

# POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

· Código: GRC-DG-06

Versión: 04

**CONTENIDO**

1	FINALIDAD .....	2
2	ALCANCE DEL SISTEMA DE GESTIÓN DE RIESGOS (SGR) .....	2
3	POLÍTICAS DE OPERACIÓN .....	2
3.1	Principios .....	3
3.2	Metodología de gestión .....	5
3.3	Estructura y gobierno para la gestión integral de riesgos .....	6
3.4	Actores del modelo .....	11
3.5	Marco general de control interno .....	12
3.6	Riesgos .....	13
3.7	Medición y mitigación del riesgo .....	15
3.8	Modelo integrado GRC (Gobierno, Riesgo, Cumplimiento) .....	19
3.9	Gestión de la información .....	19
3.10	Prácticas de presentación de informes de riesgos .....	20
4	DOCUMENTOS RELACIONADOS .....	20
5	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 aprobado por la Junta Directiva mediante el acta N° 410 del 18 de febrero del 2025 y emitido el 25 de marzo de 2025

## 1 Finalidad

La presente Política tiene como objetivo general contribuir en la generación de una arquitectura de gestión de riesgos en Proyectos de Infraestructura S.A.S. (en adelante PISA), mediante el establecimiento de principios, roles y responsabilidades respecto a las políticas, procedimientos, metodologías y lineamientos sobre esta materia, definiendo líneas de reportes que permitan una visión de los riesgos<sup>1</sup> a los que está expuesta PISA y la adopción de las medidas de control que correspondan.

## 2 Alcance del Sistema de Gestión de Riesgos (SGR)<sup>2</sup>

Es el conjunto integrado de principios, criterios generales, políticas, procedimientos, infraestructura, controles<sup>3</sup>, capacitación, divulgación y, en general aquellos parámetros mínimos que PISA debe observar con el objeto de identificar, medir, monitorear, controlar o mitigar los riesgos a los que se ve expuesta, para mantenerlos adecuadamente evaluados.

Para ello, los órganos de dirección, administración y control de PISA deben alinear sus políticas y mecanismos especiales para su adecuada administración, no sólo desde la perspectiva de su cubrimiento a través de un sistema de provisiones u otros mitigantes de riesgo, sino también a través de la administración<sup>4</sup> de toda la cadena de valor de cada proceso.

El Sistema de Gestión de Riesgos, dependiendo de su naturaleza, debe contar al menos con los siguientes componentes básicos:

- Políticas de administración del riesgo y difusión de la cultura de riesgo – control.
- Pautas de gobierno incluyendo asignación de roles y responsabilidades.
- Procesos<sup>5</sup> de administración del riesgo.
- Mapas de administración de riesgo.
- Para los riesgos que aplique, modelos internos o de referencia para la estimación o cuantificación de pérdidas<sup>6</sup> esperadas.
- Sistema de provisiones, cuando a ello hubiere lugar, para cubrir el riesgo.

## 3 Políticas de operación

- Las directrices y principios consagrados en esta Política se determinan basados en la necesidad de tener reglas y pautas de control comunes y claramente formuladas sobre agregación de datos referentes a riesgos y controles y a la presentación de informes de riesgos homogéneos que permitan una visión consistente de la situación de riesgo consolidada de PISA.
- La solidez del Sistema de Gestión de Riesgos constituye una parte integral de la propuesta de valor que ofrece PISA, por lo que una aplicación eficaz de esta Política debe incrementar el valor de PISA, al permitir facilitar ahorros, maximizar la ejecución de estrategias y optimizar las operaciones.
- Los lineamientos que figuran en este documento aplican a los datos que utiliza PISA para gestionar los riesgos que afronta, lo que incluye información fundamental para dicha gestión. Los datos sobre riesgos y los correspondientes informes deben

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> Controles: Cualquier medida que tome PISA y otras partes, para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos.

<sup>4</sup> Administración: Gerente General, Gerentes de las áreas Jurídica y Administrativa.

<sup>5</sup> Procesos: Conjunto de actividades relacionadas entre sí, las cuales transforman elementos de entrada en resultados o elementos de salida y generan un valor agregado al negocio.

<sup>6</sup> Pérdidas: Cuantificación económica de la ocurrencia de un evento de riesgo, así como los gastos derivados de su atención.

proporcionar la capacidad de hacer seguimiento y controlar los riesgos en función del apetito de riesgo<sup>7</sup> determinado por PISA.

Los Principios deben aplicarse a los Sistemas de Administración de Riesgo de PISA y están incluidos a título enunciativo y no limitativo.

### 3.1 Principios

La Política para la Gestión Integral de Riesgos de PISA, deberá regirse por los siguientes principios de general aceptación a nivel internacional, como buenas prácticas para un marco efectivo de aplicación y control de riesgos.

#### 3.1.1 PRINCIPIO 1. La cooperación, coordinación e intercambio de información entre PISA y las partes relacionadas<sup>8</sup> debe ser permanente y oportuna

PISA deberá comunicar en su interior, a todos los niveles, la cultura, filosofía y políticas de riesgos (como un elemento del ambiente de control). En desarrollo de este principio, PISA deberá propender por la generación de mecanismos efectivos de reporte de información hacia la Alta Dirección<sup>9</sup>, que sea veraz, comprensible y completa, de forma que constituya un efectivo apoyo para la adecuada administración de los riesgos.

PISA debe vigilar la coordinación del intercambio de información. PISA está obligada a suministrar a la matriz información sobre sus contrapartes<sup>10</sup> y actividades de alto riesgo que sea relevante a efectos de las normas globales (sin menoscabo del cumplimiento de normas sobre habeas data y otras normas aplicables) y a responder de manera oportuna a las solicitudes de información remitidas desde la matriz.

Las políticas y procedimientos deben tener en cuenta los aspectos y obligaciones relacionados con la protección de datos a escala local y con la legislación y regulación en materia de privacidad. También deben tener en cuenta los diferentes tipos de información que pueden compartirse dentro del grupo y los requisitos de almacenamiento, recuperación, intercambio, distribución y eliminación de esa información.

Para el efecto, Grupo Aval ha definido mecanismos de reporte por cada uno de los riesgos, para establecer funciones y responsabilidades en el proceso y garantizar el intercambio de información eficiente y efectiva, conforme a los parámetros definidos para cada riesgo.

#### 3.1.2 PRINCIPIO 2. Normas prudenciales y cobertura

PISA ha establecido e implementado un marco general normativo para cada uno de los riesgos clave mediante el establecimiento de Políticas, basadas en las Políticas Corporativas vigentes expedidas por Grupo Aval, las autoridades de supervisión y control, así como en las mejores prácticas del mercado. Para el efecto, PISA debe adoptar o adaptar las directrices impartidas por Grupo Aval y Corficolombiana mediante políticas, instrucciones, procedimientos o cualquier tipo de pronunciamiento.

<sup>7</sup> Apetito de Riesgo: Es la exposición al riesgo que una empresa está dispuesta a asumir en el desarrollo de su actividad con el fin de alcanzar sus objetivos estratégicos y cumplir con su plan de negocios. El importe total de los riesgos asumidos será la base inicial para el desarrollo de todos los procesos de gestión de riesgos y de sus límites.

<sup>8</sup> Partes Relacionadas: Son las personas naturales o jurídicas, que tienen con todas o con algunas de las Compañías que integran el conglomerado, vínculos de administración, de propiedad directa e indirecta igual o superior al 5%, y las sociedades donde cualquiera de las personas enunciadas anteriormente tenga una participación directa o indirecta, igual o superior al 10%.

<sup>9</sup> 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.

<sup>10</sup> Contraparte: Hace referencia a cualquier persona natural o jurídica con la que PISA tenga vínculos comerciales, de negocios contractuales o jurídicos de cualquier orden. Entre otros, son contrapartes, los accionistas, colaboradores, clientes y proveedores de bienes o servicios.

### 3.1.3 PRINCIPIO 3. Evaluación independiente

Corresponde a Auditoría Interna desarrollar y mantener una sólida comprensión de las operaciones de PISA, así como requerir las acciones correctivas oportunas que estimen y/o garanticen el cumplimiento del *control interno*<sup>11</sup>, a través de la realización de las actividades de auditoría que estime pertinentes, de acuerdo con su criterio y con la independencia que la caracteriza, enfocada a generar cohesión a nivel de PISA.

### 3.1.4 PRINCIPIO 4. Disponer de sistemas de control

Al diseñar escenarios para identificar eventos o situaciones de riesgo, PISA debe considerar el perfil de riesgo de sus contrapartes, elaborado a partir de metodologías que permitan la evaluación de riesgos, así como de la información obtenida en sus labores de conocimiento de sus clientes, colaboradores y proveedores, sector en el que opera y del ambiente macroeconómico, entre otros.

