con líneas de responsabilidad bien definidas, transparentes y coherentes que le permitan acceder a la Junta Directiva y al Comité de Riesgos sin ningún impedimento.

PISA es responsable de la aplicación de lo dispuesto en el presente documento en sus filiales. Así mismo, de la consolidación de la información a reportar según esta política e instructivos relacionados emitidos por el área de riesgos de Corficolombiana y de Grupo Aval.

4.3 POLÍTICA DE GESTIÓN

PISA debe asegurar que se identifiquen y evalúen los riesgos operativos en todos los procesos, incluyendo aquellos relacionados con el lanzamiento y/o modificación de cualquier proceso y/o servicio previo a su realización.

En todo caso es responsabilidad de la primera línea garantizar que los procesos se encuentren actualizados y que los nuevos procesos y/o servicios, cuenten con un análisis previo de riesgos y controles antes de su lanzamiento.

Se entiende que los riesgos se identifican y evalúan a nivel de proceso, los cuales tienen implícitos productos o servicios, actividades y sistemas, que permiten identificar los riesgos, actividades significativas, proveedores críticos, líneas de negocios, sistemas Core, controles, entre otros.

Así mismo, se deben implementar procesos para monitorear regularmente los perfiles de riesgo operativo y las exposiciones a pérdidas materiales. Igualmente se deben establecer los flujos de información que sean necesarios para apoyar la gestión proactiva del riesgo operativo por parte de los diferentes actores del modelo.

4.4 POLÍTICA DE CONTINUIDAD DE NEGOCIO

PISA debe tener planes de continuidad para 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 del negocio.

5 RESPONSABILIDADES

5.1 MODELO DE LAS TRES LÍNEAS

PISA ha establecido el principio de las tres líneas de acuerdo con el marco de referencia COSO. Igualmente, PISA debe estructurar sus funciones y responsabilidades frente a los riesgos que se exponen, siguiendo este esquema, esto es, considerando (i) la gestión por la línea de negocio, (ii) una función de gestión del riesgo independiente, y (iii) una revisión independiente.

5.1.1 Primera Línea

La primera línea la constituyen las áreas operativas y de apoyo que gestionan el negocio. Esto significa que la administración de riesgo operativo reconoce que la gestión de la primera línea es responsable de identificar, evaluar, gestionar y controlar los riesgos asociados a los procesos de los que son responsables. Esta línea debe conocer y aplicar las políticas y procedimientos, así como disponer de los recursos suficientes para realizar eficazmente estas tareas, aplicando criterios de autocontrol que permitan establecer y ejecutar las medidas para mitigar sus riesgos.

5.1.2 Segunda Línea

La segunda línea asigna responsabilidades al Área de GRC de PISA, la cual debe hacer seguimiento al cumplimiento de todas las obligaciones relacionadas con el tema. Igualmente, es responsable de la definición de la metodología para la gestión de este riesgo, así como la identificación de herramientas adecuadas para tal efecto. De esta manera es responsable por la valoración adecuada, el monitoreo y control de los riesgos operativos de PISA como apoyo técnico a la primera línea que actúa bajo el principio de autocontrol. En este sentido, la segunda línea debe velar por el buen diseño de los controles y porque los mismos mitiguen de forma adecuada, particularmente los riesgos operativos relevantes de PISA.

Los intereses comerciales de PISA no deben oponerse en absoluto al eficaz desempeño de las atribuciones anteriormente mencionadas del Coordinador de GRC. Con independencia del tamaño de la compañía, debe evitarse posibles conflictos de intereses. Así pues, para permitir juicios ecuanímenes y facilitar un asesoramiento imparcial a la dirección, el Coordinador de GRC no debe, por ejemplo, asumir competencias inherentes a la primera y tercera línea. Ante cualquier conflicto entre las líneas-áreas de negocio y las atribuciones del Coordinador de GRC, deben existir procedimientos que garanticen que las cuestiones de riesgo operativo reciben una consideración objetiva al más alto nivel.

5.1.3 Tercera Línea

La tercera línea está conformada por la función de Auditoría Interna y es responsable de evaluar de forma independiente la efectividad de la gestión del riesgo operativo de PISA.

5.2 ROLES Y RESPONSABILIDADES

Para dar cumplimiento a los objetivos de esta política, se han definido los siguientes actores claves, quienes adicional a las funciones propias, deberán cumplir las siguientes para la gestión del riesgo operativo:

5.2.1 Junta Directiva

Las funciones de la Junta Directiva son:

- Establecer y aprobar la Política del Sistema de Administración del Riesgo Operativo – SARO y sus actualizaciones.
- Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SARO.
- Analizar los informes periódicos que presente la Administración, el Área de GRC, la Revisoría Fiscal y la Auditoría Interna sobre riesgo operativo.

- Establecer el perfil de riesgo⁹ de PISA, teniendo en cuenta los niveles de apetito, tolerancia y capacidad máxima de riesgo.

5.2.2 Gerente General

El Gerente General, es el máximo cargo directivo y como tal, tiene la responsabilidad de la gestión de riesgo operativo asumida por PISA, para lo cual debe tener las siguientes funciones:

- Diseñar y someter a aprobación de la Junta Directiva, la Política del Sistema de Administración del Riesgo Operativo – SARO y sus actualizaciones.
- Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva.
- Adelantar un seguimiento permanente de las etapas y elementos constitutivos del SARO.
- Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural que la administración de este riesgo implica para PISA.
- Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta los niveles de apetito, tolerancia y capacidad máxima de riesgo, fijado por la Junta Directiva.
- Velar por la correcta aplicación de los controles del riesgo inherente, identificado y medido.
- Recibir y evaluar los informes presentados por el Área de Gobierno, Riesgo y Cumplimiento (en adelante Área de GRC).
- Velar porque las etapas y elementos del SARO se desarrollen de acuerdo con la presente Política y porque se implementen los procedimientos para la adecuada administración del riesgo operativo a que se vea expuesta PISA en desarrollo de sus actividades.

5.2.3 Comité de Riesgos

El Comité de Riesgos es el organismo que monitorea y hace seguimiento de forma integral a las actividades y funciones relacionadas con la administración de los riesgos. Tiene como función principal apoyar a la Gerencia General de PISA en la adecuada gestión de la identificación, medición, control y monitoreo de los diferentes riesgos de PISA.

Sus integrantes son:

- Gerente General
- Gerente Jurídico, o quien haga sus veces
- Gerente Administrativo, o quien haga sus veces
- Gerente de Operaciones, o quien haga sus veces
- Director Financiero, o quien haga sus veces
- Coordinador de Gobierno, Riesgo y Cumplimiento, quien actuará como Coordinador del Comité

Se podrá invitar a cualquier colaborador de PISA que se requiera, dependiendo de los temas a tratar.

