

# POLÍTICA DE CUMPLIMIENTO NORMATIVO

Código: GRC-DG-04

Versión: 02

**CONTENIDO**

1	INTRODUCCIÓN.....	2
2	OBJETIVOS .....	3
3	ALCANCE.....	3
4	POLÍTICAS DE OPERACIÓN .....	3
5	ETAPAS DEL SISTEMA .....	7
6	RIESGOS DE CUMPLIMIENTO NORMATIVO .....	9
7	AUTORIDAD Y CAPACIDADES DEL ÁREA DE GRC ANTE EL PROGRAMA DE CUMPLIMIENTO NORMATIVO	10
8	GESTIÓN DE SEGUIMIENTO DE PLANES DE ACCION .....	10
9	INFORMACIÓN Y COMUNICACIÓN .....	11
10	CAPACITACIÓN Y ENTRENAMIENTO.....	11
11	MONITOREO .....	11
12	SANCIONES .....	12
13	DOCUMENTO DE APROBACIÓN .....	12
14	DOCUMENTOS RELACIONADOS .....	12
15	FORMATOS RELACIONADOS Y/O REGISTROS .....	12
16	CONTROL DE CAMBIOS .....	13

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 INTRODUCCIÓN

Las empresas operan en entornos altamente regulados, con exigencias basadas en el cumplimiento<sup>1</sup> de obligaciones y deberes fundamentados en leyes, normas, estándares de industria, contratos y políticas internas de la más variada índole. En dichos escenarios, es indispensable contar con mecanismos que aseguren el cumplimiento de las obligaciones tanto legales como internas, dado que la materialización de cualquier incumplimiento podría afectar los resultados financieros y la imagen de PISA. Es por eso que Proyectos de Infraestructura S.A.S. (en adelante PISA), consciente de la necesidad de gestionar el cumplimiento de las normas desde la perspectiva de riesgos, ha decidido incluir dentro de su gobierno corporativo el Programa de Cumplimiento Normativo<sup>2</sup>.

Este documento define el marco común del Programa de Cumplimiento Normativo, que forma parte de las funciones de Gobierno, Riesgo y Cumplimiento (en adelante GRC) en PISA, el cual se soporta en las siguientes premisas:

- PISA reconoce la necesidad de avanzar hacia una gestión centrada en la administración del cumplimiento normativo, para lo cual requiere establecer las capacidades necesarias que permitan el desarrollo del Programa de Cumplimiento Normativo.
- PISA es consciente de la necesidad de generar y estandarizar el conocimiento sobre el cual se soportan las diferentes funciones de GRC a nivel corporativo.
- PISA reconoce la necesidad de articular el canal de comunicación y supervisión de las funciones de GRC con su filial.
- PISA debe compilar los procedimientos y controles que actualmente están implementados, para la efectiva prevención, detección y gestión del riesgo normativo, con el objetivo de promover y potenciar una verdadera Cultura de Cumplimiento Normativo<sup>3</sup> capaz de reflejar la ética corporativa, asentar sus mecanismos de control y reducir la posibilidad de que se cometan incumplimientos normativos en su nombre, directa o indirectamente.
- Grupo AVAL y Corficolombiana han generado políticas relacionadas con la gestión de riesgos y cumplimiento para la aplicación y cumplimiento de todas sus filiales, las cuales son adoptadas o adaptadas e interiorizadas en el modelo de GRC de PISA y su filial.
- La presente Política es definida teniendo en cuenta los marcos de referencia ISO 19600:2015 (Gestión de sistemas de Cumplimiento), el Estándar Australiano AS 3806-2006, y el documento de EY Cumplimiento life cycle.
- Este documento define el Programa de Cumplimiento Normativo, el cual incluye la identificación, gestión y documentación de planes de acción, definiciones básicas, la estructura para el manejo de cumplimiento normativo, los roles y responsabilidades, los mecanismos de información y comunicación, sanciones y documentos de referencia y anexos con base en los lineamientos provistos por Corficolombiana para sus filiales y subsidiarias.

<sup>1</sup> Cumplimiento: Cumplir con los requisitos de las leyes, los estándares y códigos de la industria y la organización, los principios de buen gobierno y los estándares éticos y comunitarios aceptados. En este documento se utiliza indistintamente el término Cumplimiento normativo o función de Cumplimiento normativo.

