TABLA DE CONTENIDO

1 INTRODUCCIÓN 2
2 DEFINICIONES 3
3 ALCANCE 5
4 OBJETIVOS 6
5 POLITICAS DE CUMPLIMIENTO NORMATIVO 7
6 ETAPAS DEL SISTEMA 8
7 RIESGOS DE CUMPLIMIENTO NORMATIVO (COMPLIANCE) 12
8 AUTORIDAD Y CAPACIDADES DE LA FUNCIÓN DE CUMPLIMIENTO NORMATIVO 13
9 GESTION DE SEGUIMIENTO DE PLANES DE ACCION 14
10 ESTRUCTURA, ROLES Y RESPONSABILIDADES 15
11 INFORMACIÓN Y COMUNICACIÓN 19
12 CAPACITACIÓN Y ENTRENAMIENTO 20
13 MONITOREO 20
14 SANCIONES 20
15 DOCUMENTOS DE REFERENCIA 21
16 CONTROL DE CAMBIOS 21
17 FIRMAS DE REVISIÓN Y APROBACIÓN 22

1 INTRODUCCIÓN

En el mundo moderno las empresas operan en entornos altamente regulados, con exigencias basadas en el cumplimiento de obligaciones y deberes fundamentados en leyes, normas, estándares de industria, contratos, y políticas internas de la más variada índole. En dichos escenarios, se hace realmente indispensable contar con mecanismos que aseguren el cumplimiento de dichas obligaciones legales, dado que la materialización de esos riesgos podría afectar los resultados financieros, así como la confianza del mercado y de los inversionistas en general.

Es por esto por lo que **PROINDESA S.A.S Y SUS SOCIEDADES ADMINISTRADAS,** en adelante **"LA ORGANIZACIÓN"**, consciente de la necesidad de gestionar el cumplimiento de las normas desde la perspectiva de riesgos, ha decidido incorporar dentro de su Gobierno Corporativo la función de cumplimiento normativo.

Este documento define el marco común del Modelo de Cumplimiento Normativo, que forma parte de las funciones de Gobierno, Riesgo y Cumplimiento, en adelante "GRC" en **LA ORGANIZACIÓN**, el cual se soporta en las siguientes premisas:

- **LA ORGANIZACIÓN** 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 de las funciones de Riesgo y Cumplimiento normativo.
- **LA ORGANIZACIÓN** reconoce la necesidad de articular los canales de comunicación y supervisión de las funciones de GRC, con las filiales del sector de infraestructura.
- **LA ORGANIZACIÓN** es consciente de la necesidad de generar y estandarizar el conocimiento sobre el cual se soporten las diferentes funciones de GRC a nivel corporativo.
- **LA ORGANIZACIÓN** ha compilado los procedimientos y controles que actualmente están implantados, para la efectiva prevención, detección y gestión ante cualquier tipo de riesgo normativo. Todo ello con el objetivo último de promover y potenciar una verdadera cultura de cumplimiento normativo capaz de reflejar su ética, asentar sus mecanismos de control y reducir la posibilidad de que se cometan incumplimientos normativos en su nombre, directa o indirectamente.
- **LA ORGANIZACIÓN** ha generado políticas relacionadas con la gestión del Riesgo y Cumplimiento para la aplicación y cumplimiento de todas sus filiales, las cuales serán adoptadas e interiorizadas en el modelo de GRC de **LA ORGANIZACIÓN**.

- Este documento fue definido teniendo en cuenta los marcos de referencia ISO 19600:2015 (Gestión de sistemas de Cumplimiento), el Estándar Australiano AS 3806-2006, EY Cumplimiento life cycle y la Guía de Criterios de Evaluación de la Función de Cumplimiento del Marco Integral de Supervisión MIS de la Superintendencia Financiera de Colombia.
- Este documento define en **LA ORGANIZACIÓN** el alcance del programa de Cumplimiento normativo, 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 una relación de documentos de referencia y anexos.