La Auditoría interna en su calidad de evaluador del cumplimiento de los procedimientos, podrá asistir al Comité de Riesgos como invitado, entendiendo que su presencia permitirá tener un conocimiento actualizado sobre las decisiones que allí se adopten y poder así efectuar la correspondiente evaluación al cumplimiento de los procedimientos de esta.

El Comité de Riesgos considerará y tendrá conocimiento acerca de los siguientes temas:

⁹ Perfil de Riesgo: resultado consolidado de la medición permanente de los riesgos operacionales a los que se ve expuesta la compañía.

- Riesgos operativos (*legal*¹⁰, *reputacional*¹¹ y de continuidad de negocio)
- Riesgo de Lavado de Activos, Financiación de Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva – SAGRILAFT
- Riesgo de corrupción
- Riesgos de Cumplimiento Normativo
- Riesgos emergentes
- Riesgos Inherentes de Mayor Impacto

Las siguientes serán las funciones o responsabilidades del Comité:

- Facilitar la comunicación entre los involucrados en los temas inherentes a las gestiones de riesgos.
- Coordinar el análisis y preparación de la información para la toma de decisiones relacionadas con temas de riesgos.
- Realizar seguimiento a los compromisos respecto de los temas de riesgos y *control interno*¹².
- Proponer, para aprobación de la Junta Directiva, las políticas de los diferentes sistemas de riesgos y realizar el seguimiento y control de estas.
- Establecer los procedimientos y mecanismos, aprobando las metodologías y los sistemas para una adecuada gestión y administración de los riesgos.
- Conocer y comprender los riesgos que asume PISA, evaluando permanente la exposición al riesgo.
- Desarrollar estrategias para la construcción de una cultura organizacional de gestión de riesgos dentro de PISA.

El Comité de Riesgos tendrá una periodicidad anual, con sesión en el primer cuatrimestre de cada año, pero podrá ser convocado por cualquiera de los integrantes en cualquier momento, siempre que exista una situación que lo amerite.

5.2.4 Todas las áreas de PISA

Todas las áreas de PISA son responsables de la gestión y control de los riesgos operativos. Entre otras, tendrán las siguientes responsabilidades:

- Conocer y cumplir las políticas y procedimientos correspondientes a su área, y concretamente las relativas a la gestión y control de los riesgos operativos.
- Gestionar los riesgos operativos del proceso a cargo (identificar, medir, controlar y monitorear).
- Gestionar los planes de acción establecidos a partir del registro de eventos y resultados del monitoreo del perfil de riesgo del proceso.
- Proponer la modificación de los procedimientos y controles o bien la implementación de otros nuevos, con el fin de mejorar la operativa y el nivel de control de los riesgos.
- Recibir la información periódica elaborada por el Área de GRC para su seguimiento, análisis, y toma de decisiones.

¹⁰ Riesgo Legal: Es la posibilidad de pérdida en que incurre PISA 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 PISA respecto de los procesos y/o actividades tercerizadas.

¹¹ Riesgo Reputacional: Es la posibilidad de pérdida en que incurre PISA por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de PISA y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

¹² Control Interno: Proceso ejecutado por la Junta Directiva, la Administración y demás colaboradores de PISA diseñado para garantizar razonablemente el cumplimiento de los objetivos de esta respecto a operaciones, reporte y cumplimiento.

5.2.5 Área de Gobierno, Riesgo y Cumplimiento (GRC)

El Área de Gobierno, Riesgo y Cumplimiento está a cargo del Coordinador de GRC y tendrá las siguientes funciones:

- Realizar seguimiento y control de la gestión del riesgo operativo asegurando el cumplimiento de políticas, metodologías y procedimientos establecidos por Grupo Aval o por Corficolombiana.
- Establecer y monitorear el perfil de riesgo de PISA e informarlo al Comité de Riesgos y a la Junta Directiva.
- Evaluar el impacto de las medidas de control potenciales para cada uno de los eventos de riesgo identificados y medidos.
- Respalda y ayudar en la coordinación de los procesos de identificación, evaluación, monitoreo y control del riesgo operativo en apoyo a los colaboradores de la primera línea de PISA y filiales.
- Administrar el registro de eventos de riesgo operativo.
- Desarrollar los programas de capacitación en temas de riesgo operativo y ser asesores de riesgo operativo a las áreas que lo requieran.
- Realizar seguimiento a los controles adoptados para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.
- Presentar un informe periódico, como mínimo anual a la Junta Directiva sobre la evolución y aspectos relevantes de la gestión del riesgo operativo.

5.2.6 Auditoría Interna

La Auditoría Interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de PISA. Ayuda a cumplir los objetivos organizacionales aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

Las funciones de la auditoría interna frente a la gestión de riesgo operativo están orientadas a evaluar periódicamente a través de procesos selectivos, la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SARO, a revisar periódicamente el registro de eventos de riesgo operativo, informando oportunamente sus hallazgos a las instancias responsables.

Estas evaluaciones se adelantarán a través de roles permitidos como son:

- 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.
- La validación de la ejecución de los controles se adelantará selectivamente por parte de la Auditoría Interna en sus procesos periódicos de revisión anual.
- Brindar servicios de consultoría, los cuales son por naturaleza consejos, y son desempeñados, por lo general, a pedido de un cliente interno.

No son funciones de la Auditoría:

- Establecer el *apetito de riesgo*.
- Imponer procesos de gestión de riesgo operativo.
- Manejar el aseguramiento sobre los riesgos.
- Tomar decisiones en respuesta a los riesgos.
- Implementar respuestas a riesgos en favor de la Administración.