<sup>2</sup> Programa de Cumplimiento Normativo: está conformado por las políticas y procedimientos adecuados y suficientes para asegurar que PISA, incluidos la Alta Dirección, Administración y Colaboradores, cumplen con el marco normativo aplicable. Dentro del marco normativo no han de considerarse únicamente las normas legales, como leyes, decretos, resoluciones y reglamentos, sino que también deben incluirse en el mismo las políticas internas, los compromisos con las contrapartes, y especialmente los códigos éticos que PISA se haya comprometido a respetar. El Programa tiene como finalidad hacer una vigilancia independiente de la gestión que PISA hace respecto del cumplimiento normativo (leyes, decretos, reglamentos, regulaciones), estándares de auto-regulación de PISA o de la industria a la que pertenece, políticas de revelación de información al mercado y a las partes interesadas, políticas para la generación de informes y relacionamiento con clientes, directrices y códigos internos de conducta, de ética, de transparencia, aplicables a las actividades que desarrolla en todas las jurisdicciones en las cuales opera, dentro del eje de sus negocios y como parte de su cultura organizacional.

<sup>3</sup> Cultura de cumplimiento normativo: Son los valores, ética y creencias que existen en toda la organización, e interactúan con las estructuras y sistemas de control de la organización para producir normas de comportamiento que son propicias para los resultados del cumplimiento normativo.

## 2 OBJETIVOS

### 2.1 Objetivo General

Proporcionar confianza a los Accionistas, a la Administración<sup>4</sup> y demás Contrapartes<sup>5</sup> respecto del cumplimiento normativo por parte de PISA.

### 2.2 Objetivos Específicos

- Prevenir el Riesgo de Incumplimiento Normativo<sup>6</sup> en PISA.
- Detectar posibles incumplimientos normativos con el fin de establecer los planes de acción para subsanarlos y de esta manera fortalecer el sistema de control interno de PISA.
- Fijar la posición de PISA y su filial frente a la responsabilidad de cumplimiento normativo.
- Identificar los principales riesgos normativos a que está expuesta PISA con el propósito de implementar controles y procesos efectivos, suficientes y oportunos para mitigar tales riesgos.
- Definir la metodología para la identificación, monitoreo y control, de los riesgos normativos.
- Establecer los responsables de la prevención, detección e investigación de problemas de cumplimiento normativo.
- Definir los requisitos e información base para la identificación y documentación de los planes de acción.
- Definir responsabilidades para la identificación, definición, seguimiento y cierre de planes de acción.
- Indicar las consecuencias que podrían conllevar el incumplimiento normativo.

## 3 ALCANCE<sup>7</sup>

El Programa de Cumplimiento Normativo establecido en la presente POLÍTICA abarca todas las normas internas y externas que PISA deba cumplir en el desarrollo de su objeto social.

## 4 POLÍTICAS DE OPERACIÓN

### 4.1 Programa de cumplimiento normativo

El Programa de Cumplimiento Normativo que desarrolla PISA, bajos los lineamientos de Corficolombiana, contempla la ejecución de acciones y la creación de las estructuras necesarias para identificar, valorar, controlar y documentar el cumplimiento de requerimientos normativos, así como procedimientos de supervisión.

El Programa de Cumplimiento Normativo tendrá, entre otros, los siguientes objetivos:

---

<sup>4</sup> Administración: Gerente General, Director Financiero, Gerente Jurídico, Gerente Administrativo y Gerente de Operaciones.

<sup>5</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 y los clientes y proveedores de bienes o servicios.

<sup>6</sup> Riesgo de Incumplimiento Normativo: El riesgo de sanciones legales o reglamentarias, pérdidas financieras materiales o pérdida de la reputación que PISA puede sufrir como resultado del incumplimiento de las leyes, decretos, reglamentos, y demás normas relacionadas, de las normas de instituciones reguladoras, así como de los CÓDIGOS DE CONDUCTA aplicables a sus actividades de negocio.

<sup>7</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.

- Implementar de forma proactiva con las diferentes áreas de PISA la GESTIÓN DEL RIESGO DE INCUMPLIMIENTO NORMATIVO.
- Desarrollar y mejorar las herramientas para fortalecer las tres líneas de defensa para detectar, comunicar, administrar e informar sobre posibles Riesgos de Incumplimiento Normativo.
- Apoyar la estrategia de PISA estableciendo roles y responsabilidades claros para ayudar a incorporar buenas prácticas de cumplimiento normativo al interior de esta, mediante el uso de un enfoque basado en riesgo, para alinear los resultados comerciales con el apetito de riesgo de PISA.
- Profundizar la Cultura de Cumplimiento Normativo para aumentar la cultura de confianza, responsabilidad, transparencia e integridad en la evaluación de la gestión.
- Presentar informes a la *Alta Dirección*<sup>8</sup> sobre el Riesgo de Incumplimiento Normativo.

Para tal efecto, PISA ha definido que el Programa de Cumplimiento Normativo sea liderado por el área de GRC, quien cuenta con los recursos humanos, metodológicos y técnicos para la gestión de dicho Programa en PISA.