2 DEFINICIONES

- **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 el presente documento se utiliza indistintamente el término Cumplimiento normativo o función de Cumplimiento normativo.
- **Cumplimiento Normativo:** El Cumplimiento Normativo es el programa conformado por las políticas y procedimientos adecuados y suficientes para asegurar que, en la organización incluida la Alta Dirección, colaboradores y agentes vinculados, 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 clientes, proveedores o terceros, y especialmente los códigos éticos que la organización se hayan comprometido a respetar.
- **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.
- **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.
- **Falla de Cumplimiento normativo:** Es todo acto u omisión, voluntario o involuntario, por el cual una Organización no ha cumplido con sus obligaciones de cumplimiento normativo, procesos u obligaciones de comportamiento.
- **Función de Cumplimiento normativo:** Tiene como finalidad hacer una vigilancia independiente de la gestión que las entidades hacen respecto del cumplimiento

normativo (leyes, decretos, reglamentos, regulaciones), estándares de auto-regulación de la organización o de la industria a la que pertenecen, políticas de revelación de información al mercado y a las partes interesadas, políticas para la generación de informes y relacionamiento con clientes, directrices y el código de ética y conducta aplicable 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.[1]

- **Director de Riesgos:** Es la persona responsable de gestionar las políticas y procedimientos del cumplimiento normativo para **LA ORGANIZACIÓN**.

  La Dirección de Riesgos es la encargada de administrar el Programa de Cumplimiento Normativo. Administra el Normograma como repositorio de información de la gestión de **LA ORGANIZACIÓN** para asegurar el cumplimiento de la normatividad.

- **Normograma:** Es el inventario general de requisitos normativos. Permite identificar las políticas, procedimientos o controles definidos internamente por la organización, para dar cumplimiento a dichos requisitos establecidos en la normatividad. 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.

- **Oportunidad de mejora:** Son situaciones evidenciadas en los procesos por observaciones en las evaluaciones de control interno, revisoría fiscal, eventos de riesgo, acciones definidas por Alta Dirección o situaciones identificadas por los propios dueños de procesos para el mejoramiento de sus procedimientos.

- **Plan de acción:** Es el conjunto de acciones tomadas para eliminar la(s) causa(s) de una oportunidad de mejora derivada de evaluaciones de control interno, eventos de riesgo o mejora de proceso.

- **Programa de Cumplimiento normativo:** Es el conjunto de políticas y procedimientos adecuados y suficientes para asegurar que, en **LA ORGANIZACIÓN**, incluidos sus directivos, colaboradores y agentes vinculados, cumplen con el marco normativo aplicable.

[1] Tomado de la Guía Cumplimiento del Marco Integral de Supervisión de la Superintendencia Financiera de Colombia.

- **Riesgo de incumplimiento normativo:** El riesgo de sanciones legales o reglamentarias, pérdidas financieras materiales o pérdida de la reputación que la organización puede sufrir como resultado del incumplimiento de las leyes, decretos, reglamentos, y demás normas relacionadas, de las normas de instituciones reguladoras, así como el código de ética y conducta aplicable a la organización.

3 ALCANCE

En **LA ORGANIZACIÓN,** el control y el cumplimiento normativo hacen parte indispensable de la cultura de trabajo. La observación estricta de esta normativa puede evitar considerables riesgos económicos y reputacionales para la esta, sus administradores y colaboradores. Por lo anterior, se ha adoptado el Sistema de gestión de riesgo normativo, el cual es administrado por la Dirección de Riesgos de PROINDESA S.A.S

La Presente Política está dirigida y será aplicable a **Proindesa S.A.S y sus Sociedades Administradas[2], en adelante "LA ORGANIZACIÓN".**

El programa de cumplimiento normativo establecido en el presente documento abarca todas las actividades y negocios que se realiza **LA ORGANIZACIÓN** en desarrollo de su objeto social.