6 POLÍTICAS DE OPERACIÓN

6.1 POLÍTICA DE RIESGO OPERATIVO

- La gestión del riesgo forma parte integral de las responsabilidades de la *Alta Dirección*¹³, lo que debe traducirse en una fuerte cultura de control, el conocimiento de los riesgos y el propio estilo de administración. PISA debe efectuar la gestión del SARO bajo su entera responsabilidad conforme a las políticas internas definidas y la normatividad vigente aplicable.
- La Administración, a todos los niveles, es responsable de gestionar, controlar y *mitigar*¹⁴ los riesgos operativos en sus áreas de responsabilidad. Debe existir una participación activa de la Alta Dirección.
- El *control del riesgo*¹⁵ operativo, de forma independiente a la propia gestión, tiene por objeto facilitar la identificación, evaluación, el seguimiento del grado de gestión, la mitigación y la medición de los riesgos operativos, utilizando para ello herramientas cualitativas y cuantitativas de diferente naturaleza.
- La administración del riesgo operativo se realiza directamente en el Área de GRC, debido a la necesaria segregación de funciones y a la especialización que se requiere para ejecutarlas.
- Todos los colaboradores de PISA deben participar en las diferentes etapas del SARO, particularmente en la recolección de la información. Cualquier conflicto de intereses que pueda surgir deberá ser estudiado de acuerdo con lo indicado en los procedimientos internos relacionados con el tema.
- Todos los colaboradores de PISA deben cumplir con todas las políticas, procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento del Sistema de Administración del Riesgo Operativo (SARO).
- PISA debe establecer que sus filiales tengan el mismo esquema de gestión de riesgo operativo, garantizando la homogeneidad en la implementación del SARO.
- Los colaboradores de PISA, en cualquier función y categoría profesional, debe conocer los riesgos operativos de su responsabilidad, y su eficacia en la gestión y control de estos riesgos debe formar parte de su evaluación anual.
- PISA debe propender por mantener una base íntegra y sólida de datos de eventos de riesgo operativo que permita la adecuada gestión y seguimiento a los mismos. Por lo tanto, todos los Oficiales de Riesgo Operativo (OROS) deben reportar al Área de GRC los *eventos de riesgo*¹⁶ que resulten en su actividad laboral o los que se presenten en su área de trabajo. Para ello PISA adopta el Instructivo Corporativo Mejores Prácticas en el Manejo de las Pérdidas por Riesgo Operativo emitido por Grupo Aval, de acuerdo con los alcances definidos en dicho Instructivo.
- La implementación del *Plan de Continuidad de Negocio*¹⁷ 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.
- Debe existir herramientas cualitativas y cuantitativas que permitirán identificar, medir, controlar y monitorear los riesgos operativos.
- La Alta Dirección debe optimizar las inversiones destinadas a la gestión y control del riesgo operativo.
- La divulgación de la información forma parte esencial del Sistema de Administración del Riesgo Operativo, la cual está a cargo del Área de GRC de PISA.

¹³ Alta Dirección: Es la persona o grupo de personas con responsabilidad por la conducción de las operaciones de PISA, incluye a la Junta Directiva, Gerente General y Representantes Legales Suplentes.

¹⁴ Mitigar: Reducción del nivel de riesgo existente a un nivel aceptable por PISA.

¹⁵ Control del Riesgo: Parte de la administración del riesgo que involucra la implementación de políticas, normatividad, procedimientos y cambios físicos a fin de eliminar o minimizar los riesgos adversos. Cualquier medida que tome la compañía para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos.

¹⁶ 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.

¹⁷ Plan de Continuidad de Negocio: Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retomar y continuar la operación, en caso de interrupción.

- La capacitación en riesgo operativo se debe realizar a todos los colaboradores de PISA dentro del proceso de inducción de un colaborador nuevo y anualmente.

6.2 MARCO DE REFERENCIA DE EVALUACIÓN DEL RIESGO OPERATIVO

El proceso de *evaluación de los riesgos*¹⁸ operativos de PISA 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 PISA selecciona 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.

6.3 ETAPAS DEL MODELO

La metodología establecida por PISA para la administración del riesgo operativo se fundamenta en cuatro etapas: Identificación, Medición, Control y Monitoreo.

6.3.1 Identificación

6.3.1.1 Análisis del Entorno

El análisis del entorno es el punto de partida de una identificación eficiente de los factores internos o externos que pueden generar riesgos y, por lo tanto, atentar contra el cumplimiento de la misión y objetivos de PISA.

El análisis del entorno se realiza a partir del conocimiento e identificación de situaciones externas, las cuales pueden ser de carácter social, cultural, económico, tecnológico, ecológico, político y legal, bien sean internacionales, nacionales o regionales.

Las situaciones internas están relacionadas con la estrategia, objetivos, estructura, cultura organizacional, el modelo de operación, el cumplimiento de los planes, programas y proyectos, los sistemas de información, los procesos, procedimientos y los recursos humanos y económicos con los que cuenta PISA.

El Área de GRC deberá documentar el resultado de este análisis en el documento Contexto Interno y Externo, documento que servirá de guía a los dueños de proceso para las sesiones de identificación de riesgos, de tal manera que permita darles información de referencia respecto del entorno en el que se desenvuelve PISA. Sin embargo, esta información podrá ser modificada y corregida durante la ejecución de las sesiones con los aportes de los participantes.

6.3.1.2 Definir Factores de Riesgo

Los dueños de procesos con apoyo del Área de GRC deben establecer los factores de riesgo que materializan o exponen a PISA al riesgo descrito. Los factores de riesgo pueden ser: Recurso Humano, Procesos, Tecnología de Información, Infraestructura o Eventos Externos (Naturales o Provocados).

- **Recurso Humano:** Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de PISA. 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 PISA 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 de Información:** Es el conjunto de herramientas empleadas para soportar los procesos de PISA. Incluye: hardware, software y telecomunicaciones.

¹⁸ Evaluación del Riesgo: Proceso usado para determinar las prioridades de administración del riesgo mediante la comparación de la probabilidad del riesgo y su impacto.

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

6.3.1.3 Determinación de Riesgos

Consiste en que los *dueños de procesos*¹⁹ con apoyo del Área de GRC reconozcan y determinen los *riesgos inherentes*²⁰ a los procesos de PISA, riesgos que de llegar a materializarse impedirían el logro de los objetivos. En otras palabras, se refiere a los posibles fallos o deficiencias en los recursos y procesos de las actividades del día a día.

También se deberá evaluar la aplicabilidad en PISA de los riesgos operativos incluidos en el catálogo de *riesgos genéricos*²¹ SARO que actualiza regularmente Grupo Aval y los riesgos asociados a Derechos Humanos, Sociales y Ambientales aplicables a PISA.

La identificación de los riesgos debe tener en cuenta el conocimiento previo de situaciones, tales como:

- Situaciones que han o que pueden llegar a entorpecer u obstaculizar el cumplimiento de un objetivo, la obtención de un resultado, el cumplimiento de un requisito legal, organizacional o externo, o la satisfacción de los usuarios.
- Retroalimentación de los hallazgos de las auditorías internas o externas realizadas a los procesos de PISA y los registros efectuados en la base de datos de registro de eventos de riesgo operativo.
- Disponer de un mecanismo interno, que permita alertar la ocurrencia de los eventos por parte de cualquier colaborador; dicha situación está sujeta a la verificación por parte del Área de GRC para la posterior solicitud del registro de evento operativo. (Ver numeral 6.4. Registro de eventos de riesgo operativo).
- Sesiones periódicas de monitoreo de los procesos con el acompañamiento del Área de GRC y los dueños de procesos.
- Identificación y análisis de nuevos proyectos, servicios o procesos en PISA.

El alcance de la identificación se encuentra determinado por los procesos que se encuentren totalmente documentados, ya que con ello se tiene un mapa de todos los subprocesos y actividades que implican y, por tanto, es posible listar más fácilmente los eventos de riesgo posibles.