El área de GRC, en el desarrollo del Programa de Cumplimiento Normativo, deberá ayudar a PISA, de manera independiente y eficaz, a vigilar el cumplimiento de la normatividad, así como la ejecución de medidas correctivas cuando se requieran para asegurar el cumplimiento de las obligaciones normativas.

## 4.2 Ambiente de control

### 4.2.1 Declaración de Compromiso

En PISA el control y el cumplimiento normativo hacen parte indispensable de la cultura de trabajo. Es por eso que PISA está comprometida en establecer y mantener un Programa de Cumplimiento Normativo con el fin de asegurar que se cumpla con la normatividad aplicable (tanto interna como externa) y se esfuerza por cumplir las normas y buenas prácticas que le apliquen en sus actividades y responsabilidades cotidianas, con el objetivo de evitar riesgos económicos y reputacionales para PISA, la Administración y sus *colaboradores*<sup>9</sup>.

### 4.2.2 Responsables de la Política

- La Junta Directiva de PISA es responsable por la aprobación de la POLÍTICA DE CUMPLIMIENTO NORMATIVO, así como sus modificaciones posteriores.
- La Alta Dirección de PISA es responsable por:
  - Establecer un conjunto fuerte de valores corporativos que se encuentren arraigados en la cultura de PISA.
  - Operar bajo los objetivos de cumplimiento normativo definidos por la Junta Directiva para alinear la estrategia de PISA.
  - Asegurarse que el área de GRC, en el desarrollo del Programa de Cumplimiento Normativo, tenga la autoridad para actuar de manera independiente y no se vea comprometida por prioridades en conflicto con dicho Programa.
  - Comunicar la importancia del Programa de Cumplimiento Normativo
  - Asegurar la aplicación de la Política de Cumplimiento Normativo para la efectiva y permanente acción del Programa Cumplimiento Normativo.
  - Recibir informes con respecto a casos relevantes de incumplimiento normativo que hubieren sido identificados, así como las medidas investigativas y conclusiones sobre las mismas.
  - Asegurar que se mantiene un compromiso de cumplimiento normativo en toda PISA y que los incumplimientos normativos son tratados apropiadamente.

<sup>8</sup> Alta dirección: Junta Directiva y Gerente General / Representantes Legales.

<sup>9</sup> Colaboradores: Trabajadores incluyendo Alta Dirección, estudiantes en práctica y aprendices de PISA.

- Ubicar los recursos apropiados para implementar, evaluar, mantener y mejorar el Programa de Cumplimiento Normativo.

### 4.2.3 Responsables de la Implementación y Monitoreo

PISA debe estructurar las funciones y responsabilidades en general frente a todos los riesgos siguiendo el esquema de las tres líneas de defensa, esto es, considerando (i) la gestión por la línea de negocio, (ii) la gestión del área de GRC<sup>10</sup> y (iii) la gestión de quien haga revisiones independientes de la administración.

#### 4.2.3.1 Primera Línea

La primera línea en lo relacionado con el Programa de Cumplimiento Normativo es responsable por:

- Áreas de operación y apoyo:
  - Operar dentro de las estrategias de negocio aprobadas, las políticas, estrategias y objetivos de cumplimiento normativo.
  - Desarrollar e implementar procesos y controles efectivos que aseguren el cumplimiento de los requisitos normativos, siendo conscientes de los requisitos normativos relevantes a sus roles y responsabilidades.
  - Construir un inventario y mantener actualizado y consolidado los requisitos normativos que afecten el proceso o área.
  - Asegurar que los Riesgos de Incumplimiento Normativo sean identificados, evaluados, gestionados y comunicados apropiadamente.
  - Asegurar que los controles se mantienen, son monitoreados y evaluados adecuadamente para mitigar los Riesgos de Incumplimiento Normativo.
  - Promover, asesorar, entrenar y supervisar activamente a los colaboradores para promover un comportamiento de cumplimiento normativo.
  - Identificar los requisitos normativos con el apoyo de Gerencia Jurídica o mediante fuentes adicionales de información, y traducir esos requisitos en políticas y procedimientos procesables.
  - Colaborar con el Programa de Cumplimiento Normativo, brindando todo el apoyo necesario.
  - Cumplir con las políticas y procedimientos requeridos para su rol.
  - Asegurar que la responsabilidad del cumplimiento normativo es incluida en las descripciones de trabajo de los colaboradores y en las políticas internas.
  - Promover una cultura donde los empleados se sientan libres de alertar de situaciones relacionadas a cumplimiento normativo, tales como incidentes, brechas o incumplimientos normativos.
  - Dar solución oportuna a las situaciones de incumplimiento normativo según lo dispuesto en la presente Política.
  - Identificar y reportar oportunamente situaciones de posibles incumplimientos normativos.
  - Elaborar planes de acción para el cierre de brechas en incumplimientos normativos identificados.
  - Asistir a las capacitaciones del Programa de Cumplimiento Normativo convocadas por PISA.
- Gerencia Jurídica:

La Gerencia Jurídica además de cumplir con las responsabilidades indicadas en el punto anterior, es responsable por:

  - Mantenerse actualizado con las regulaciones generadas.
  - Informar a los dueños de procesos y al área de GRC sobre nueva normatividad que sea aplicable a PISA.
  - Brindar asesoría en el entendimiento de los requisitos normativos que aplican a PISA.