Es decisión de la Junta Directiva de Corficolombiana que las entidades financieras y entidades del sector real subordinadas de esta, apliquen procedimientos similares a los implementados por la Corporación, atendiendo en todo caso las características particulares de la actividad desarrollada por cada una de las mencionadas entidades.

Asimismo, PROINDESA S.A.S debe velar porque las sociedades del sector de infraestructura adopten las políticas y demás metodologías indicadas en la presente política.

El Programa de Cumplimiento Normativo persigue dos grandes objetivos a saber:

- Prevención del riesgo: Su objetivo es impedir los incumplimientos normativos en **LA ORGANIZACIÓN**.
- Control del riesgo: Busca 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 **LA ORGANIZACIÓN**.

[2] Incluye a aquellas sociedades con las cuales Proindesa mantenga vigente acuerdo de colaboración.

La Función de Cumplimiento Normativo se lleva a cabo de manera independiente a los diferentes procesos, sin perjuicio a aquellas tareas que realizan las áreas de auditoría interna.

La gestión de la Función de Cumplimiento Normativo abarca todo tipo de normatividad, principalmente las siguientes:

- Leyes, decretos, resoluciones, reglamentos, etc.
- Estándares de auto-regulación de la organización 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 código de ética y conducta
- Instrucciones y lineamientos corporativos

4 OBJETIVOS

4.1. Objetivo General

Proporcionar confianza a los Accionistas, a la Alta Dirección y al mercado respecto del cumplimiento normativo en general por parte de **LA ORGANIZACIÓN**.

4.2. Objetivos Específicos

- Fijar la posición de **LA ORGANIZACIÓN** frente a la responsabilidad de cumplimiento normativo.
- Identificar los principales riesgos normativos a los que está expuesto **LA ORGANIZACIÓN** con el propósito de implementar controles y procesos efectivos, suficientes y oportunos para mitigar tales riesgos.
- Definir las metodologías 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 requisitos para la identificación y documentación de planes de acción.
- Definir responsabilidades para la identificación, definición, seguimiento y cierre de planes de acción.
- Definir la información base para el registro de planes de acción.
- Indicar las consecuencias que podrían conllevar el incumplimiento normativo.

5 POLITICAS DE CUMPLIMIENTO NORMATIVO

5.1. Política General

LA ORGANIZACIÓN se compromete a establecer los elementos del Programa de Cumplimiento Normativo con el fin de asegurar que se cumple con la normatividad aplicable (tanto interna como externa), y se aúnan esfuerzos por cumplir las normas y buenas prácticas que se aplican a sus actividades y responsabilidades cotidianas.

5.2. Función de Cumplimiento Normativo

La función de Cumplimiento Normativo supone 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. Para tal efecto, **LA ORGANIZACIÓN** ha definido una función de Cumplimiento Normativo liderada por el Director de Riesgos, quien cuenta con los recursos humanos, metodológicos y técnicos para la gestión de dicha función en **LA ORGANIZACIÓN**.

5.3. Órgano de verificación – Dirección de Riesgos

La Dirección de Riesgos es la encargada de la administración del Programa de Cumplimiento Normativo. Es considerada parte de la Función de Cumplimiento, que ayuda a **LA ORGANIZACIÓN** a vigilar regularmente el cumplimiento de la normatividad, así como la ejecución de medidas correctivas cuando se requieran para asegurar el cumplimiento de las obligaciones normativas de la misma.

5.4. Independencia de la función

La Función de Cumplimiento Normativo se posiciona independientemente del negocio que supervisa. Esta posición independiente es garantizada por informes autónomos, acceso a la Alta Dirección y a la Junta Directiva o quien haga sus veces.