### 3.1.5 PRINCIPIO 5. Realizar un seguimiento continuo

El seguimiento continuo constituye un aspecto esencial de una sólida y eficaz gestión del riesgo. Para el efecto, PISA debe gestionar eficazmente sus riesgos con base en el conocimiento de las actividades financieras/operativas de sus contrapartes, así como del sector en el que opera y del ambiente macroeconómico.

### 3.1.6 PRINCIPIO 6. Autocontrol

El Sistema de Gestión de Riesgos de PISA debe propender por el autocontrol, entendido como la capacidad de las personas que participan en los distintos procesos, de considerar el control como parte inherente de sus responsabilidades, campos de acción y toma de decisiones, asegurando que se tengan implementados y documentados los controles para mitigar los riesgos a los que se encuentre expuesta. Los métodos y procedimientos para la evaluación de la implementación de los controles pueden ser integrados como parte de las responsabilidades diarias (evaluaciones o monitoreo continuo) o implementados de manera específica (prueba periódica de controles) a través de pruebas independientes.

En desarrollo de este principio, los colaboradores que participan en los distintos procesos y la Alta Dirección, serán responsables de identificar, evaluar, medir, controlar, monitorear y reportar los riesgos, definiendo metodologías y asegurando que la administración de riesgos es consistente.

Con las evaluaciones continuas se supervisa la presencia y el funcionamiento de los componentes de control interno en el curso ordinario de la gestión del negocio. Pueden ser llevadas a cabo por los superiores directos de quien realiza las operaciones o funciones correspondientes. Estos colaboradores deben ser profesionales competentes, que dispongan de experiencia y conocimiento suficientes para comprender los temas evaluados.

En el mismo sentido, el autocontrol puede incluir pruebas independientes, las cuales no necesariamente están integradas dentro del negocio, pero son de gran utilidad en la evaluación del sistema de control interno; dentro ellas se incluyen observaciones, consultas y revisiones, entre otros, y pueden ser realizadas por personal independiente a la operación diaria pero que se encuentren capacitados sobre la forma en que funcionan las actividades sujetas a evaluación. PISA puede utilizar colaboradores de diferentes áreas operativas o funcionales para hacer las evaluaciones.

### 3.1.7 PRINCIPIO 7. Liquidez

PISA deberá contar con mecanismos y procedimientos que identifiquen, midan, monitoreen y controlen el riesgo de liquidez, con el objetivo de monitorear la suficiencia de recursos para atender las necesidades de liquidez en tiempos normales y durante períodos de estrés.

---

<sup>11</sup>Control Interno: Es el sistema integrado por un conjunto de políticas, métodos, principios, normas, procedimientos y mecanismos de prevención, control, evaluación y de mejoramiento continuo de PISA que le permiten tener una seguridad razonable acerca de la consecución de los objetivos previstos, de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por PISA.

### 3.1.8 PRINCIPIO 8. Marco de gestión de riesgos

PISA debe elaborar sus propias políticas independientes, exhaustivas y eficaces para cada uno de sus riesgos, en lo que legalmente le corresponde o según lo establezca Corficolombiana o Grupo Aval. Para el efecto debe guiarse por los parámetros mínimos consagrados en las normas vigentes, así como en las directrices corporativas impartidas por Corficolombiana o Grupo Aval para cada uno de sus riesgos.

### 3.1.9 PRINCIPIO 9. Cultura de gestión de riesgos

PISA debe contar con los procesos y procedimientos necesarios para generar y mantener una cultura de gestión de riesgos.

### 3.1.10 PRINCIPIO 10. Niveles de tolerancia al riesgo y la política de apetito por riesgo

PISA debe establecer, en sus políticas de administración de riesgo, niveles de tolerancia al riesgo<sup>12</sup>, atendiendo los niveles definidos desde Grupo Aval en esta materia, los cuales deben ser aprobados por la Alta Dirección.

Estas políticas deben ser definidas atendiendo lo indicado en el siguiente gráfico, cuando el tipo de riesgo lo amerite:



### 3.1.11 PRINCIPIO 11. Seguimiento a Riesgos Materiales

PISA como parte del objetivo de la presente Política para la Gestión Integral de Riesgos, debe dar seguimiento a los riesgos materiales determinados teniendo en cuenta el apetito y nivel de tolerancia al riesgo aprobados por la Junta Directiva.

### 3.1.12 PRINCIPIO 12. Transacciones y Exposiciones ENTRE PARTES RELACIONADAS

Las transacciones y exposiciones entre partes relacionadas pueden facilitar las sinergias dentro de las diferentes Compañías y, por ende, conducir a una rentabilidad sana y máxima, mejoras en la administración de riesgos, y un control más eficaz del capital y financiamiento, siempre y cuando se eviten eventuales contagios que compliquen su resolución.

PISA debe monitorear las transacciones y exposiciones entre partes relacionadas relevantes e importantes de manera oportuna.

Igualmente debe establecer lineamientos de conducta y ética que oriente la actuación de los colaboradores de PISA, incluyendo disposiciones sobre la confidencialidad de la información, manejo de información privilegiada y conflictos de interés.

PISA debe adoptar y poner en marcha sistemas y procesos eficaces a nivel individual; así como las operaciones y exposiciones entre partes relacionadas e implementar mecanismos para asegurar que las mismas se realicen a precios y condiciones de mercado.

## 3.2 Metodología de gestión

De acuerdo con la naturaleza del riesgo, la metodología de gestión de riesgos debe comprender, como mínimo, las siguientes fases:

Identificación	Medición	Monitoreo	Control
<ul style="list-style-type: none"> <li>Catálogo de Riesgos genéricos</li> <li>Identificación de riesgos relevantes</li> </ul>	<ul style="list-style-type: none"> <li>Valoración de los riesgos relevantes</li> <li>Generación del Perfil de riesgos de la Compañía</li> </ul>	<ul style="list-style-type: none"> <li>Generación de reportes a las diferentes instancias</li> <li>Compartir eventos relevantes y mejores practicas</li> </ul>	<ul style="list-style-type: none"> <li>Planes de mejoramiento y seguimiento a los controles</li> </ul>

<sup>12</sup> Tolerancia al Riesgo: Nivel aceptable de desviación del riesgo según el Apetito de Riesgo definido en relación con la consecución de los objetivos de negocio.

- **Identificación:** El objetivo de esta etapa es generar una lista exhaustiva de riesgos con base en aquellos eventos que podrían crear, aumentar, prevenir, degradar, acelerar o retrasar el logro de los objetivos de PISA. Para desarrollar esta etapa se debe tener en cuenta el inventario de riesgos genéricos, así como identificar y documentar los procesos y establecer metodologías para identificar los eventos de riesgo.
- **Medición:** El propósito de esta etapa es facilitar la toma de decisiones acerca de cuáles riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento. Para esta etapa se debe establecer la metodología de medición de los eventos de riesgo, medir los eventos de riesgo (*Probabilidad*<sup>13</sup> e *Impacto*<sup>14</sup>) y así determinar el perfil de riesgo de PISA.
- **Monitoreo:** Con el fin de garantizar que la gestión de riesgo sea eficaz y continua, se desarrolla un proceso de seguimiento, en el cual se valida que los controles sean efectivos y que el *riesgo residual*<sup>15</sup> se encuentra dentro de los niveles de tolerancia establecidos por PISA, generando los reportes a que haya lugar a las diferentes instancias.
- **Control:** La selección de las opciones más adecuadas para el control de riesgos implica equilibrar los costos y los esfuerzos de la implementación frente a los beneficios derivados. Para llevar a cabo esta etapa se debe establecer una metodología para definir medidas de control y determinar el riesgo residual.

### 3.3 Estructura y gobierno para la gestión integral de riesgos

#### 3.3.1 Estructura del grupo

Grupo Aval, como sociedad matriz da seguimiento consolidado a la gestión integral de riesgos de PISA a través de Corficolombiana. PISA debe contar con una estructura funcional y de gestión transparente, que sea consistente con su estrategia y perfil de riesgo global, necesaria para la ejecución apropiada del proceso, que permita generar información para la toma de decisiones.

En cuanto a su estructura y gobierno, PISA se caracteriza por:

- Ser totalmente autónoma en sus operaciones y contar con una estructura administrativa independiente.
- Las decisiones de asignación de recursos son tomadas por la Alta Dirección.
- Tener independencia para adoptar modelos o mejores prácticas adicionales siempre y cuando no vayan en contravía de las normas y/o directrices de Grupo Aval.
- Manejar la contabilidad de forma independiente.
- Manejar de forma autónoma la gestión de los riesgos inherentes.