#### 4.2.3.2 Segunda Línea

La segunda línea asigna responsabilidades al área de GRC. La segunda línea en lo relacionado con el Programa de Cumplimiento Normativo es responsable por:

- Liderar la implementación de un Programa de Cumplimiento Normativo efectivo y eficiente.
- Dar asesoramiento a las áreas para la implementación del Programa de Cumplimiento Normativo.
- Apoyar la identificación de requerimientos de cumplimiento normativo y colaborar con las áreas en la creación de políticas procedimientos y controles.
- Evaluar los Riesgos de Incumplimiento Normativo y los riesgos asociados con el mismo, con el fin definir el perfil de riesgos de cumplimiento normativo de PISA y posteriormente establecer los controles necesarios.
- Establecer la estructura metodológica y funcional para administrar el inventario de los requisitos normativos que aplican a PISA.
- Estar al tanto de los cambios en la legislación y reglas aplicables y en el perfil de riesgos del Programa de Cumplimiento Normativo en PISA.
- Proveer de capacitaciones y entrenamientos necesarios a los colaboradores de PISA.
- Proponer la actualización oportuna de la Política de Cumplimiento Normativo de PISA cuando surjan nuevos lineamientos emitidos por Corficolombiana, o se modifiquen los existentes.
- Administrar los indicadores de cumplimiento normativo y realizar el monitoreo respectivo para generar acciones de mejora sobre el Programa.
- Presentar informes semestrales de gestión al Comité de Riesgos.
- Adoptar y socializar las mejores prácticas para asegurar el Programa de Cumplimiento Normativo por parte de PISA.
- Coordinar la evaluación de riesgos de cumplimiento normativo con los dueños de proceso.
- Presentar requerimientos de recursos informáticos, tecnológicos, físicos, humanos y financieros necesarios para las actuaciones del área de GRC ante el Programa.
- Promover una Cultura de Cumplimiento Normativo dentro de PISA.
- Asegurar que el Programa de Cumplimiento Normativo sea revisado de manera regular.
- Revisar el cumplimiento de los planes de acción propuestos por la primera línea para subsanar las brechas identificadas en el tema de normatividad.

#### 4.2.3.3 Tercera Línea

La tercera línea juega un papel importante al evaluar de forma independiente la gestión y los controles del Programa de Cumplimiento Normativo de PISA, rindiendo cuentas a la Junta Directiva y/o al Comité de Auditoría mediante evaluaciones periódicas de la eficacia del cumplimiento de las políticas y procesos relacionados. La Auditoría Interna, quien debe realizar estas revisiones, debe ser competente y estar debidamente capacitada, y no participar en el desarrollo, implementación y operación del Programa de Cumplimiento Normativo. Esta revisión puede ser realizada por la auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados.

La tercera línea en lo relacionado con el Programa de Cumplimiento Normativo es responsable por:

- Realizar una evaluación del Programa de Cumplimiento Normativo con enfoque de riesgos, sobre la efectividad de los controles existentes y el tratamiento de los eventos de incumplimiento normativo reportados, cuando lo consideren pertinente según su plan de trabajo.
- Evaluar de manera independiente los controles definidos por la primera línea para mitigar los Riesgos de Incumplimiento Normativo.

## 5 ETAPAS DEL SISTEMA

### 5.1 Identificación de requerimientos normativos y de terceras partes, y principios de buen gobierno

La identificación de requerimientos normativos se realiza utilizando el NORMOGRAMA<sup>11</sup> definido por PISA, el cual consolida información de la normatividad que se debe cumplir, las políticas que responden a cada requerimiento normativo y un análisis preliminar sobre el cumplimiento del requisito. Este análisis puede generar un plan de acción con el dueño del proceso para identificar mecanismos que aseguren el cumplimiento de cada uno de los requisitos.

También es necesario identificar las necesidades que tengan otras partes respecto al cumplimiento de requisitos, tales como proveedores y demás contrapartes.

Es necesario que los principios de buen gobierno sean identificados para conocimiento de todos los colaboradores previo a la identificación de riesgos de cumplimiento normativo.