5.5. Propósito de la función

- Trabajar de forma proactiva con las sociedades de infraestructura y asesorarlas para gestionar el riesgo de incumplimiento normativo.
- Desarrollar y mejorar herramientas para fortalecer las tres líneas de defensa para detectar, comunicar, administrar e informar sobre riesgos de incumplimiento normativo.
- Apoyar la estrategia de **LA ORGANIZACIÓN** estableciendo roles y responsabilidades claros para ayudar a incorporar buenas prácticas de

cumplimiento normativo en toda LA ORGANIZACIÓN mediante el uso de un enfoque basado en el riesgo para alinear los resultados comerciales con el apetito por el riesgo de **LA ORGANIZACIÓN**.

- Profundizar la cultura de cumplimiento normativo de **LA ORGANIZACIÓN** para aumentar la cultura de confianza, responsabilidad, transparencia e integridad en la evaluación la gestión y la presentación de informes sobre el riesgo de incumplimiento normativo.

6 ETAPAS DEL SISTEMA

6.1. Identificación de requerimientos normativos, requerimientos de terceras partes y principios de buen gobierno

La identificación de requerimientos normativos se realiza utilizando el normograma definido por **LA ORGANIZACIÓN,** 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 entidades certificadoras o proveedores y 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 los 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 las Direcciones Jurídicas de **LA ORGANIZACIÓN** son aplicables a los procesos.

- **Direcciones Jurídicas**[3]**:** Al estar en contacto con nuevas leyes, circulares y normas normatividad en general, las Direcciones Jurídicas de Proindesa tienen la responsabilidad informar sobre nueva normatividad que podría ser aplicada en los procesos de **LA ORGANIZACIÓN**. Estas Direcciones también cuenta con la obligación de asesorar a los dueños de los procesos en la validación de la aplicabilidad de los requisitos normativos.

- **Dirección de Riesgos:** En esta etapa, la Dirección de Riesgos brinda asesoría a las áreas dueñas de proceso para el diligenciamiento del Normograma y proporciona los mecanismos necesarios para realizar seguimiento a los planes de acción que se generen a partir de nuevos requisitos normativos.

6.2. 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.

6.3. Control de cumplimiento normativo

Se necesitan controles efectivos para garantizar que se cumplan los requisitos normativos en **LA ORGANIZACIÓN**, 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 la organización 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 del proceso y a la Dirección de Riesgos aquellos casos en que se identifiquen incumplimientos normativos.

[3] Dirección Jurídica Corporativa, Dirección Jurídica Administrativista y Dirección de Litigios.

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

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 la Dirección de Riesgos con el fin de realizar seguimiento oportuno sobre la implementación de acciones.

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, la Dirección de Riesgos decidirá si se otorga un nuevo plazo y si es necesario informar a la Alta Dirección del incumplimiento en los plazos.

6.4. Informes de cumplimiento normativo y evaluación del desempeño de cumplimiento

Semestralmente, la Dirección de Riesgos informará a la Alta Dirección a través de los Informes de gestión de riesgos, el estado de cumplimiento generado en el normograma y el estado actual de las acciones de mejora definidas por los dueños de procesos.

Asimismo, la Dirección de Riesgos incorporara en los mencionados informes 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 **LA ORGANIZACIÓN** logra sobre los requisitos normativos a los que está obligada. Para tal efecto, el programa cuenta con un modelo de evaluación de desempeño mediante el

monitoreo de indicadores medibles[4], con el fin de mejorar continuamente la eficiencia y efectividad del sistema de gestión.

6.5. 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 del incumplimiento
- Determinar si incumplimientos similares están ocurriendo o podrían ocurrir teniendo en cuenta la causa raíz identificada.
- Definir un plan de acción
- Validar la efectividad de la implementación de planes de acción

El seguimiento de estos planes de acción se realizará de acuerdo con en lo establecido en el Procedimiento de seguimiento y consolidación de planes de acción de cumplimiento, P-0212.