Para identificar las situaciones de riesgo que puedan afectar a PISA, se utilizará la técnica de identificación de riesgos denominada entrevistas estructuradas o semiestructuradas.

Para ejecutar la identificación del proceso será necesario desarrollar sesiones de identificación con el dueño del proceso, directivos (si se considera necesario) y colaboradores que participan en el proceso implementando la técnica seleccionada.

El resultado de la ejecución de esta actividad se debe documentar en la Matriz ERM Sector Infraestructura.

Para la adecuada identificación de los riesgos se deben tener en cuenta los siguientes parámetros: El objetivo del proceso, los productos y/o servicios que genera el proceso, el dominio del riesgo, la categoría del riesgo y el sistema de riesgo afectado.

Para cada evento identificado, es necesario redactar un riesgo. Al momento de redactar los riesgos deberán tenerse en cuenta los siguientes criterios:

- El riesgo debe estar escrito en un lenguaje claro, común y comprensible para toda PISA.
- Debe responder fácilmente a la pregunta si ocurre el riesgo ¿Qué pérdida es generada? Es decir, permite identificar la pérdida potencial: fraude, multa, demanda, reproceso, robo, sanción, entre otros.
- No se debe confundir con un problema.
- Debe permitir establecer la probabilidad e impacto, obteniendo así la calificación de este.

¹⁹ Dueño del Proceso: Es el representante del proceso, que conoce sus expectativas y necesidades y las traduce en requerimientos (acuerdos de niveles de servicio - ANS) al interior de PISA. En coordinación con los ejecutores, diseña el proceso y asigna responsables dentro de las etapas o subprocesos.

²⁰ Riesgo Inherente: nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

²¹ Riesgo Genérico: nombre del riesgo operacional que a nivel de Grupo Aval ha sido establecido para ser homologado con los riesgos nivel entidad, que mide de manera transversal la exposición del riesgo por entidad y grupo, tanto en impacto como en probabilidad.

- Se debe determinar de manera clara las situaciones de riesgo, a fin de no generar o estructurar riesgos que sean causas generadoras o consecuencias.
- Se deben emplear verbos en infinitivo.
- Evitar las negaciones para expresar el Riesgo. Ejemplo: No realizar la actualización de una información.
- El riesgo no debe ser el efecto o el impacto de este. Ejemplo: Sanciones, multas, sobrecostos.
- La ausencia o deficiencia de un control no es un riesgo.

Cuando se generen dudas con respecto a si se identificó un riesgo o realmente lo identificado es una causa, se sugiere recordar la frase del riesgo:

Debido a **CAUSA** puede ocurrir **RIESGO** lo que conllevaría a **EFEECTO**

Igualmente, PISA deberá hacer una evaluación de los riesgos emergentes. Los riesgos emergentes son riesgos nuevos e imprevistos que emergen de condiciones, situaciones o tendencias locales o internacionales que podrían afectar significativamente la solidez financiera, la posición competitiva o la reputación de PISA o del sector en el que opera PISA. Los riesgos emergentes implican un alto grado de incertidumbre y una dificultad en su cuantificación por la ausencia de datos por lo que en general su frecuencia e impacto son difíciles de evaluar y a menudo surgen de tendencias globales y con frecuencia están más allá de la capacidad de cualquier parte en particular para controlarlo. Suelen tener baja frecuencia y alto impacto y su fuente puede estar relacionada con cambios en el entorno político, normativo, legal, demográfico, tecnológico, de mercado o socioeconómico.

6.3.2 Medición

Los dueños de los procesos con apoyo del Área de GRC evalúan los riesgos identificados, con el fin de determinar la probabilidad y el impacto del riesgo. Esta etapa tiene como objetivo establecer el nivel de riesgo inherente al cual está expuesto cada uno de los procesos de PISA, teniendo en cuenta los criterios definidos por la Junta Directiva. Esta actividad se debe revisar anualmente o antes si llega a haber un cambio sustancial en los riesgos.

6.3.2.1 Probabilidad de Ocurrencia

Consiste en determinar qué tan factible es la materialización de un riesgo, para lo cual en primera instancia se utilizará la probabilidad cuantitativa, de acuerdo con la siguiente escala:

PROBABILIDAD CUANTITATIVA		
Calificación	Nivel	Eventos Occurridos en los Últimos Años
1	Muy baja	El evento no se ha presentado o se ha presentado una vez en los últimos 20 años.
2	Baja	El evento se ha presentado una vez en la entidad o en el sector en los últimos 5 años.
3	Moderada	El evento se ha presentado por lo menos una vez cada año.
4	Alta	El evento se ha presentado con alguna frecuencia (1 vez cada trimestre).
5	Muy Alta	El evento se ha presentado con cierta periodicidad (1 vez cada mes o más).

En caso de no poseer información respecto de la cantidad de eventos ocurridos en los últimos años, se deberá determinar qué tan factible es la materialización de un riesgo, mediante la probabilidad cualitativa, de acuerdo con la siguiente tabla:

PROBABILIDAD CUALITATIVA			
Aspecto a Evaluar	Niveles		
Grado de automatización de la actividad	Totalmente Automático	Semiautomático	Manual
Nivel de complejidad de ejecución	Requiere un conocimiento básico	Requiere un conocimiento avanzado	Requiere de un experto
Periodicidad de la ejecución de la actividad	Semestral - Anual	Mensual - Trimestral	Diario - Semanal
Dispersión en la ejecución de la actividad	Interviene 1 persona	Intervienen 2 o 3 personas	Intervienen 4 o más personas

6.3.2.2 Impacto

Consiste en estimar las consecuencias que tendría la *materialización del riesgo*²² sobre cada uno de los procesos de PISA. El impacto será representado, en primera instancia, teniendo en cuenta el efecto que en materia económica y reputacional pueda tener la materialización de un riesgo, de acuerdo con la siguiente escala:

MAGNITUD DEL IMPACTO				NIVEL DE RIESGOS
Calif.	Nivel de Impacto	Impacto Económico	Reputacional	
1	Inferior	Pérdida menor a 1.800 SMMLV.	Deterioro de la imagen a nivel interno, No afecta la relación con los accionistas, No afecta la consecución de clientes o negocios.	Apetito de Riesgo
2	Menor	Pérdidas entre 1.801 Y 4.500 SMMLV.	Deterioro de la imagen a nivel local. Puede afectar la relación con los accionistas. Puede afectar la consecución de clientes o negocios	
3	Importante	Pérdidas entre 4.501 y 9.000 SMMLV.	Deterioro de la imagen a nivel Regional. Afecta la relación con los accionistas. Dificulta la consecución de nuevos clientes o negocios.	Tolerancia
4	Mayor	Pérdidas entre 9.001 y 18.000 SMMLV.	Deterioro imagen a nivel Nacional. Afecta ampliamente la relación con los accionistas. Impide la consecución de nuevos clientes o negocios.	
5	Superior	Pérdidas superiores 18.000 SMMLV.	Deterioro imagen a nivel internacional. Afecta ampliamente la relación con los accionistas. Impide la consecución de nuevos clientes o negocios en el ámbito internacional.	Capacidad Máxima

En segunda instancia se debe analizar el efecto que, en materia de cumplimiento legal, de pérdida de información y ambiental pueda tener la materialización de un riesgo, de acuerdo con la siguiente escala:

²² Materialización del Riesgo: Ocurrencia de un evento considerado como incierto (riesgo) y que su desarrollo implica una consecuencia positiva o negativa a PISA.