#### 3.3.2 Líneas frente al riesgo

PISA debe estructurar las funciones y responsabilidades frente a sus riesgos, siguiendo el esquema de las tres líneas, esto es, considerando (i) la gestión por línea de negocio, (ii) una función de gestión del riesgo independiente, y (iii) una revisión independiente.

##### 3.3.2.1 Primera Línea

La primera línea la constituyen cada una de las áreas o colaboradores al interior de PISA que gestionan el negocio. Esto significa que tales áreas o colaboradores son responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos inherentes a las actividades, procesos y sistemas de los que son responsables. Quienes conforman esta línea deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas. Para el efecto PISA debe:

- Especificar claramente y por escrito las políticas y procedimientos para la gestión de sus riesgos y comunicarlos / publicarlo a todos los colaboradores.

<sup>13</sup> Probabilidad: Es la posibilidad que un riesgo se materialice. Para determinar la probabilidad se puede utilizar el análisis cualitativo y/o cuantitativo.

<sup>14</sup> Impacto: Es la pérdida (monetaria o no monetaria) generada por la materialización de un riesgo, que puede ser medida de manera cualitativa y/o cuantitativa.

<sup>15</sup> Riesgo Residual: Nivel resultante de riesgo después de aplicar los controles.

- Incluir una descripción clara de las obligaciones de los colaboradores y de las instrucciones que deben seguir, así como orientaciones para que la actividad de PISA cumpla las regulaciones, políticas, procedimientos y lineamientos que conforman su arquitectura de gestión integral de riesgos.
- Implementar procedimientos internos para detectar y notificar operaciones que generan riesgo y los controles para su mitigación.
- Disponer de políticas y procesos adecuados para seleccionar a su personal, a fin de garantizar unos elevados principios éticos y profesionales.
- Implementar programas de formación del personal de modo que sus colaboradores estén adecuadamente capacitados para aplicar y ejecutar las políticas y procedimientos de gestión del riesgo de PISA.
- Adaptar la programación y contenido de la inducción y formación para el personal de las distintas áreas de acuerdo con sus necesidades y con el perfil de riesgo de PISA bajo la premisa de que: las necesidades de formación varían dependiendo de las funciones de los colaboradores y de las responsabilidades de los distintos puestos de trabajo, así como de su antigüedad. La organización y los materiales de los cursos de formación deben adaptarse a la responsabilidad o función concreta de cada colaborador con el fin de garantizar que éste cuenta con suficientes conocimientos e información para aplicar eficazmente las políticas y procedimientos de riesgo. En virtud de lo anterior:
  - Los nuevos colaboradores deben recibir formación adecuada dentro del proceso de inducción a PISA.
  - Deben impartirse cursos de actualización para garantizar que el personal mantiene un conocimiento vigente de sus obligaciones y que sus destrezas se mantienen al día. El alcance y frecuencia de esta formación debe adaptarse a los factores de riesgo a los que los colaboradores se encuentren expuestos al tenor de sus responsabilidades y al nivel y naturaleza del riesgo presente en PISA.

### 3.3.2.2 Segunda Línea

Esta línea está conformada por el Área de GRC<sup>16</sup>, la cual debe hacer un seguimiento continuo al cumplimiento de todas las obligaciones en materia de riesgo, utilizando metodología junto con herramientas adecuadas de gestión del riesgo.

Como parte de la segunda línea (Responsable por la Administración de un Sistema de Riesgo)<sup>17</sup>, el Área de GRC es:

- Responsable de la verificación y cumplimiento de la normativa junto con las políticas de PISA; examen de los informes de anomalías para alertar a la Alta Dirección si se considera que la Administración no está aplicando los procedimientos para gestionar el riesgo de forma responsable.
- Es el punto de contacto para todas las consultas que realicen las autoridades internas y externas, incluidas las autoridades supervisoras o las autoridades jurisdiccionales.

Los intereses comerciales de PISA no deben oponerse al eficaz desempeño de las atribuciones anteriormente mencionadas del Área de GRC. Con independencia del tamaño de PISA deben evitarse posibles conflictos de interés. Así pues, para permitir juicios ecuanímenes y facilitar un asesoramiento imparcial a la Dirección, los colaboradores que pertenecen al Área de GRC no deben asumir competencias inherentes a la primera y tercera línea. Ante cualquier conflicto entre las líneas de negocio y las atribuciones de esta Área, deben existir procedimientos que garanticen que las cuestiones de riesgo reciban una consideración objetiva al más alto nivel.

<sup>16</sup> GRC (Gobierno, Riesgo, Cumplimiento): Es un modelo de gestión que promueve la unificación de criterios, la coordinación de esfuerzos y colaboración entre los diferentes involucrados en la dirección de PISA; a través de:

- La integración de los órganos o responsables del gobierno, la administración y gestión de riesgos, el control interno y el cumplimiento.
- La asignación puntual de roles y responsabilidades del personal clave.
- La formalización de los canales de comunicación.
- La aplicación de un enfoque basado en riesgos.
- La implementación de un programa de cumplimiento.

<sup>17</sup> Responsable por la Administración de un Sistema de Riesgo: Colaborador de la segunda línea (Coordinador de GRC) asignado por la Alta Dirección, encargado entre otros de las siguientes actividades:

- Informar periódicamente al comité de riesgos correspondiente acerca del cumplimiento de metas y objetivos en relación con la administración de riesgo.
- Someter a consideración del comité los resultados obtenidos de la cuantificación de exposiciones de riesgo.
- Monitorear la implementación de políticas e instrucciones relacionadas en los comités de riesgos.

El Coordinador de GRC también puede desempeñar la función de Líder SAGRILAFT o equivalente, si así lo permite la legislación. Este responsable debe rendir cuentas directamente a la Alta Dirección. En caso de separación de tareas, la relación entre los roles previamente citados y sus respectivas funciones deben definirse y conocerse con claridad.

### 3.3.2.3 Tercera Línea

La tercera línea juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de PISA, así como los procesos y sistemas que conforman, rindiendo cuentas al Comité de Auditoría. Las personas encargadas de las auditorías internas, que deben realizar estas revisiones, deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control. Esta revisión puede ser realizada por el personal de auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados, los cuales proveen un aseguramiento objetivo sobre la efectividad de la gestión de riesgos al Comité de Auditoría, a PISA en su calidad de sociedad matriz, a Corficolombiana y a Grupo Aval, para ayudar a asegurar que los riesgos claves de negocio están siendo gestionados apropiadamente y que el sistema de control interno implementado está siendo operado efectivamente.

## 3.3.3 Organigrama de responsabilidad frente al SGR

Grupo Aval, en relación con sus entidades subordinadas establece el marco de responsabilidad frente al Sistema de Administración de Riesgo:

### 3.3.3.1 Responsabilidad en Cabeza del Conglomerado Financiero

La Junta Directiva y/o Alta Gerencia de Grupo Aval propenden por la existencia de una estrategia y apetito de riesgo para cada tipo de riesgo, donde resulte pertinente, mediante el establecimiento de una Política para la Gestión Integral de Riesgos de la Organización (Nivel 1) y mediante Políticas Corporativas (Nivel 2) e instrucciones establecidas en forma concreta para los principales riesgos por la Vicepresidencia de Riesgo de Grupo Aval, que inciden sobre las actividades desarrolladas por cada una de sus entidades subordinadas y por el conglomerado, y se asegura que esta estrategia se implemente y ejecute en las diferentes entidades que lo conforman.

### 3.3.3.2 Responsabilidades de PISA como sociedad matriz

- Gestionar (identificar, medir, controlar y monitorear) sus riesgos bajo su entera responsabilidad conforme a las directrices generales, las políticas internas definidas y la normatividad vigente aplicable.
- Fomentar la cultura de gestión de riesgos por parte de sus entidades subordinadas.
- Velar por la gestión eficiente del riesgo por parte de sus entidades subordinadas.

### 3.3.3.3 Responsabilidades de PISA

- Gestionar sus riesgos bajo su entera responsabilidad conforme a la presente Política y demás lineamientos generales de Grupo Aval, teniendo en cuenta sus propias políticas internas definidas y la normatividad vigente aplicable.
- Asegurarse de que dispone de sistemas de información, que sean proporcionales a su tamaño, estructura organizativa o complejidad, basados en criterios de importancia relativa y en los riesgos.
- Comunicar a la Junta Directiva de forma puntual y oportuna, completa, comprensible y precisa, la información sobre la evaluación de los diferentes tipos de riesgo a los que se ve expuesta PISA, a fin de ilustrarlos para adoptar decisiones informadas.
- Propender porque sus subordinadas adopten e implementen la presente Política, las Políticas Corporativas, las directrices y lineamientos generales de Grupo Aval y armonicen sus propias políticas conforme a estos preceptos organizacionales.