La identificación de requerimientos de cumplimiento normativo comprende acciones de 3 tipos de actores:

- **Dueños de procesos:** Tienen la responsabilidad de identificar y reconocer los requisitos normativos que le aplican a cada proceso, así como de estar atentos a los hallazgos de los órganos de control para incluir oportunamente nuevos requisitos normativos. Es obligación de los dueños de procesos validar si los requisitos normativos identificados por la Gerencia Jurídica son aplicables a los procesos.
- **Gerencia Jurídica:** Al estar en contacto con nuevas leyes, circulares y la normatividad en general, la Gerencia Jurídica tiene la responsabilidad de informar sobre nueva normatividad que podría ser aplicada en los procesos de PISA. Esta Gerencia también cuenta con la obligación de asesorar a los dueños de procesos en la validación de la aplicabilidad de los requisitos normativos.
- **Área de GRC:** Brindar asesoría a las áreas dueñas de proceso para el diligenciamiento del NORMOGRAMA, en línea con lo establecido en el procedimiento ACTUALIZACIÓN DE NORMOGRAMA y proporcionar los mecanismos necesarios para realizar seguimiento a los planes de acción que se generen a partir de nuevos requisitos normativos.

### 5.2 Identificación de normas internas mediante las cuales se da cumplimiento a los requerimientos normativos

Después de realizar la identificación de obligaciones normativas, los dueños de proceso deben identificar las políticas, procedimientos, instructivos y manuales internos mediante los cuales se da cumplimiento a los requerimientos normativos identificados.

Las políticas, procedimientos, instructivos y manuales internos identificados se deben asociar a los requisitos normativos. De esta manera es posible identificar falencias de cumplimiento cuando los requisitos normativos no están cubiertos o están siendo cumplidos de manera parcial.

### 5.3 Control de cumplimiento normativo

Se necesitan controles efectivos para garantizar que se cumplan los requisitos normativos en PISA, que permitan evitar, detectar y corregir incumplimientos oportunamente. Los tipos y niveles de controles deben diseñarse con suficiente rigor para facilitar el logro de las obligaciones de cumplimiento que son particulares para las actividades de PISA y el entorno operativo. Dichos controles deberían, cuando sea posible, integrarse en los procesos organizacionales normales.

Todos los colaboradores están en la obligación de informar al dueño de proceso y al área de GRC aquellos casos en que se identifiquen incumplimientos normativos.

---

<sup>11</sup> Normograma: Es el inventario general de requisitos normativos. Permite identificar las políticas, procedimientos o controles definidos internamente por PISA, para dar cumplimiento a dichos requisitos establecidos en las normas. Se utiliza para verificar el cumplimiento normativo y generar planes de acción. También es un insumo para la identificación, por parte de las áreas, de los riesgos operativos por incumplimiento normativo.

PISA también debe garantizar que los procesos subcontratados sean controlados y monitoreados. El outsourcing de las operaciones de PISA no exime a esta de sus responsabilidades legales u obligaciones de cumplimiento. En caso de tercerización de actividades de PISA, se debe llevar a cabo una debida diligencia para garantizar que no se reduzcan los estándares y su compromiso con el cumplimiento normativo.

Así las cosas, si se identificaran situaciones que evidencien que no se da cumplimiento a algún requisito normativo, es necesario implementar planes de acción para dar solución oportuna. Estas acciones deben indicar los siguientes aspectos:

- ¿Qué se va a realizar?
- ¿Quién será responsable?
- ¿Cuándo se completará la acción?
- ¿Cómo se documenta?
- ¿Cómo se evaluará el cumplimiento normativo una vez se implemente la acción?

Estos planes de acción serán consolidados por el área de GRC con el fin de realizar seguimiento oportuno sobre la implementación de las acciones requeridas.

Todas las acciones deben tener definido un horizonte de tiempo razonable para su implementación teniendo en cuenta la criticidad del requisito normativo. En el caso en que el plazo se cumpla y la acción no haya finalizado, el área de GRC en asocio con la Administración decidirá si se otorga un nuevo plazo y si es necesario informar a la Alta Dirección del incumplimiento en los plazos.

#### 5.4 Informes de cumplimiento normativo y evaluación del desempeño de cumplimiento

Semestralmente, el área de GRC informará al Comité de Riesgos de PISA el estado de cumplimiento generado en el normograma y el estado actual de las acciones de mejora definidas por los dueños de procesos. Igualmente, reportará al Comité de Riesgos a aquellas situaciones en que se presenten riesgos significativos de incumplimiento, como también los planes de acción que no hayan sido resueltos de acuerdo con los tiempos definidos por las áreas responsables.

Los informes de cumplimiento normativo deben indicar el grado de cumplimiento que PISA logra sobre los requisitos normativos a los que está obligada. Para tal efecto, el Programa de Cumplimiento Normativo cuenta con un modelo de evaluación de desempeño mediante el monitoreo de indicadores medibles, con el fin de mejorar continuamente la eficiencia y efectividad del sistema de gestión.