LA ORGANIZACIÓN 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 **LA ORGANIZACIÓN** deben ser informados a la Dirección de Riesgos 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 Vicepresidencia Financiera y Administrativa, con el fin de que sea informado a la Alta dirección y se establezcan los planes de acción prioritarios para subsanar el incumplimiento.

Si la normatividad exige a **LA ORGANIZACIÓN** que le sea avisado de cualquier incumplimiento, se debe avisar a las autoridades regulatorias a la mayor brevedad posible de acuerdo con las normas aplicables, indicando los planes de acción definidos.

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

[4] P-0213 Procedimiento para la Gestión de Riesgo de Cumplimiento Normativo.

Todos los colaboradores de la organización están en la obligación de avisar a los dueños del proceso y a la Dirección de Riesgos sobre cualquier situación de incumplimiento que se pueda evidenciar en los procesos de **LA ORGANIZACIÓN**.

La información recopilada, analizada y evaluada debe ser utilizada como base para identificar oportunidades para mejorar el desempeño de cumplimiento de la organización.

7 RIESGOS DE CUMPLIMIENTO NORMATIVO (COMPLIANCE)

Los dueños de procesos tienen la máxima responsabilidad sobre la gestión de riesgos, controles y el cumplimiento normativo, apoyándose en la Dirección de Riesgos, la cual supervisa y desafía objetivamente la ejecución, la gestión y el control de riesgos de incumplimiento.

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

7.1. Riesgo de cumplimiento normativo

La Función de Cumplimiento Normativo debe permitir la identificación de los riesgos de incumplimiento, específicamente el riesgo de sanciones legales o normativas, pérdida financiera material, o pérdida de reputación que puede sufrir **LA ORGANIZACIÓN** como resultado de incumplir con las leyes, regulaciones, normas, estándares de auto-regulación de **LA ORGANIZACIÓN**, y Código de Ética y Conducta aplicable a las actividades realizadas, entre otras.

Existen dos potenciales tipologías de riesgo asociadas al riesgo de incumplimiento normativo, pues el impacto adverso puede manifestarse en los resultados, o en las expectativas de desarrollo de los negocios de **LA ORGANIZACIÓN**, como consecuencia de:

- Sanciones
- Deterioro de la reputación

- **Riesgo Normativo (Sanciones):** Se da cuando el incumplimiento normativo de la ley, las normas, los estándares, o el Código de Ética y Conducta se traduce, o potencialmente puede traducirse, en sanciones para **LA ORGANIZACIÓN** 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 **LA ORGANIZACIÓN**, que pueda provocar un impacto

adverso en los resultados, en el patrimonio, y en las expectativas de desarrollo de los negocios de **LA ORGANIZACIÓN**. 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 **LA ORGANIZACIÓN**.

7.2. 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 la Dirección de Riesgos 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 de cumplimiento normativo corporativos 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 de Riesgo Operacional de **LA ORGANIZACIÓN,** identificando la probabilidad de ocurrencia del riesgo, la magnitud del impacto del riesgo y la identificación y evaluación de controles definidas para la gestión de riesgo operativo.

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

De acuerdo con lo definido en la Política de Riesgo operativo, las matrices deben ser actualizadas y monitoreadas en caso de presentarse cambios en los procesos, productos o cuando se presenten cambios normativos.

8 AUTORIDAD Y CAPACIDADES DE LA FUNCIÓN DE CUMPLIMIENTO NORMATIVO

8.1. Investigar y cuestionar:

Cuando los representantes de la Función de Cumplimiento Normativo perciben un riesgo de cumplimiento normativo o cuando una decisión de **LA ORGANIZACIÓN** pueda dar lugar a un riesgo de incumplimiento significativo para **LA ORGANIZACIÓN**, esta debe estar en la capacidad de investigar y cuestionar la decisión con independencia del negocio. Si el asunto no se resuelve rápidamente, la Dirección de Riesgos debe poder iniciar el proceso de

escalamiento. En este escenario, corresponde al Director de Riesgos tener la autoridad informar a los niveles superiores de la Organización.