- o Una vez formalizados, revisar por lo menos una vez al año, que los límites de los indicadores clave de riesgo (Key Risk Indicator -KRI), se mantengan alineados a la estrategia y cambios del entorno (interno y externo) de modo que las alertas generen valor para PISA.
- o Una vez formalizados, garantizar la actualización periódica de los distintos *tableros de control*<sup>18</sup>(indicadores claves) de riesgo de PISA y de subordinadas atendiendo los lineamientos corporativos.

Definir los protocolos frente a eventuales desviaciones de los límites definidos y los mecanismos de reporte.

### 3.3.3.4 Responsabilidades de la Junta Directiva y la Alta Dirección de PISA

En materia de riesgos, la Junta Directiva tiene, en general, las siguientes responsabilidades:

- o Conocer y aprobar las políticas en materia de riesgos.
- o Asegurar que la administración tenga implementada una adecuada Política para la Gestión Integral de Riesgos.
- o Asegurar la coordinación y comunicación efectiva con los responsables de la gestión de riesgos que le permita tomar las medidas que estime pertinentes.
- o Estar informado y tener entendimiento acerca de los procesos y actividades desarrolladas por la Alta Dirección en la administración y gestión de los riesgos de PISA, los cuales deben cumplir con los estándares y requerimientos relevantes incorporados en esta Política y en las Políticas Corporativas de cada riesgo.
- o Cuestionar a la Alta Dirección sobre el proceso estructurado para identificar, evaluar y reportar periódicamente los riesgos, el adecuado diseño y operatividad de controles que permitan mitigar los riesgos.
- o Requerir y recibir información por parte de la Alta Dirección sobre gestión de los riesgos y, si es el caso, sugerir que se realicen los ajustes o tomen medidas sobre aquellos aspectos que en su criterio no se hayan considerado.
- o Supervisar el proceso de reporte financiero periódico implementado por la Administración y revisar los estados financieros anuales antes de su publicación.
- o Recibir información sobre las principales denuncias de fraude identificadas y reportadas en PISA y evaluar el seguimiento dado por la Alta Dirección y el efecto que pudiera tener en el Sistema de Control Interno.
- o Contar con un Experto Financiero, el cual es el responsable de entender en detalle la operación financiera de PISA, su Control Interno y las implicaciones de falla en el mismo.
- o Analizar el reporte de avance del cumplimiento de la evaluación de control interno de la Ley Sarbanes - Oxley y dar recomendaciones sobre el mismo, cuando PISA esté incluida dentro del alcance de reporte.
- o Revisar las conclusiones de la Evaluación de Control Interno de Auditores Internos, Externos y de la Administración y considerar si las recomendaciones realizadas han sido implementadas.
- o Obtener informes periódicos de la Administración de PISA con respecto a asuntos de cumplimiento que tengan impacto material sobre los estados financieros de PISA, sus estrategias, operaciones o reputación.

En lo relacionado con riesgos, la Alta Dirección tiene, entre otras, las siguientes responsabilidades:

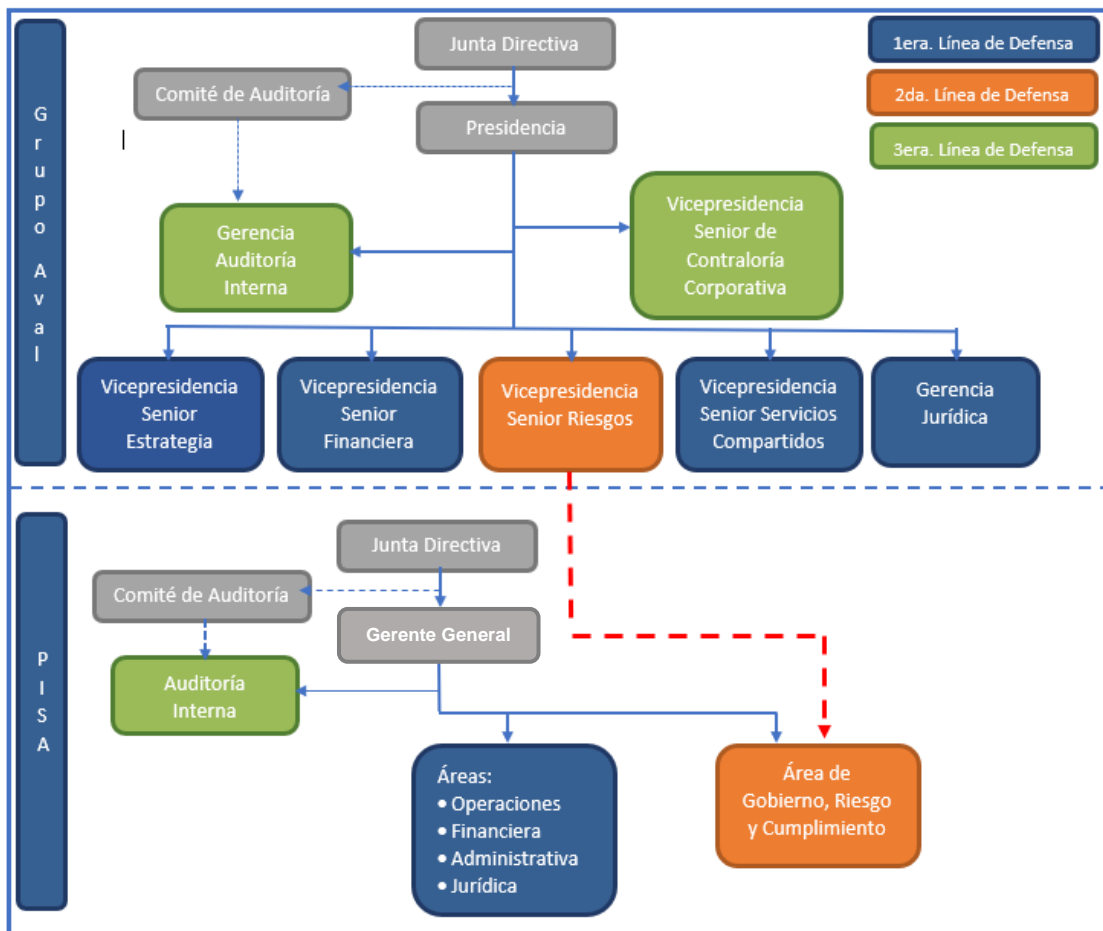
- o Velar por la aplicación de las políticas de cada uno de los riesgos, su gestión, monitoreo, control, planes de mejora e informes.
- o Asignar las competencias (roles y responsabilidades) en PISA, teniendo en cuenta la estructura de gobierno de esta para garantizar la gestión eficaz de las políticas y procedimientos de riesgo.
- o Cuando PISA esté incluida dentro del alcance de reporte, velar por el cumplimiento de la Ley Sarbanes-Oxley a nivel de Entidad y a nivel del Grupo, asegurándose que se tienen diseñados e implementados los controles, que se están realizando todas las actividades de cumplimiento definidas y certificar el resultado de la evaluación realizada sobre el Sistema de

<sup>18</sup> Tablero de Control: Tablero de indicadores de información consolidada, administrado por el Área de GRC.

Control Interno. Igualmente, entender la metodología de cumplimiento de esta Ley y estar de acuerdo sobre el alcance definido por la Alta Gerencia de Grupo Aval para su aplicación, así como expedir las certificaciones exigidas por dicha norma.

- o Analizar los informes de avance del cumplimiento de los riesgos y velar porque se estén aplicando de forma oportuna las remediaciones requeridas.
- o Informar a la Junta Directiva si existen deficiencias significativas, debilidades materiales o sospechas de fraude sobre los reportes financieros, que involucren a la Administración.
- o Propiciar una adecuada independencia y segregación de funciones<sup>19</sup> en la gestión de riesgos en la realización de las actividades del proceso.

### 3.3.3.5 Organigrama de la relación de Gestión de Riesgos de Grupo Aval y el Área de GRC de PISA.



<sup>19</sup> Segregación de Funciones: Asignación de las responsabilidades de autorización de transacciones, registro de transacciones y mantenimiento de la custodia de los activos a diferentes personas para reducir la oportunidad de que cualquier persona tenga la posibilidad de perpetrar y ocultar errores o fraude durante el normal desarrollo de sus funciones. La segregación de funciones debe ser habilitada mediante los sistemas de información, así como a través de controles manuales para restringir el acceso a los activos físicos, a fin de garantizar la separación de roles y responsabilidades en toda PISA.