Los siguientes indicadores serán medidos trimestralmente de acuerdo con la información que se tenga a la fecha del cálculo.

Nivel de compliance	Oportunidad en la resolución de acciones
$\frac{\text{No. de requisitos normativos marcados con compliance en el normograma}}{\text{No. de requisitos normativos aplicables a la compañía}} \times 100$	$\frac{\text{No. de acciones finalizadas oportunamente dentro de los tiempos definidos}}{\text{No. de acciones definidas con fecha de finalización previa a la medición}} \times 100$

#### 5.5 Gestión de incumplimientos y mejora continua

En caso de que se identifique alguna situación que evidencie que no se da cumplimiento a algún requisito normativo se debe:

- Revisar, validar y entender la situación de incumplimiento.
- Determinar la Causa Raíz<sup>12</sup> del incumplimiento.
- Determinar si incumplimientos similares están ocurriendo o podrían ocurrir teniendo en cuenta la Causa Raíz identificada.

<sup>12</sup> Causa Raíz: Factor que da origen a la oportunidad de mejora identificada. Puede ser originado en recurso humano, procesos, tecnología, infraestructura, acontecimientos externos o controles.

- Definir un plan de acción.
- Validar la efectividad de la implementación de planes de acción.

El seguimiento de estos planes de acción se realizará utilizando la misma metodología descrita en el numeral 5.3. Control de cumplimiento normativo.

PISA debe mantener documentadas las situaciones de incumplimientos identificadas, las acciones generadas para su solución y los resultados de dichas acciones.

Todos los incumplimientos identificados por las áreas de PISA deben ser informados al dueño de proceso y al área de GRC a la mayor brevedad posible con el fin de evaluar la gravedad del incumplimiento y coordinar los planes de acción correspondientes. Los incumplimientos que se evalúen con impacto significativo deben ser informados a la Administración, con el fin de que sean informados a la Alta Dirección y se establezcan los planes de acción prioritarios para subsanar el incumplimiento.

Si la normatividad exige a PISA que cualquier incumplimiento deba ser avisado a las autoridades regulatorias, dicho aviso debe hacerse a la mayor brevedad posible de acuerdo con las normas aplicables, indicando los planes de acción definidos.

Incluso si PISA no está obligada a dar aviso de situaciones de incumplimiento, PISA debe analizar el caso con el fin de decidir un aviso voluntario a las entidades regulatorias para mitigar las consecuencias del incumplimiento.

La información recopilada, analizada y evaluada debe ser utilizada como base para identificar oportunidades para mejorar el desempeño del Programa Cumplimiento Normativo de PISA.

## 6 RIESGOS DE CUMPLIMIENTO NORMATIVO

Los dueños de procesos tienen la máxima responsabilidad sobre la gestión de riesgos, controles y el cumplimiento normativo, apoyándose en la Gerencia Jurídica y en el área de GRC; esta última quien supervisa y revisa objetivamente la ejecución, la gestión y el control de riesgos de incumplimiento.

La identificación de riesgos de incumplimiento normativo se debe realizar desde 2 enfoques, a saber:

### 6.1 Riesgo corporativo de cumplimiento normativo

El Programa de Cumplimiento Normativo debe permitir la identificación de los Riesgos de Incumplimiento Normativo, específicamente el riesgo de sanciones legales o normativas, pérdida financiera material, o pérdida de reputación que puede sufrir PISA como resultado de incumplir con las leyes, regulaciones, normas, estándares de auto-regulación de PISA, y códigos de conducta aplicables a las actividades realizadas, entre otras.

Existen dos potenciales tipologías de riesgo asociadas al Riesgo de Incumplimiento Normativo, a saber:

- Riesgo Normativo (Sanciones): Se da cuando el incumplimiento normativo de la ley, las normas, los estándares, o los códigos de conducta se traduce, o tiene el potencial de traducirse, en sanciones para PISA por parte de las autoridades o de los organismos regulatorios.
- Riesgo Reputacional (deterioro de la reputación): Se materializa en el deterioro del buen nombre y la reputación de PISA, lo cual puede provocar un impacto adverso en los resultados, en el patrimonio, y en las expectativas de desarrollo de los negocios de PISA, pudiendo tener varias causas este deterioro. Se considera riesgo de cumplimiento normativo cuando se origina en el incumplimiento de las normas que le apliquen a PISA.

### 6.2 Riesgo Operacional de cumplimiento normativo

Las áreas, dentro de su análisis de riesgos realizado según metodología SARO, deben utilizar el NORMOGRAMA y demás herramientas generadas por el área de GRC para identificar posibles riesgos operacionales que no hayan sido previamente detectados.