8.2. Escalar:

Toda persona que identifique una situación que pueda poner en riesgo de incumplimiento normativo a **LA ORGANIZACIÓN**, debe informarlo a la Dirección de Riesgos a la mayor brevedad posible, para que se defina si se debe informar a la Alta Dirección, después de analizar si se genera riesgo significativo de incumplimiento normativo.

En caso de presentarse casos importantes de riesgo de incumplimiento normativo, el Director de Riesgos o quien hagas sus veces debe coordinar a la mayor brevedad posible la definición oportuna de planes de acción para dar solución al posible riesgo de incumplimiento.

8.3. Acceso:

El Director de Riesgos o quien haga sus veces debe tener acceso a todas las actividades en su área de responsabilidad. Esto incluye acceso a todos los niveles de la organización, como también a la documentación, información, sistemas, que requiera para llevar a cabo los análisis de la Función de Cumplimiento Normativo.

8.4. Consolidación de planes de acción

LA ORGANIZACIÓN se compromete 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 estos.

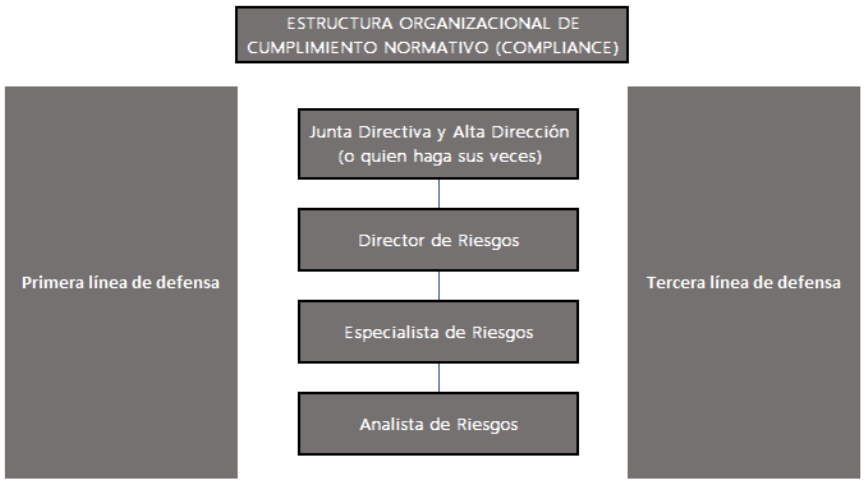
9 GESTION DE SEGUIMIENTO DE PLANES DE ACCION

- Es responsabilidad de todos los líderes de los procesos definir y registrar planes de acción sobre los diferentes procesos y sistemas de **LA ORGANIZACIÓN**, 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 sean requeridas.

- 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.
- La Dirección de Riesgos realizará la consolidación de los planes de acción definidos por las áreas para poder presentar periódicamente el estado de cumplimiento normativo de planes de acción a la alta dirección.

10 ESTRUCTURA, ROLES Y RESPONSABILIDADES



- El Director de Riesgos cuenta con jerarquía y autoridad dentro de la organización para el desarrollo efectivo de sus responsabilidades.
- La Función de Cumplimiento Normativo es independiente de las unidades de negocio y de los procesos de cumplimiento normativo que ejecutan en el día-a-día de sus actividades funcionales.

10.1. Roles y responsabilidades -Primera Línea de defensa –

10.1.1 Alta Dirección (Asamblea de Accionistas, Junta Directiva, representante Legal y Vicepresidentes o quienes hagan sus veces

- Establecer un conjunto fuerte de valores que se encuentren arraigados en la cultura de **LA ORGANIZACIÓN**.
- Operar bajo los objetivos de Cumplimiento normativo definidos por la Junta Directiva o quien haga sus veces, para alinear la estrategia de **LA ORGANIZACIÓN**.
- La Alta Dirección debe asegurarse que la función de Cumplimiento normativo tenga la autoridad para actuar de manera independiente y no se vea

comprometida por prioridades en conflicto, particularmente cuando el cumplimiento normativo está incrustado en el negocio.