### 3.4 Actores del modelo

Las responsabilidades de cada estamento de PISA frente al modelo corporativo y a su propio modelo es la siguiente:

- La Alta Dirección es responsable de aprobar las políticas para la administración de riesgos, así como los niveles de tolerancia al riesgo y la política de apetito de riesgo, que permitan una adecuada gestión de riesgos. Tales políticas deberán establecer los parámetros y lineamientos aplicables por tipo de riesgo y la forma en la cual se deberá administrar la exposición a los mismos.
- La Junta Directiva es responsable por conocer y supervisar periódicamente la exposición efectiva de PISA a los límites máximos de riesgo definidos, y plantear acciones de corrección y seguimiento en caso de desviaciones.
- El Comité de Riesgos de PISA 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:

- Riesgos operativos (legal, reputacional y de continuidad de negocio)
- Riesgo de Lavado de Activos, Financiación de Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva – SAGRILAF
- 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.
- 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 se reunirá con 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.

- La Administración es la dueña de los procesos y responsable de la administración de riesgos, es decir, de identificar, evaluar, medir, controlar, monitorear y reportar los riesgos, definiendo metodologías, y asegurando que la administración de riesgos sea consistente con la estrategia y las políticas establecidas por tipo de riesgos.
- La Alta Dirección de PISA cuenta con una política de delegación de niveles jerárquicos y funciones a cargo de los órganos de dirección, administración y demás áreas en materia de riesgos, por la que establece los límites de riesgo que pueden ser administrados directamente por cada nivel en PISA. Las políticas del SGR deben incluir criterios para la delegación de riesgos y las atribuciones asignadas a los colaboradores delegados para la administración de tales riesgos en función de su relevancia y la magnitud ante la configuración de posibles eventos.
- Sin perjuicio del papel de PISA en su condición de sociedad matriz, PISA es responsable directa de la administración de sus riesgos.
- La administración de riesgos debe ejecutarse conforme lo manda la ley y los estatutos.

### 3.5 Marco general de control interno

La documentación de los controles y el proceso de evaluación de la gerencia requieren que se utilice un “marco de control interno generalmente aceptado”. Este marco de referencia define los elementos que se espera estén presentes y funcionando en un sistema de control interno efectivo. En la evaluación de la efectividad, la Administración evalúa si el control interno sobre reporte financiero incluye políticas, procedimientos y actividades para cubrir los elementos que el marco de referencia describe.

Para el efecto, PISA seleccionó COSO<sup>20</sup> (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.

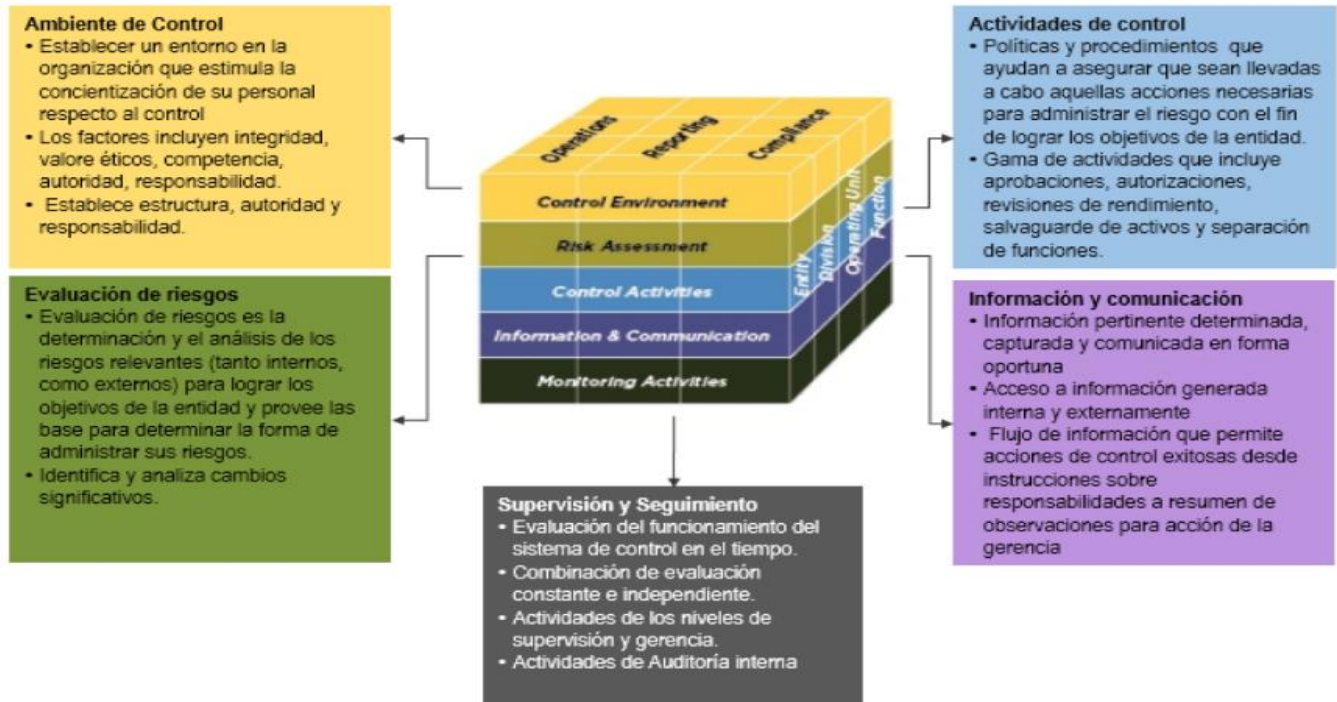
En este contexto el control interno se define como un proceso efectuado por PISA como un todo, con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

El marco de gestión COSO identifica cinco componentes de control interno que deben existir de manera integrada para asegurar cada uno de los objetivos. Los 5 componentes del Control Interno interactúan entre sí, y forman un sistema.

Este sistema debe estar integrado a las actividades operativas de PISA, cuanto más integrado esté el Sistema de Control Interno con las actividades de PISA, tanto mayores serán las posibilidades de éxito de este. Todos los colaboradores de PISA son responsables de la implementación y el correcto funcionamiento del Sistema de Control Interno, tal y como se muestra en el gráfico adjunto. Así mismo, de acuerdo con la actualización del marco (“COSO 2013”), existen 17 principios distribuidos en los 5 componentes, sobre los cuales la Alta Dirección de PISA debe conservar apropiada evidencia que demuestre que están “presentes” y “funcionando” de manera integrada.

<sup>20</sup> COSO: Marco de referencia de control interno. En 1992, el “Committee of Sponsoring Organizations (COSO)” publicó este marco de control, definiendo cinco componentes interrelacionados que deberán ser aplicados en cualquier nivel de PISA. Estos componentes son: evaluación de riesgo, ambiente de control, información y comunicación, actividades de control y monitoreo de controles.



### 3.6 Riesgos

PISA debe estandarizar las metodologías y herramientas para la gestión integral de riesgos, asegurando que se atiendan los principios y normatividad dispuestos por sus órganos internos y externos de control en aras a mitigar, transferir, aceptar o eliminar, y mantener sus riesgos en niveles acordes a su apetito.

Igualmente, debe propender por la existencia de un sistema de control con alcance consolidado, formal, y que abarque a todas las empresas subordinadas, estableciendo responsabilidades respecto a las políticas y lineamientos sobre esta materia y definiendo líneas de reporte claras que permitan una visión consolidada de los riesgos a los que está expuesta y la adopción de las medidas de control que correspondan trasladarlo.

El cumplimiento de estos objetivos debe ser un propósito permanente, de acuerdo con las directrices contempladas en las normas expedidas por sus Entes Supervisores, así como las dispuestas en esta Política y demás Políticas Corporativas originadas en Grupo Aval.

La implementación y documentación de tales procedimientos es responsabilidad de PISA.

#### 3.6.1 Sistemas de Administración de Riesgos abordados

Los principales riesgos a los cuales está expuesta PISA son los siguientes:

- o **Riesgo de Liquidez:** Corresponde a la contingencia de no poder cumplir plenamente, de manera oportuna y eficiente los flujos de caja esperados e inesperados, vigentes y futuros, sin afectar el curso de las operaciones diarias o la condición financiera de PISA. Esta contingencia (riesgo de liquidez de fondeo) se manifiesta en la insuficiencia de activos líquidos disponibles para ello y/o en la necesidad de asumir costos inusuales de fondeo.
- o **Riesgo Operativo:** Se entiende 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 y reputacional, asociados a tales factores.

- **Riesgo Emergente:** Entiéndase por aquellos riesgos nuevos o no identificados que nunca han sido considerados previamente por PISA, o riesgos conocidos que están evolucionando de manera inesperada, que pueden afectar no solo a una compañía sino a todo un sector o toda la economía.
- **Riesgo de Cumplimiento:**
  - Prevención del Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva - LA/FT/FPADM
  - Anticorrupción
  - Ley Sarbanes Oxley – Control Interno sobre Reporte Financiero, siempre y cuando PISA esté incluida dentro del alcance de reporte.
  - Sistema de Gestión de Seguridad de la Información – SGSI

Cada Sistema de Riesgo de Cumplimiento tiene su normatividad particular y cuenta con una estructura específica para su gestión.