MAGNITUD DEL IMPACTO				
Calificación	Nivel de Impacto	Cumplimiento Legal	Pérdida de Información	Ambiental
1	Inferior	No afecta la oportunidad del manejo y entrega de la información a entes reguladores.	No afecta la disponibilidad de la información.	No existe contaminación de ningún tipo.
2	Menor	Solicitudes de entes reguladores sobre el incidente operativo.	No afecta la disponibilidad de la información de manera significativa, no altera el funcionamiento de las áreas receptoras y procesadoras de información.	Las consecuencias del impacto generan modificaciones mínimas sobre el medio ambiente o la comunidad
3	Importante	Requerimientos emitidos por los entes reguladores a inconformidades sobre el cumplimiento de las normas establecidas.	Indisponibilidad de la información ocasionando retrasos en las labores de las áreas y/o en la respuesta a los entes reguladores.	El efecto no es suficiente para poner en grave riesgo los recursos naturales o la comunidad, pues solo se generan afectaciones o alteraciones moderadas en el entorno analizado.
4	Mayor	Sanciones por incumplimiento de normas establecidas por los entes reguladores.	Pérdida de información crítica de la compañía o de terceros que no se pueda recuperar fácilmente, generando cese temporal en las actividades.	El efecto genera un deterioro o alteración del ecosistema y/o la comunidad, puede haber pérdida ambiental o económica intermedia
5	Superior	Intervención a la Compañía por los Entes Regulatorios y de Control.	Pérdida de información crítica de la compañía o de terceros que no se pueda recuperar y afecte definitivamente los procesos y funciones de la compañía.	El impacto afecta de manera significativa o grave los ecosistemas o el entorno social o causa pérdidas económicas significativas

6.3.2.3 Calificación del Riesgo Inherente

Se logra a través de la evaluación de la probabilidad de ocurrencia (cuantitativa o cualitativa) y el impacto de la materialización del riesgo. Los *criterios*²³ para la calificación son subjetivos, depende de la particularidad del riesgo y los antecedentes en cada uno de los procesos y de los equipos de trabajo. La calificación del riesgo inherente se debe realizar por parte de los dueños de procesos con apoyo del Área de GRC.

6.3.2.4 Severidad

El grado de severidad es el indicador cualitativo que resulta de multiplicar el impacto por la probabilidad. El resultado permite establecer el nivel de cada uno de los riesgos identificados, acorde con la siguiente escala:

Nivel de severidad	Respuesta del Riesgo
Extremo	Evitar, compartir o transferir el riesgo
Alto	Mitigar el riesgo
Moderado	Mitigar el riesgo
Bajo y Muy Bajo	Asumir el riesgo

A continuación, se hace una breve descripción de cada uno de los niveles de severidad:

²³ Criterios de evaluación o medición de un riesgo: Son los términos de referencia frente a los cuales la importancia de un riesgo es evaluada. Los criterios de evaluación de un riesgo se basan en los objetivos y en el contexto externo e interno de PISA. Los criterios de evaluación de un riesgo se pueden derivar de normas, leyes, políticas y otros requisitos.

Zona de Severidad Extremo (Rojo): Riesgos Inaceptables: Se debe dar tratamiento a las causas que generan el riesgo. Es decir, se deben implementar controles de prevención para reducir la probabilidad del riesgo o disminuir el impacto de los efectos, a través de la adopción de medidas de protección para compartir o transferir el riesgo si es posible, por ejemplo, a través de pólizas de seguros u otras opciones que estén disponibles. Las acciones que se definan como tratamiento se deben establecer a corto plazo.

Zona de Severidad Alto (Amarillo) y Moderado (Verde): Riesgos Moderados: Se deben tomar medidas para mitigar los riesgos llevándolos al nivel de severidad bajo o muy bajo, fortaleciendo los controles existentes o implementando controles complementarios.

Zona de Severidad Bajo y Muy Bajo (Azul): Riesgos Aceptables: El riesgo se encuentra en un nivel que puede ser aceptado sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

6.3.3 Control

El objetivo es determinar los controles que se tienen implementados para cada uno de los riesgos inherentes identificados, con el propósito de evaluar la efectividad de estos y el efecto en la reducción que éstos producen en los factores generadores de riesgos.

Para aquellos riesgos inherentes que se encuentran en un nivel de severidad superior al nivel bajo o muy bajo es necesario definir un plan de tratamiento a implementar.

Cada uno de los riesgos evidenciados dentro de la etapa de identificación deberá poseer como mínimo un control documentado que ayude a la mitigación del riesgo.

6.3.3.1 Diseño de Controles

Los controles se definen como mecanismos, políticas, prácticas u otras acciones existentes que actúan para minimizar el riesgo o potenciar oportunidades positivas en la gestión del riesgo, con el fin de garantizar el desarrollo y cumplimiento de las actividades de PISA.

Los controles, de acuerdo con su naturaleza, se pueden clasificar en:

Control Preventivo: Acciones aplicadas previamente al inicio de una actividad. Se emplean para que, dadas unas condiciones, el resultado final sea el esperado. Este tipo de control se utiliza para minimizar la probabilidad de materialización del evento de riesgo.

Control Detectivo y Correctivo: Son las acciones que se toman una vez materializado el evento de riesgo. Pueden ser correcciones para eliminar la situación indeseable o las acciones correctivas para eliminar la causa del evento de riesgo. Este tipo de control se utiliza para minimizar el impacto del riesgo.

Los controles, de acuerdo con su modo de ejecución, se pueden clasificar en:

Control Manual: Acciones que son ejecutadas por completo con intervención humana.

Control dependiente de Tecnología: Control que efectúa parte de su funcionamiento de manera automática tras una ayuda manual o que requiere un componente tecnológico para poder ser ejecutado.

Control Automático: Control que es ejecutado sin necesidad de intervención humana.