- Comunicar la importancia del sistema de gestión de cumplimiento normativo.
- Asegurar la aplicación de la Política de Cumplimiento Normativo para la efectiva y permanente acción de la Función de 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 la organización y que los incumplimientos normativos son tratados apropiadamente.
- Ubicar los recursos apropiados para implementar, evaluar, mantener y mejorar el sistema de gestión de cumplimiento normativo.

10.1.2. Áreas de negocio, apoyo y operativas

- 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.

- Asegurar que los riesgos son 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 las Direcciones Jurídicas o mediante fuentes adicionales de información, y traducir esos requisitos en políticas y procedimientos procesables.

- Colaborar con la Dirección de Riesgos brindando todo el apoyo necesario.

- 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 incumplimiento normativos.

- Dar solución oportuna de situaciones de incumplimiento normativo según lo dispuesto en el presente documento.

10.1.3. Direcciones Jurídicas

- Mantenerse actualizado con las regulaciones generadas.
- Informar a los dueños de procesos y a la Función de Cumplimiento Normativo sobre nueva normatividad que sea aplicable a la organización.
- Brindar asesoría en el entendimiento de los requisitos normativos que aplican a la organización.

10.1.4. Todos los colaboradores

- Ser conscientes de los requisitos normativos relevantes a sus roles y responsabilidades.
- Cumplir con las políticas y procedimientos requeridos para su rol.
- Identificar y reportar oportunamente situaciones de posibles incumplimientos normativos.
- Asistir en las capacitaciones de cumplimiento normativo convocadas por **LA ORGANIZACIÓN**.

10.2. Roles y responsabilidades Segunda Línea de defensa

10.2.1. Dirección de Riesgos

Como parte de la segunda línea de defensa, tiene entre sus responsabilidades las siguientes:

- Diseñar un sistema de gestión de Cumplimiento normativo efectivo y eficiente.
- Asegurar que los riesgos regulatorios y reputacionales sean adecuadamente identificados, controlados, monitoreados, evaluados y reportados.
- Desarrollar un marco de referencia y políticas estructuradas para soportar la gestión de Cumplimiento normativo.
- Dar asesoramiento a las áreas para la implementación del sistema de gestión 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 cumplimento normativo de la organización y, posteriormente establecer los controles necesarios.

- Establecer la estructura metodológica y funcional para administrar el inventario de los requisitos normativos que aplican a **LA ORGANIZACIÓN**.

- Asegurar que la función de cumplimiento normativo esté al tanto de los cambios en la legislación y reglas aplicables y en el perfil de riesgos de **LA ORGANIZACIÓN**.

- Proveer de capacitaciones y entrenamientos necesarios en esta materia a los colaboradores de **LA ORGANIZACIÓN**.

- Proponer la actualización oportuna de las políticas de cumplimiento normativo de **LA ORGANIZACIÓN** cuando surja nueva legislación o se modifique la existente. A su turno, cuando **LA ORGANIZACIÓN** afronte nuevos requerimientos legislativos como consecuencia del desarrollo de nuevos negocios o cambios en sus negocios actuales.

- Administrar los indicadores de cumplimiento normativo y realizar el monitoreo respectivo para generar acciones de mejora sobre el sistema.

- Presentar informes semestrales de gestión a la Junta Directiva o quien haga sus veces.

- Adoptar y socializar las mejores prácticas para asegurar el cumplimiento normativo por parte de **LA ORGANIZACIÓN**.

- 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 de la Función de Cumplimiento normativo.

- Promover una cultura Cumplimiento normativo dentro de **LA ORGANIZACIÓN**.