### 3.6.2 Administración del Sistema de Gestión Integral de Riesgos

PISA debe contar con sus propios modelos de gestión de riesgo, dentro de los cuales recopila la información de los resultados obtenidos periódicamente y los casos relevantes que considere el Área de GRC, para que con esta información se puedan diligenciar los reportes que PISA remite a la Vicepresidencia de Riesgo de Grupo Aval a través de Corficolombiana.

Cuando hay cambios en los lineamientos Corporativos, el Área de GRC orienta y ejecuta su implementación en el interior de PISA.

### 3.6.3 Evaluación y comprensión de los riesgos

Una sólida gestión del riesgo exige la identificación y el análisis de los riesgos presentes en PISA y el diseño y la eficaz aplicación de políticas y procedimientos acordes con los riesgos identificados. Al realizar un análisis integral del riesgo, PISA debe considerar todos los factores de riesgos relevantes, inherentes y residuales, a escala nacional, sectorial, financiera y de relación comercial, entre otras, para determinar su perfil de riesgo y el adecuado nivel de mitigación que se aplicará.

Así pues, las políticas y procedimientos en materia de conocimiento de las contrapartes deben tener en cuenta la evaluación del riesgo y el resultante perfil de riesgo de PISA. Este conocimiento debe basarse en datos concretos de operaciones y transacciones y en otra información interna recogida por PISA, así como en fuentes de información externa, como evaluaciones del riesgo de ámbito nacional e informes sobre países elaborados por organismos internacionales. Las políticas y procedimientos en materia de aceptación de contrapartes, diligencia debida y seguimiento continuo deben diseñarse y aplicarse para controlar adecuadamente esos riesgos inherentes identificados. Cualquier riesgo residual resultante debe gestionarse en consonancia con el perfil de riesgo de PISA establecido a partir de su evaluación del riesgo.

PISA debe disponer de mecanismos adecuados para documentar y notificar información sobre la evaluación del riesgo a las autoridades competentes.

### 3.6.4 Evaluación y gestión del riesgo

PISA debe tener un conocimiento exhaustivo de todos los riesgos asociados a sus procesos y contrapartes, individualmente o por categorías (según sea el nivel de precisión exigido por la Alta Dirección y el modelo de administración de riesgo), y debe documentar y actualizar periódicamente esa información, en consonancia con el nivel, naturaleza y apetito del riesgo.

### 3.6.5 Marco de gestión de riesgos

PISA debe elaborar un marco de gestión de riesgo independiente, exhaustivo y eficaz evidenciado en Políticas, las cuales deben guiarse por los parámetros mínimos consagrados en las normas vigentes, así como en las directrices corporativas impartidas por Grupo Aval para cada uno de los riesgos. En caso de que se contradigan prevalece lo requerido por el regulador de la jurisdicción específica, siempre y cuando sea más rigurosa que la política de Grupo Aval.

### 3.6.6 Determinación de riesgos genéricos

PISA debe determinar de la lista de riesgos genéricos para cada uno de los sistemas de riesgo los que les aplique. Dichos riesgos son la base de identificación de controles clave que se deben incluir en las matrices de riesgos de los procesos clave del negocio.

El Área de GRC de PISA debe hacer una selección preliminar del inventario de riesgos genéricos de aquellos que les impacta en cada proceso. Dicha selección debe ser, a su vez, acordada con los *dueños de proceso*<sup>21</sup>, con quienes también documentan las justificaciones de aquellos riesgos que no fueron considerados como aplicables en cada proceso.

Toda modificación (Inclusión, modificación o eliminación de riesgos), que surja como resultado de la evolución natural del negocio y de la maduración de los sistemas de riesgos, debe surtir el siguiente proceso de control de cambios:

1. Se debe enviar a la Gerencia de Riesgo respectiva de Grupo Aval la solicitud del cambio indicando: Referencia del riesgo / Riesgo / Tipo de cambio (Inclusión, modificación o eliminación) / Cambio sugerido / Justificación.
2. La Gerencia de Riesgo respectiva de Grupo Aval debe analizar la solicitud del cambio y da su opinión sobre la aplicabilidad del mismo; sugerencia que es comunicada al Comité de Riesgo de Grupo Aval - Entidades Subordinadas, dependiendo del SGR a que pertenezca.
3. En las sesiones del Comité de Riesgo de Grupo Aval - Entidades Subordinadas, se analizan los comentarios realizados por las Entidades Subordinadas y se definen las acciones a seguir.
4. La Gerencia de Riesgo de Grupo Aval manifestará tanto la aprobación como la negación en las respectivas actas del comité.
5. Una vez el cambio se considere procedente, la Gerencia de Riesgo de Grupo Aval debe actualizar la lista respectiva y comunica la modificación mediante Instrucción General.

### 3.6.7 Proceso global para la Gestión del Riesgo

La gestión del riesgo implica establecer y administrar un proceso de coordinación y aplicación de políticas y procedimientos para toda PISA. En este contexto, el diseño de las políticas y procedimientos indicados en esta Política no persiguen únicamente el estricto cumplimiento de toda la legislación y regulación pertinentes, sino el objetivo más general de identificar, medir, controlar, vigilar y mitigar los riesgos en toda PISA.

Se debe establecer un proceso para identificar y evaluar los riesgos susceptibles de eventos potenciales con impactos significativos.

Los procedimientos de evaluación de riesgos requieren, entre otras cosas, la obtención de una comprensión detallada de PISA, su entorno, así como del control interno. Así mismo, se requiere el establecimiento de un proceso para la evaluación de los riesgos identificados, que incluya la determinación de las posibles fuentes de errores potenciales, así como la probabilidad y magnitud de los potenciales eventos y hallazgos.

## 3.7 Medición y mitigación del riesgo

### 3.7.1 Riesgos inherentes de mayor impacto

Con el fin de realizar una efectiva gestión de riesgos, PISA debe identificar sus Riesgos Inherentes de Mayor Impacto, los cuales estarán conformados por:

- o Los riesgos emergentes de nivel alto y extremo. Un riesgo emergente es aquel que puede afectar, no solo a una compañía, sino a todo un sector o toda una economía, siendo de reducida probabilidad de ocurrencia, pero de un impacto crítico, y de difícil evaluación o predicción (por ejemplo, grandes crisis económicas, caídas de las comunicaciones, desastres

---

<sup>21</sup> Dueño de Proceso / Controles: Es el responsable de la gobernabilidad del proceso que tiene asignado, por cuanto se asegura que, en el proceso, los controles son ejecutados y monitoreados, dejando evidencia suficiente de ambas tareas. Cuenta con una estructura funcional que abarca el proceso, sus riesgos y controles dentro de PISA según sus políticas internas. Cuando se menciona en este documento al dueño de proceso / controles, debe entenderse que el dueño de proceso cuenta con un grupo de personas que en conjunto se encargan de asegurar y monitorear que se ejecuten los controles tal y como fueron diseñados, de tal forma que, la responsabilidad del dueño de proceso / controles involucre a todos los actores vinculados en el proceso.

naturales, etc.). Los riesgos emergentes pueden ser eventos nuevos e imprevistos y / o la evolución de riesgos conocidos previamente que el negocio no ha comprendido o permitido.

- o Los riesgos claves. Se consideran riesgos claves aquellos riesgos que afecta un proceso misional y el resultado del *riesgo inherente*<sup>22</sup> se ubica en los niveles de alto y extremo sobre el mapa de calor y afecta a los objetivos estratégicos de PISA. Adicionalmente se considera como riesgo clave aquel riesgo que genera un impacto reputacional mayor o superior.

El Coordinador de GRC actualizará como mínimo dos veces al año (enero y julio) el listado de los Riesgos Inherentes de Mayor Impacto, listado que deberá ser aprobado por la Gerencia General y presentado anualmente al Comité de Riesgos.