Los controles acordes a su tipo (detectivo, correctivo o preventivo), o a su modo de ejecución (manual, dependiente de tecnología o automático), deben tener en cuenta la viabilidad de implementación y el costo de estos. Se debe propender por la implementación de controles preventivos y automáticos sobre cualquier otro tipo de control.

La clasificación de los controles puede estar asociada a:

Controles Operativos: Son aquellos controles enfocados a garantizar la ejecución de las actividades. Se encuentran soportados en los manuales, procedimientos, guías o instructivos definidos para desarrollar dicha actividad; también hacen parte las funciones y responsabilidades determinadas al personal, la infraestructura y todos los recursos dispuestos para la realización de dichas actividades.

Algunos ejemplos de controles operativos son: conciliaciones, consecutivos, verificación de firmas, listas de chequeo, registro controlado, segregación de funciones, niveles de autorización, custodia apropiada, procedimientos formales aplicados, pólizas, seguridad física, contingencias y respaldo, personal capacitado en aseguramiento y calidad.

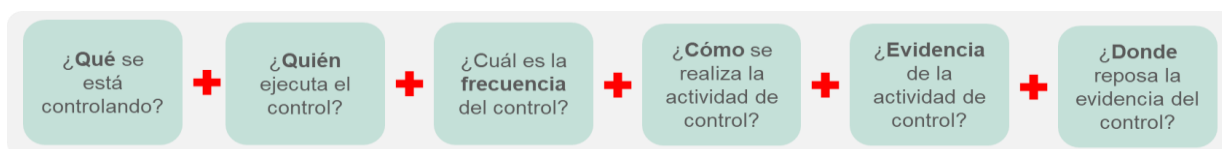
Controles Legales: Son aquellos en los cuales hacen parte la *normatividad*²⁴ interna y externa aplicable a PISA. Por ejemplo, Acuerdos, Resoluciones, etc.

6.3.3.2 Lineamientos o mejores prácticas para la redacción de controles

Con el fin de tener un criterio de referencia para documentar los controles de los riesgos operativos, a continuación, se mencionan algunos aspectos para tener en cuenta, por parte de los dueños de procesos, como mejores prácticas para la redacción de los mismos dentro de las matrices de riesgo operativo.

- El control debe mitigar la causa que genera el riesgo.
- El control ha de estar incluido en los procedimientos del proceso analizado y debe tener asignado un responsable de su ejecución.
- Los controles deberán ser claros tanto para quienes hayan de usarlos como por aquellos que de un modo u otro consulten la *Matriz ERM Sector Infraestructura*. La redacción de los controles ha de ser comprensible, exponiendo claramente la acción que realizan.

El control deberá atender a los siguientes interrogantes:



Adicionalmente, el control debe tener en cuenta el nivel de precisión que se desea tener para mitigar efectivamente el riesgo, este se puede ver afectado por:

- **Objetivo de la revisión:** El grado en que se revisa a detalle el paso a paso del proceso para prevenir o detectar errores, más allá de solamente identificar y explicar diferencias encontradas.
- **Alcance del control:** Un control que se realiza a un nivel más detallado generalmente es más preciso que uno realizado en un nivel superior. Por ejemplo, un análisis de variación de costos por etapa de proyecto normalmente es más preciso que un análisis a nivel general de proyecto.
- **Consistencia de los resultados:** Un control que se lleva a cabo de forma rutinaria y consistente, es generalmente más preciso que uno que se lleva a cabo de forma esporádica. Se recomienda que el control esté en función directa de la periodicidad de la operación generadora del riesgo.
- **Previsibilidad de las expectativas:** Algunos controles están diseñados para detectar errores mediante el uso de *indicadores clave*²⁵ sobre situaciones inusuales reportadas u otra información desarrollada sobre expectativas. La precisión de los controles depende de la capacidad para desarrollar las expectativas suficientemente precisas para resaltar discrepancias o errores potenciales.
- **Cobertura del control:** Un control puede ejecutarse en la totalidad de elementos en los que se realiza la revisión (es decir, en la población o mediante censo) o puede tomarse una muestra representativa que permita extrapolar los resultados de la validación. Un control dará mayor seguridad cuando se ejecuta sobre la totalidad de la población.

6.3.3.3 Implementación y evaluación de controles

En la implementación de controles se debe asegurar que estén claramente definidos, documentados, implementados, conocidos y puestos en marcha acorde a los criterios establecidos por parte de sus responsables.

²⁴ Normatividad: Conjunto de disposiciones de carácter jurídico que permite regular una materia, actividad o sector específico. Incluyen la Constitución Nacional, leyes, decretos, resoluciones, reglamentos técnicos, entre otros.

²⁵ Indicadores Clave de Riesgo (KRI): Conjunto de métricas cuantitativas para los riesgos relevantes a los que está expuesta la compañía, que reflejan su perfil de riesgo y que permiten el control y seguimiento del mismo.

En la valoración de los riesgos identificados, se tendrán en cuenta la calidad de los controles establecidos para el tratamiento de estos, para así valorar el *riesgo residual*²⁶. Los criterios base para determinar la calidad de los controles se encuentran establecidos en la *Matriz ERM Sector Infraestructura*.

La calificación de estos criterios arroja la evaluación del diseño de cada control, para así definir el nivel de exposición por causa, una vez aplicados los controles.

Después de evaluado el diseño del control, se establece el nivel de ejecución del mismo, con lo cual se determina el nivel de Riesgo Residual.

6.3.3.4 Tratamiento de los Riesgos

El tratamiento de los riesgos involucra identificar las opciones para tratar los riesgos, evaluar esas opciones (Costo-Beneficio, Viabilidad Operativa, Técnica y Jurídica, etc.) y preparación de planes para tratamiento de los riesgos con su implementación.

Se deben tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto.

- **Evitar el riesgo:** Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar. Se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.
- **Compartir o Transferir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras compañías, como en el caso de los contratos de seguros. Es así como, 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 sólo lugar.
- **Mitigar el riesgo:** Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La mitigación del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.
- **Aceptar el riesgo:** Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el dueño del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

El nivel permitido o aceptado por PISA en su evaluación residual son los riesgos cuya severidad sea baja o muy baja.

Para los riesgos inherentes con severidad extrema, alta o moderada, el dueño del proceso deberá establecer planes de acción que tengan como objetivo disminuir su probabilidad y/o su impacto, ya sea a través de la creación de nuevos controles, la implementación de modificaciones a los controles existentes o la creación de actividades de corrección inmediata, con el fin de disminuir su severidad al nivel aceptado por PISA (severidad baja o muy baja).

6.3.4 Monitoreo

Es necesario monitorear frecuentemente los riesgos, la efectividad de los planes de tratamiento, las estrategias y el sistema de administración que se establece para controlar la implementación.

Los riesgos y la efectividad de los controles necesitan ser revisadas frecuentemente para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos o la aparición de riesgos remanentes.