Todos los requisitos normativos que requieran de algún tipo de operatividad del proceso, tales como la realización de cálculos, envío de reportes o que involucren algún tipo de periodicidad, deben ser considerados en la identificación de riesgos toda vez que podría ser necesaria la definición de controles específicos para mitigar el riesgo de fallas en la operación del proceso.

Indistintamente de si los riesgos identificados corresponden a los riesgos corporativos de cumplimiento normativo o a riesgos operacionales de cumplimiento normativo por proceso, se debe utilizar la metodología para la valoración, control y monitoreo de los riesgos definida en la Política SARO de PISA, identificando la probabilidad de ocurrencia del riesgo, la magnitud del impacto del riesgo y la identificación y evaluación de controles del procedimiento para la gestión de riesgo operativo.

Los riesgos que se identifiquen deben ser registrados en la matriz de riesgos y controles del proceso.

Al igual que lo definido en el procedimiento de gestión de riesgo operacional, las matrices deben ser actualizadas y monitoreadas en caso de presentarse cambios en los procesos o cuando se presenten cambios normativos.

## 7 AUTORIDAD Y CAPACIDADES DEL ÁREA DE GRC ANTE EL PROGRAMA DE CUMPLIMIENTO NORMATIVO

### 7.1 Investigar y cuestionar

Cuando el área de GRC perciba un riesgo de cumplimiento normativo o cuando una decisión de PISA pueda dar lugar a un Riesgo de Incumplimiento Normativo significativo para PISA, el área de GRC debe estar en la capacidad de investigar y cuestionar la decisión con independencia del negocio. Si el asunto no se resuelve rápidamente, el área de GRC debe poder iniciar el proceso de escalamiento. En este escenario, corresponde al Coordinador de GRC el deber de informar a la Administración y a la Alta Dirección.

### 7.2 Escalar

Toda persona que identifique una situación que pueda poner en Riesgo de Incumplimiento Normativo a PISA, debe informarlo al dueño de proceso y al área de GRC a la mayor brevedad posible, para que se defina si se debe informar a la Administración y/o a la Alta Dirección, después de analizar si se genera Riesgo de Incumplimiento Normativo significativo.

En caso de presentarse casos importantes de Riesgo de Incumplimiento Normativo, el Coordinador de GRC debe coordinar a la mayor brevedad posible la definición oportuna de planes de acción para dar solución al posible Riesgo de Incumplimiento Normativo.

### 7.3 Acceso

El área de GRC debe tener acceso a todas las actividades en su área de responsabilidad. Esto incluye acceso a todos los niveles de PISA, como también a la documentación, información, sistemas, que requiera para llevar a cabo los análisis del Programa de Cumplimiento Normativo.

### 7.4 Consolidación de planes de acción

PISA se debe comprometer al desarrollo de acciones de mejora para la eliminación de las causas de incumplimiento normativo de requisitos y corregir aquellos eventos que puedan afectar el desempeño de los procesos con el fin último de mejorar continuamente la eficacia, eficiencia y efectividad de los procesos.

## 8 GESTIÓN DE SEGUIMIENTO DE PLANES DE ACCIÓN

Es responsabilidad de todos los líderes de procesos definir y registrar planes de acción sobre los diferentes procesos y sistemas de PISA, así como realizar el seguimiento y cierre de las acciones en los periodos establecidos.

Los planes de acción deben ser definidos entre el área que identifica la oportunidad de mejora y el dueño del proceso.

Las personas responsables de los planes de acción deberán realizar los seguimientos y cierre de los mismos, garantizando contar con las evidencias necesarias cuando sea necesario.

Las áreas deben identificar la Causa Raíz de la situación presentada con el objetivo de generar un plan de acción enfocado a la eliminación de la Causa Raíz.

El área de GRC realizará la consolidación de los planes de acción definidos por las áreas para poder presentar periódicamente el estado del Programa de Cumplimiento Normativo y sus planes de acción al Comité de Riesgos y/o a la Alta Dirección.

## 9 INFORMACIÓN Y COMUNICACIÓN

### 9.1 Repositorio de Información

PISA debe contar con un repositorio de información (normograma) que permita soportar los elementos del Programa de Cumplimiento Normativo, así como con herramientas que permiten hacer una gestión de los riesgos identificados y los controles implementados (matriz de riesgos y controles). Con lo anterior se garantiza la disponibilidad, oportunidad y confiabilidad de la información relacionada con los eventos de incumplimiento normativo gestionados.