A los Riesgos Inherentes de Mayor Impacto se les debe realizar seguimiento permanente y oportuno, considerando las siguientes premisas:

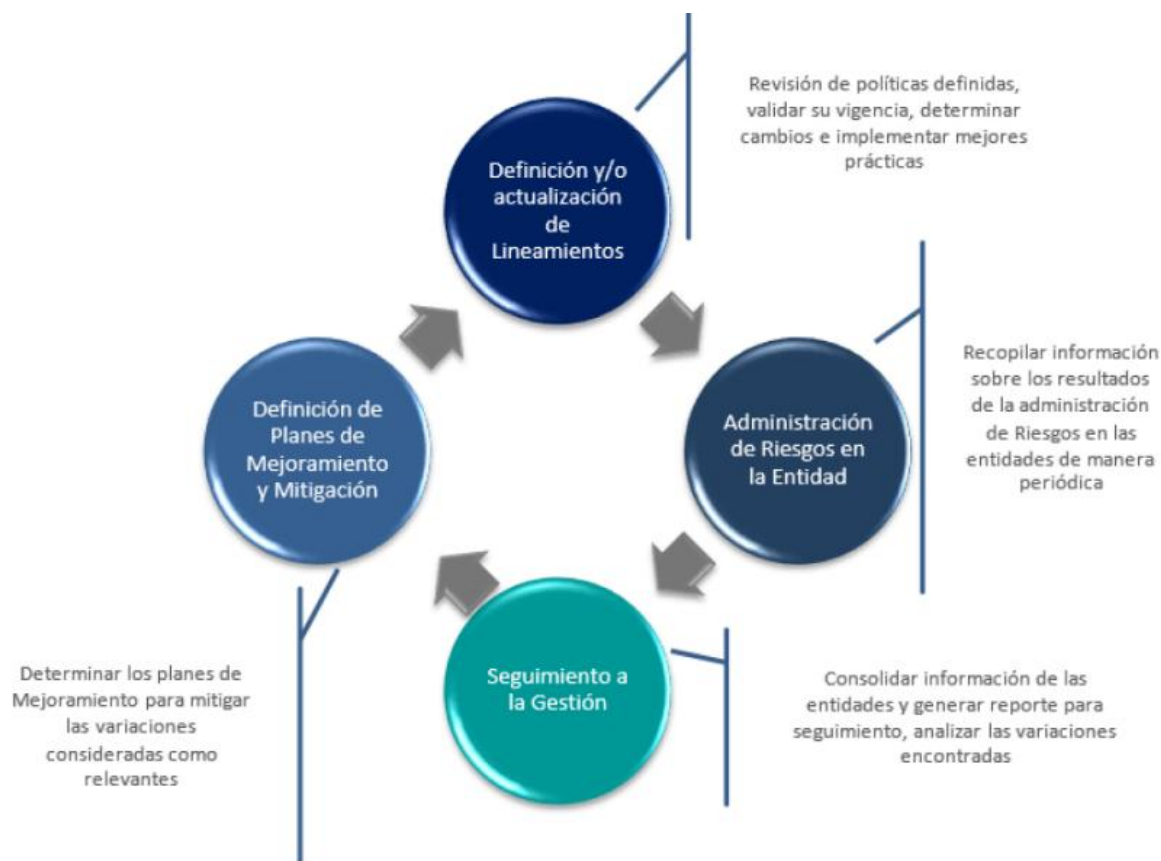
- o Los Riesgos Inherentes de Mayor Impacto de PISA deben tener dueños responsables de su entendimiento, gestión y mitigación.
- o La valoración periódica de los Riesgos Inherentes de Mayor Impacto es responsabilidad fundamental de la primera línea con el apoyo de la segunda línea.
- o El monitoreo continuo es una responsabilidad principal de la primera línea en el ejercicio del autocontrol y para los Riesgos Inherentes de Mayor Impacto la segunda línea deberá a través de indicadores o pruebas de recorrido o metodologías de valoración revisar y monitorear la evolución de dichos riesgos.
- o Cualquier riesgo de mayor impacto que a nivel de riesgo residual supere los umbrales de apetito definidos por PISA, deberá contar con planes de acción para su mitigación.
- o PISA debe asegurarse de que exista un proceso de evaluación, previo al lanzamiento y/o modificación de cualquier proceso y/o servicio, que identifique los riesgos materiales, actividades significativas, proveedores críticos, líneas de negocios, sistemas Core y controles SOX; este último, siempre y cuando PISA esté incluida dentro del alcance de reporte.
- o Los riesgos de mayor impacto junto con sus actividades de control y planes de acción requieren ser revisados por PISA para asegurar que las circunstancias cambiantes no alteran la priorización de los riesgos evaluados. Para ello el Área de GRC como mínimo anualmente, coordinará con los dueños de los riesgos su actualización, incorporando nuevos riesgos, reevaluando el nivel de los riesgos inherentes y definiendo nuevas actividades de control.
- o El Comité de Riesgo de PISA anualmente monitoreará la gestión de riesgo de PISA y dará seguimiento a la implementación de planes de acción en caso de requerirse.

### 3.7.2 Modelo de Gestión Corporativo

El modelo consta de cuatro etapas, las cuales están definidas para direccionar y unificar los criterios de administración del riesgo. Estas etapas se relacionan de manera cíclica y continua, de acuerdo con el siguiente diagrama:

<sup>22</sup> Riesgo Inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. En otras palabras, el Riesgo Inherente es la probabilidad de que PISA pueda incurrir en una pérdida como resultado de su exposición y de la incertidumbre que surge de, potenciales eventos adversos.

El Riesgo Inherente es intrínseco a cada actividad significativa y se evalúa sin tener en consideración el tamaño de la misma en relación con PISA y antes de evaluar la calidad de la administración de los riesgos que ésta realiza. Para identificar y evaluar los Riesgos Inherentes a los que está expuesta PISA es esencial tener un conocimiento profundo tanto de la naturaleza de las actividades que ésta realiza como del entorno en el que opera.



### 3.7.3 Análisis de Controles

El análisis de los controles debe permitir evaluar si un control es capaz de prevenir o detectar posibles eventos. Consiste en obtener una comprensión y evaluación de lo siguiente, de forma que sea posible reforzar aquellos aspectos que puedan considerarse débiles:

- Si cumple el objetivo de control correspondiente, incluyendo si aborda los riesgos de errores materiales a la afirmación correspondiente de la cuenta o revelación significativa.
- Los factores que afectan la precisión del examen, incluido el objetivo de la revisión y la adecuación de las expectativas, nivel de agregación, y los criterios de investigación para la identificación de errores potencialmente materiales.
- Los pasos necesarios para identificar, investigar y resolver las diferencias significativas de las expectativas.
- Las personas que realizan el control, incluida su competencia y la autoridad.
- La frecuencia de funcionamiento del mando, es decir, si la revisión se produce con la periodicidad suficiente para prevenir o detectar errores.
- La información utilizada en la revisión, por ejemplo, si en el análisis se utilizan datos o informes generados por el sistema.

La segunda línea debe realizar procedimientos de verificación de la efectividad del diseño de los controles, con el fin de establecer si los mismos mitigan los riesgos establecidos.

Por su parte, la tercera línea realiza pruebas de manera independiente, de acuerdo con los programas de trabajo aprobados por el Comité de Auditoría.

En todo caso, atendiendo el principio de Autocontrol, la primera línea es responsable por el apropiado diseño y funcionamiento sistemático de los controles para lograr la mitigación del riesgo hasta los niveles de apetito definidos.

### 3.7.3.1 Directrices metodológicas respecto a los controles

PISA debe implementar un enfoque de arriba hacia abajo. En otras palabras, no debe colocarse un énfasis indebido en la gestión de las pruebas de revisión de controles y otros controles de detección, sin considerar si se están abordando adecuadamente los riesgos con eventual impacto material en la cuenta contable asociada al proceso crítico.

La metodología requiere entre otros:

- Una vigilancia permanente para confirmar que no ha habido cambios significativos en los procesos.
- Reforzar el entendimiento de los riesgos a través de las pruebas de controles y procedimientos sustantivos.
- Realizar pruebas de recorrido de controles.

En la implementación de un enfoque de arriba hacia abajo, el énfasis debe colocarse en los controles preventivos antes que en la gestión de controles detectivos.

Sobre estos controles se podrán realizar pruebas de recorrido con el fin de evaluar el diseño adecuado del mismo cuando este se encuentra en operación, estas pruebas tendrán alcance a diseño y no a la validación de la efectividad del control.

Para determinar la suficiencia del esquema de control es necesario validar si los controles, en forma individual o en combinación, son capaces de hacer frente a los riesgos materiales. Algunos de los riesgos, especialmente los relacionados con procesos complejos o estimaciones subjetivas, podría requerir una combinación de controles para prevenir o detectar errores.

Los Controles a nivel de la Gerencia pueden realizarse para supervisar los resultados de las operaciones. Tales controles pueden ser:

- Comparaciones mensuales de los resultados reales frente a los presupuestados.
- Comparaciones de otros indicadores.
- Comparaciones temporales de estados financieros y otros informes.

La consideración principal en la evaluación del nivel de precisión es si el control está diseñado y operando para prevenir o detectar oportunamente errores básicos que podrían causar la no detección de operaciones inusuales con potenciales efectos.

Dependiendo de la naturaleza del riesgo, PISA deberá distribuir los niveles de Riesgo o Amenaza en la matriz de acuerdo con su apetito de riesgo definido internamente, pero reportan a Grupo Aval el número de riesgos inherentes y residuales que se encuentran clasificados en cada uno de los niveles.