Es importante tener en cuenta que pocos riesgos permanecen estáticos. Es esencial realizar una revisión periódica con el fin de asegurar que el plan de administración mantiene su relevancia. Pueden cambiar los factores que generan los riesgos o las condiciones usadas para calificar la probabilidad/frecuencia y el impacto sobre los resultados, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento.

Los dueños de proceso son responsables de contactar al Área de GRC en los casos en que existan cambios significativos en sus procesos y se requiera ejecutar nuevamente el proceso de identificación, medición y control de riesgos operativos.

²⁶ Riesgo Residual: Nivel resultante del riesgo después de aplicar los controles.

En consecuencia, es necesario repetir regularmente el ciclo de administración de riesgos. Por lo tanto, el monitoreo será una parte integral de la administración de riesgos de PISA.

En el monitoreo anual al sistema, se enfocará en:

- Verificar que los controles que mitigan los riesgos inherentes altos y extremos estén funcionando en forma oportuna, eficiente y efectiva.
- Verificar que los riesgos residuales se encuentren en los niveles de aceptación establecidos y aprobados por la Junta Directiva.

De esta etapa, se desprenden continuos ajustes al sistema para hacerlo efectivo de acuerdo con sus propósitos, que son:

- Asegurar que los riesgos residuales sean de severidad baja o muy baja.
- Mantener actualizados los mapas de riesgos de los procesos de PISA, teniendo en cuenta los cambios que se den en éstos.
- Analizar el comportamiento de los eventos de pérdida, con el fin de determinar su incidencia en la probabilidad e impacto de los riesgos.
- Asegurar que los nuevos procesos, actividades y sistemas usados sean incluidos en el sistema.

6.3.4.1 Reportes

El Área de GRC reportará anualmente al Gerente General y a la Junta Directiva, el desempeño del SARO teniendo en cuenta:

- Nivel de implementación del sistema.
- Eventos de Riesgo Operativo presentados y planes de acción generados.
- Estatus de los planes de acción vigentes.
- Eventos relacionados con el curso del negocio, procesos o actividades identificados que puedan afectar el SARO o requerir una modificación de este.

Igualmente, deberá efectuar los reportes periódicos requeridos por Grupo Aval, Corficolombiana y Proindesa.

6.3.4.2 Planes de Acción

El Área de GRC realizará seguimiento mensual a:

- Los eventos de riesgo operativo (ERO) que no posean un plan de acción definido.
- Los planes de acción definidos para los ERO anotados en el documento *Registro de Eventos de Riesgo Operativo*.

El dueño del plan de acción es el único responsable de certificar que el plan ha sido cerrado a conformidad ante el Área de GRC.

6.4 REGISTRO DE EVENTOS DE RIESGO OPERATIVO

El Área de GRC es la responsable de establecer y mantener actualizado el registro de eventos de riesgo operativo de PISA.

El registro de eventos de riesgo operativo es un inventario de los eventos que implican la materialización de un riesgo operativo, esto con el objetivo de:

- Generar los planes de acción y la modificación necesaria en los controles, procesos, perfil de riesgo, riesgos y supuestos usados en la ejecución del SARO.
- Ser una fuente de información para La Alta Dirección respecto de la exposición de PISA al riesgo operativo.
- Servir de insumo para la generación de revelaciones en los estados financieros, en caso de que el evento de riesgo operativo esté dentro del nivel de tolerancia o capacidad de riesgo.

El Registro de eventos de riesgos operativo debe cumplir con los criterios de disponibilidad, confidencialidad, integridad y privacidad de la información allí contenida y llevará cuenta de todos los eventos que impliquen los siguientes tipos de pérdidas:

- Tipo A: Generan pérdidas y afectan el estado de resultados de PISA.
- Tipo B: Generan pérdidas y no afectan el estado de resultados de PISA.

6.4.1 Reporte de Eventos

En la situación en la que cualquier colaborador de PISA identifique que se ha presentado un evento que implica la materialización de un riesgo operativo (sea que este riesgo haya sido o no identificado con antelación en la *Matriz ERM Sector Infraestructura*), es decir, si el evento comprende la falla en un proceso, persona, sistema informático, infraestructura o representa un perjuicio para PISA debido a un acontecimiento externo, deberá dirigirse al Oficial de Riesgo Operativo (ORO) del proceso afectado para que este notifique la existencia del evento de riesgo operativo (ERO).

El colaborador que identifique el evento deberá llevar la información soporte de este al Oficial de Riesgo Operativo del proceso al que corresponda el ERO, quién, en primer lugar, identificará:

- Si el evento implica otros procesos. En cuyo caso contactará a los demás dueños de proceso para realizar un solo análisis del evento. El primer dueño de proceso contactado en razón del evento será el responsable del ERO ante el Área de GRC y ejecutará toda su documentación.
- Si existen controles vulnerados durante la ejecución del evento.
- Qué riesgos dentro de sus procesos (y de los demás dueños de proceso, si aplica) se materializaron con el evento.
- Si existen controles, circunstancias o acciones que PISA puede ejecutar para mitigar el impacto del evento.
- La cuantía de dinero que es posible mitigar gracias a los controles, circunstancias o acciones identificadas.

Posterior a la identificación, el responsable del ERO diligenciará el Formato de *Evento de Riesgo Operativo* y lo remitirá mediante correo electrónico al Área de GRC para su validación. Una vez validado por el Área de GRC, ésta se encargará de documentarlo en el *Registro de Eventos de Riesgo Operativo* y será el responsable de ejecutar seguimiento a los planes de acción definidos.

De acuerdo con instrucciones corporativas, se deberá informar de manera inmediata a Grupo Aval cualquier evento que, de forma unificada o individual, supere el límite de pérdida potencial o bruta del umbral, es decir cuantías mayores y/o iguales a los cien millones de pesos (\$ 100.000.000), También se consideran *eventos de alto impacto*²⁷ los eventos tipo B que a juicio del Coordinador de GRC, previo el visto bueno de la Gerencia General, se consideren importantes o materiales en términos reputacionales o regulatorios.

6.5 PLAN DE CONTINUIDAD

La continuidad del negocio es el conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar con la operación en caso de interrupción. Para ello, PISA debe definir los mecanismos necesarios para establecer las funciones y responsabilidades que se deben llevar a cabo en el desarrollo de los planes de contingencia.

6.6 ACTUALIZACIÓN

Se llevará a cabo anualmente y/o de acuerdo con las actualizaciones realizadas de los riesgos y controles de cada uno de los procesos de PISA, junto con los dueños de los procesos y/o ejecutores de estos, o sus delegados; con el fin de actualizar los mapas de riesgos existentes, de acuerdo con los cambios, observaciones u oportunidades de mejoras, tanto de entes de control externos como internos, respecto de los procesos auditados, hallazgos y/o eventos materializados que se hayan presentado.