### 9.2 Plan de Comunicación

Conscientes que una comunicación efectiva es un elemento fundamental para la implementación, interiorización, mantenimiento y sostenibilidad del Programa de Cumplimiento Normativo, PISA debe desarrollar un plan de comunicación anual que promueva y afiance la Cultura de Cumplimiento Normativo, además de concientizar a los colaboradores de la importancia de prevenir, denunciar y gestionar dicho Programa. El plan de comunicaciones debe incluir campañas internas, material de apoyo, comunicaciones escritas, correos electrónicos, etc., donde se subrayan los aspectos más relevantes del Programa de Cumplimiento Normativo, sus lineamientos relacionados y la importancia del control interno.

## 10 CAPACITACIÓN Y ENTRENAMIENTO

Dentro del proceso de inducción de un colaborador nuevo y al menos anualmente se debe realizar una capacitación y/o actualización sobre la Política de Cumplimiento Normativo, que abarque:

- El compromiso de PISA en la prevención de incumplimientos normativos.
- Las ventajas de un Programa de Cumplimiento Normativo.
- Los eventos o conductas que pueden constituir incumplimiento normativo y la forma de reportarlas.
- Los perjuicios de cometer un incumplimiento normativo y las sanciones disciplinarias que ello implica.

La capacitación y entrenamiento se puede brindar en forma periódica, virtual o presencial y de manera selectiva a los colaboradores de PISA, con el propósito de fortalecer los conceptos y asegurar la continuidad y sostenibilidad del Programa de Cumplimiento Normativo.

## 11 MONITOREO

Se debe realizar una revisión, como mínimo, anual de los objetivos y componentes de la Política de Cumplimiento Normativo y de las políticas o lineamientos relacionados, además de un monitoreo de los riesgos identificados y de la suficiencia, idoneidad y efectividad de los controles implementados en los diferentes procesos como parte de la implementación de esta Política por parte del Área de GRC, quien es responsable de velar porque se ejecute adecuadamente el Programa de Cumplimiento Normativo.

En todo caso cada colaborador de PISA es responsable por asegurar el cumplimiento de los controles a su cargo y de los estándares éticos establecidos en esta Política, así como de reportar los incidentes conocidos y/o identificados, al dueño del proceso y al área de GRC, a través de correo electrónico, correo físico, o de cualquier otro medio que se considere adecuado.

## 12 SANCIONES

El incumplimiento de lo previsto en la presente Política por parte de cualquier colaborador constituye una falta que será investigada y sancionada de conformidad con lo contemplado en el Reglamento Interno de Trabajo, en el contrato de trabajo y en la Ley.

Lo anterior, sin perjuicio de las acciones penales, administrativas, civiles o de cualquier otra índole a que dé lugar el incumplimiento, consagradas en las normas jurídicas que conforman el marco legal de la presente Política.

## 13 DOCUMENTO DE APROBACIÓN

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

## 14 DOCUMENTOS RELACIONADOS

CÓDIGO	NOMBRE DEL DOCUMENTO
PE-DG-06	Código de ética y conducta
N/A	Código de buen gobierno
N/A	Política de cumplimiento normativo de Corficolombiana
GRC-PT-04	Gestión del riesgo de cumplimiento normativo
GRC-PT-02	Actualización de normograma
GRC-PT-03	Gestión de planes de acción por incumplimientos normativos

## 15 FORMATOS RELACIONADOS Y/O REGISTROS

CÓDIGO	NOMBRE DEL FORMATO
CFC-RE-CO-43	Normograma

## 16 CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
N° Acta 358 23-02-2021	01	<p>Documento aprobado por: Jefe de Mejoramiento y Sostenibilidad (10/02/2021), Coordinador de GRC (11/02/2021), Gerente Administrativo (11/02/2021), Gerente Jurídico (15/02/2021), Gerente Financiero (04/03/2021)</p> <p>Primera versión del documento.</p> <p>03/06/2022 – 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 el nombre de los siguientes cargos: <ul style="list-style-type: none"> <li>○ Presidente por Gerente General</li> <li>○ Gerente Financiero por Director Financiero</li> </ul> </li> </ul> <p>23/05/2024 – Se realiza el siguiente cambio menor:</p> <ul style="list-style-type: none"> <li>• Se actualiza la estructura del documento, de acuerdo con el estándar actualmente establecido por el área de Mejoramiento.</li> <li>• Se elimina la palabra "Defensa" al término Línea de Defensa.</li> <li>• Se cambia el nombre del cargo Director Financiero por Jefe Financiero.</li> </ul>
N° Acta 410 18-02-2025	02	<p>Se realizan los siguientes ajustes.</p> <ul style="list-style-type: none"> <li>• 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 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.</li> <li>• Se incluye la competencia que tiene la Junta Directiva frente a las políticas corporativas</li> <li>• Se actualiza el nombre del cargo del área responsable de la autorización y acceso de este documento, pasado de área de Mejoramiento y Sostenibilidad y Área de Procesos.</li> <li>• Se cambia el nombre del cargo del Jefe Financiero por Director Financiero</li> </ul>