Esta matriz se utiliza para analizar la evolución de la clasificación, es decir, se revisa si los riesgos que están en los niveles han disminuido o aumentado con el fin de saber la gestión que PISA realiza frente a los mismos. Posteriormente, se presenta dicha información para su revisión y observaciones a la Vicepresidencia Senior de Riesgo y al Comité de Auditoría de Grupo Aval.

### 3.7.4 Evolución de riesgos residuales

Cada uno de los riesgos reportados por PISA se analiza utilizando la siguiente escala de medición de acuerdo con los indicadores de riesgo definidos en cada SGR y se consolidan en Grupo Aval respetando su homogeneidad por tipo de industria.

Esta colorimetría será usada en los mapas de calor y en los tableros de control para el monitoreo de indicadores y del apetito del riesgo a nivel de entidad.



### 3.8 Modelo integrado GRC (Gobierno, Riesgo, Cumplimiento)

Con la implementación de este modelo se contribuye a tener una visión integral sobre los tres componentes del modelo de GRC, (Gobierno, Riesgo y Cumplimiento), de manera que se pase de tener una visión de gestión de riesgos por unidad de negocio, tipo de riesgos específico, a tener una visión holística de riesgos que integra el plan estratégico con la gestión de riesgo y planes de cumplimiento regulatorio. Se precisa que en una visión integrada de GRC se consideran las necesidades de corto y largo plazo de PISA, incrementándose así sustancialmente la eficiencia y efectividad, y dándole confianza ante terceros.

GRC es un modelo de gestión que integra las actividades y funciones de gobierno corporativo, la administración de riesgos y las responsabilidades de cumplimiento; mejorando con esto la capacidad de PISA para lograr sus objetivos de negocio. Con esta integración se contribuye a tener una visión integral sobre los siguientes tres (3) componentes:

- **Gobierno:** Son las estructuras, políticas, procesos y controles de la Administración y la Alta Dirección.
- **Riesgos:** Es el proceso sistemático de PISA que busca identificar, evaluar, administrar y monitorear todos los riesgos.
- **Cumplimiento:** El proceso de PISA que busca demostrar adherencia a las políticas, procedimientos internos, externos y normas en general, así como a las leyes y regulaciones.

### 3.9 Gestión de la información

#### 3.9.1 Mantenimiento de registros

PISA debe:

- Garantizar el registro de toda la información recolectada en el contexto del sistema de conocimiento de sus contrapartes.
- Desarrollar y aplicar reglas claras sobre los registros que deben mantenerse para documentar la debida diligencia practicada a sus contrapartes y a las transacciones individuales. Estas reglas deben tener en cuenta cualquier medida preceptiva en materia de privacidad. Deben incluir una definición de los tipos de información y documentación que habrán de incluirse en los registros, así como del periodo de conservación de esos registros.
- Mantener registros adecuados que documenten el proceso de evaluación relacionado con el análisis y seguimiento continuo y con las conclusiones extraídas, de forma que permitan demostrar el cumplimiento de los requisitos y parámetros de calificación y valoración del riesgo.
- Mantener actualizada la información para que PISA vigile eficazmente las actividades anómalas, y permita que los controles preventivos, o que los indicadores de alerta temprana tengan la efectividad que de ellos se espera.
- Ser capaz de demostrar a la Auditoría Interna la adecuación de sus sistemas de evaluación, gestión y mitigación de riesgos; de su política de aceptación de contrapartes, de sus procedimientos y políticas; de sus procesos de seguimiento continuo y de sus procedimientos para notificar eventos de riesgo, así como de todas las medidas adoptadas en el contexto del (SGR).
- Informar oportunamente a Grupo Aval acerca de los eventos de riesgo que se presenten y que tengan la categoría de alto impacto.
- Seguir los lineamientos establecidos por el Comité Corporativo de Riesgo de Grupo Aval – Entidades, según corresponda.
- Fomentar la confianza del público y de los inversionistas; velando por mantener la reputación, seriedad y transparencia del negocio.
- Aplicar las normas de cada riesgo consagradas en los Manuales, Políticas y Procedimientos vigentes en PISA y los de naturaleza Corporativa y adoptar los controles adecuados para evitar sanciones que puedan imponer los entes de control a PISA o a sus colaboradores.

### 3.10 Prácticas de presentación de informes de riesgos

Contar con datos exactos, completos y oportunos es fundamental para una gestión eficaz del riesgo. Sin embargo, los datos por sí solos no garantizan que la Alta Dirección y la Administración dispongan de información idónea para adoptar decisiones eficaces sobre riesgos. Para gestionar eficazmente los riesgos, la información idónea debe presentarse a las personas apropiadas en el momento oportuno. Los informes basados en datos sobre riesgos deben ser exactos, claros y completos, su contenido debe ser el adecuado y han de entregarse a las personas competentes en la toma de decisiones con tiempo suficiente como para permitir una respuesta adecuada.

## 4 Documentos relacionados

Hacen parte integral de esta política todos aquellos documentos relacionados en cada uno de los sistemas de administración de riesgos, que para efecto sean emitidos por la Vicepresidencia de Riesgos de Grupo Aval, los cuales deben ser adoptados o adaptados por PISA.

## 5 Control de cambios

Fecha	Versión	Descripción del cambio
19-12-2017	01	Creación del documento. Aprobado por Junta Directiva en acta No. 243 del 19 de diciembre de 2017.
Acta N°350 Fecha: 30-06-2020	02	Se alinea todo el documento con la última versión de la Política para la Gestión Integral de Riesgos del Conglomerado de Grupo Aval. Los principales cambios son: <ol style="list-style-type: none"> <li>1. Se Incluyen nuevos términos usados en la Política.</li> <li>2. Se incluye el numeral. Sistema de Gestión de riesgos (SGR).</li> <li>3. Se incluye el numeral. Consideraciones.</li> <li>4. Se actualizan los Principios incluidos en el numeral 5.</li> <li>5. Se elimina el numeral Unidad de Riesgo Corporativo – URC mencionado en la V1 de la Política.</li> <li>6. Se incluye el numeral Metodología de Gestión.</li> <li>7. Se actualiza el numeral Estructura y Gobierno para la Gestión Integral de Riesgos.</li> <li>8. Se incluye el numeral Marco General de Control Interno.</li> <li>9. Se incluye el numeral Riesgos.</li> <li>10. Se incluye el numeral edición y Mitigación del Riesgo.</li> <li>11. Se incluye el numeral Modelo Integrado de GRC (Gobierno, Riesgo, Cumplimiento).</li> <li>12. Se incluye el numeral Gestión de la Información.</li> <li>13. Se incluye el numeral Prácticas de Presentación de Informes de Riesgo.</li> <li>14. Se incluye el numeral Documentos relacionados.</li> <li>15. Otros cambios menores de redacción en todo el documento para ajustarlo de acuerdo con las modificaciones indicadas anteriormente y para alinearlos con las actividades desarrolladas en PISA.</li> </ol> <p>Aprobado por Junta Directiva mediante Acta N°350 Fecha: 30 de junio 2020</p> <p>02/06/2022 – Se realiza el siguiente cambio menor:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Se reemplaza el término Compañía por PISA.</li> <li>• Se actualiza la imagen del organigrama general de PISA.</li> <li>• Se actualiza el nombre de los siguientes cargos: <ul style="list-style-type: none"> <li>○ Presidente por Gerente General (también en el organigrama del punto 3.3.3.5)</li> <li>○ Director Jurídica por Gerente Jurídico</li> <li>○ Director Administrativo por Gerente Administrativo</li> </ul> </li> </ul>
Acta 397 20/03/2024	03	Se realizan los siguientes cambios: <ol style="list-style-type: none"> <li>1. Se modifica el numeral 3.4 para establecer que el Comité de Riesgos debe sesionar anualmente a más tardar en el primer cuatrimestre del año y se alinea las funciones de dicho Comité con lo indicado en la Política SARO.</li> <li>2. Se modifica el numeral 3.7.1 para establecer que el listado de Riesgos Inherentes de Mayor Impacto debe tener la aprobación de la Gerencia General.</li> <li>3. Se modifica la responsabilidad de la Auditoría Interna de reportar a la Junta Directiva directamente, en su lugar debe reportar al Comité de Auditoría.</li> <li>4. Se elimina la palabra Defensa al término Línea de Defensa.</li> <li>5. Se hacen cambios menores de redacción.</li> </ol>
Acta 410 18/02/2025	04	Se realiza el siguiente ajuste: <ol style="list-style-type: none"> <li>1. Se incluye nota al pie en el alcance del documento 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</li> <li>2. 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.</li> <li>3. Se actualiza el cargo de Jefe financiero a Director Financiero</li> </ol>