²⁷ Eventos de Alto Impacto: corresponde a cualquier evento que supere el límite del umbral monetario establecido y/o tengan una importancia material con una posible afectación a la marca (servicio) o impactos regulatorios.

6.7 CAPACITACIÓN

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

Esta cultura organizacional, se encuentra soportada en la observancia la POLÍTICA DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO, el CÓDIGO DE BUEN GOBIERNO, la POLÍTICA ANTICORRUPCIÓN, así como la aplicación del CÓDIGO DE ÉTICA Y CONDUCTA y la adecuada ejecución de los procedimientos dispuestos por PISA y las capacitaciones de riesgo operativo que se brinden.

6.7.1 Divulgación

En línea con lo anterior, la divulgación debe incluir:

- La Política del Sistema de Administración del Riesgo Operativo – SARO debe ser socializada a los colaboradores de PISA.
- Se debe garantizar que el mapa de riesgos operativos de cada proceso sea de fácil acceso y de conocimiento de los colaboradores de PISA 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 de proceso o programas de tecnología, para presentarlos al dueño del proceso para su aprobación.
- La copia de los mapas de riesgo debe reposar en el servidor de PISA y deben encontrarse disponibles para los órganos de control y vigilancia internos y externos cuando estos lo requieran.

7 DOCUMENTO DE APROBACIÓN

Junta Directiva N° Acta 410 del 18 de febrero de 2025.

8 DOCUMENTOS RELACIONADOS

CÓDIGO	NOMBRE DEL DOCUMENTO
OP-DG-03	Plan de Continuidad del Negocio
TIC-IT-06	Plan de Contingencias - Sistema de Recaudo
GRC-DG-02	Política Anticorrupción
PE-DG-06	Código de Ética y Conducta
PE-DG-09	Código de Buen Gobierno
N/A	Instructivo mejores prácticas en el manejo de las pérdidas por Riesgo Operativo

9 FORMATOS RELACIONADOS

CÓDIGO	NOMBRE DEL FORMATO
N/A	Registro de Eventos de Riesgo Operativo
N/A	Reporte de Eventos de Riesgo con Alto Impacto
N/A	Matriz ERM Sector Financiero

10 CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
23-09-2009	01	Primera versión del documento
06-05-2011	02	El grupo directivo de PISA está comprometido con la identificación de riesgos potenciales considerados críticos por su impacto y consecuencias en la operatividad de la empresa. Lo anterior se ve soportado con la implementación del Sistema de Control Interno, enfocado a la prevención, mitigación y medidas de contingencia en caso de su ocurrencia.
16-06-2011	03	Se establece el compromiso de la Organización frente a la gestión y control de sus riesgos críticos
23-02-2016	04	Se define el Riesgo Operativo como "la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal ¹ y reputacional ² , asociados a tales factores 5.1 Política para la Gestión del Riesgo Operativo 5.2 Estructura Organizacional del SARO 6. Metodología Sistema De Administración Del Riesgo Operativo Calificación de Probabilidad Calificación de Impacto
29-08-2017	05	Se hace revisión de los lineamientos contenidos en este documento versus los establecidos por la "POLÍTICA CORPORATIVA PARA LA GESTIÓN DEL RIESGO OPERATIVO" y se hacen los ajustes necesarios, los cuales incluyeron ajustes de forma y redacción. Para facilidad de identificación de los cambios aplicados, estos se encuentran en formato subrayado, adicionalmente (Inclusión de nuevas definiciones, Nuevo numeral, Inclusión de los lineamientos utilizados en el desarrollo de la Gestión de Riesgo Operativo a nivel Colombia y a nivel internacional, Nuevo numeral, el cual establece que la compañía seleccionó a COSO (Committee on Sponsoring Organizations of the Treadway Commission) como marco para la evaluación de su Sistema de control interno, Nuevo numeral, el cual referencia los 12 principios que se acogen para la Administración de Riesgo Operativo, Nuevo numeral, el cual indica las fases de la metodología de gestión SARO, Nuevo numeral y donde las 4 etapas son: (i) Identificación, (ii) Medición, (iii) Control, (iv) Monitoreo, Nuevo numeral y en el cual se indican cuáles son los elementos del modelo y que buscan obtener una efectiva administración del riesgo operativo (Políticas, Procedimientos, Documentación, Estructura Organizacional, Órganos de Control, Herramientas Tecnológicas, divulgación, Capacitación)
Nº Acta 343 29-11-2019	06	Todo el documento se alinea con directrices corporativas y a la estructura documental del SIG. 27/05/2022 – Se realiza el siguiente cambio menor: <ul style="list-style-type: none"> Se cambia el tipo de sociedad de la empresa PROYECTOS DE INFRAESTRUCTURA S.A., ahora PROYECTOS DE INFRAESTRUCTURA S.A.S, debido a que se transformó en una sociedad por acciones simplificadas. Se reemplaza el término Compañía por PISA. Se actualiza el nombre de los siguientes cargos: <ul style="list-style-type: none"> o Presidente por Gerente General o Gerente Financiero por Director Financiero o Director de GRC / Líder del Área de Cumplimiento/Riesgos por Coordinador de GRC
Nº Acta 393 12-12-2023	07	Todo el documento se alinea con la metodología del Modelo GRC, lo cual incluye: <ul style="list-style-type: none"> Se ajustan los objetivos específicos, el alcance, las definiciones y los formatos relacionados del documento. Se actualizan las tablas de probabilidad e impacto. Se incluyen los apartados de declaración de compromiso, las políticas para la administración del riesgo operativo, las responsabilidades de acuerdo con el modelo de las tres líneas. Se ajustan las responsabilidades de los actores claves de la gestión del riesgo. Se elimina el apartado de principios. Se ajustan, dentro de las políticas de operación del documento, la política de riesgo operativo y las etapas del modelo. Se incluye la directriz de reporte inmediato a Grupo Aval cuando se supere el límite de pérdida potencial. 23/05/2024 – Se realiza el siguiente cambio menor: <ul style="list-style-type: none"> Se actualiza el logo de PISA y la portada del documento, de acuerdo con la nueva imagen corporativa.
Nº Acta 410 18-02-2025	08	Se realiza el siguiente ajuste. <ul style="list-style-type: none"> Se incluye en el alcance nota al pie para referenciar a concesiones CCFC, de acuerdo con lo establecido en el otrosí No. 5 del contrato de prestación de servicios suscrito entre PISA y CCFC, y a las instrucciones dadas por la junta directiva. Se actualiza el nombre del área responsable de la autorización para el acceso del documento pasando del Área de Mejoramiento y Sostenibilidad a Responsable de Procesos.