- Asegurar que el programa de Cumplimiento normativo sea revisado de manera regular.

- Participar en el proceso de creación de nuevas líneas de negocio con el fin de asegurar que los riesgos de cumplimiento normativo estén debidamente identificados y controlados, y que la incursión en estas, el cumpla con la regulación y políticas internas aplicables.

- Liderar el proceso de escalamiento de asuntos no éticos en **LA ORGANIZACIÓN** para garantizar una adecuada atención y manejo de los temas que así lo requieran. La Dirección de riesgos es responsable de coordinar y establecer las acciones a seguir con las áreas requeridas en la investigación.

10.3. Roles y responsabilidades Tercera Línea de defensa

10.3.1. Auditoría

- Evaluar de manera independiente los controles definidos por la primera línea de defensa para mitigar los riesgos de incumplimiento normativo.
- La Auditoría debe realizar una evaluación de la Política 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.

11 INFORMACIÓN Y COMUNICACIÓN

11.1. Repositorio de información

LA ORGANIZACIÓN debe contar con un repositorio de información (normograma) que permita soportar los elementos del programa de Cumplimiento normativo, así como con herramientas que permitan 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.

11.2. Plan de comunicación

Una comunicación efectiva es un elemento fundamental para la implementación, interiorización, mantenimiento y sostenibilidad de un programa de cumplimiento normativo.

LA ORGANIZACIÓN debe desarrollar planes de comunicaciones anualmente para promover y afianzar la cultura de cumplimiento normativo, además de concientizar a los colaboradores de la importancia de prevenir, detectar y gestionar el cumplimiento normativo (compliance). El plan de comunicaciones debe incluir campañas internas, material de apoyo, comunicaciones escritas, correos electrónicos, etc., donde se subrayen los aspectos más relevantes de la Política Cumplimiento Normativo, sus lineamientos relacionados y la importancia del control interno.

12 CAPACITACIÓN Y ENTRENAMIENTO

Dentro del proceso de inducción de un colaborador nuevo y al menos anualmente, deben realizarse capacitaciones sobre la Política de Cumplimiento Normativo, que abarque, entre otros temas, los siguientes:

- El compromiso de **LA ORGANIZACIÓN** con la prevención del incumplimiento normativo.
- Las ventajas de un programa cumplimiento normativo.
- Los eventos o conductas que pueden constituir incumplimiento normativo y que deban ser reportadas.
- Los perjuicios de cometer un incumplimiento normativo, actos ilegales o conductas antiéticas, y las sanciones disciplinarias que ello implica.

La capacitación y entrenamiento se puede brindar en forma continua, virtual o presencial y de manera selectiva a los colaboradores de **LA ORGANIZACIÓN**, con el propósito de fortalecer los conceptos y asegurar la continuidad y sostenibilidad del programa de cumplimiento normativo.

13 MONITOREO

Al menos una vez al año, se debe realizar una revisión de los objetivos y componentes de la Política de Cumplimiento Normativo y 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. Esta revisión está a cargo de la Dirección de Riesgos.

En todo caso, cada colaborador de **LA ORGANIZACIÓN** es responsable por asegurar el cumplimiento normativo 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 de proceso y a la Dirección de Riesgos, a través de correo electrónico o mesas de trabajo, o cualquier otro medio que se considere adecuado.

14 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 y el Código de Ética y Conducta, 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.

15 DOCUMENTOS DE REFERENCIA

- P-0213 Procedimiento para la gestión de riesgo de cumplimiento normativo
- P-0214 Procedimiento para la actualización del normograma
- P-0212 Procedimiento de seguimiento y consolidación de planes de acción de cumplimiento.

16 CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	25/02/2021	Creación del documento. Definición de lineamientos de Cumplimiento Normativo (Compliance) de acuerdo con la iniciativa de GRC de CFC número 11. Definición del programa corporativo de compliance.

17 FIRMAS DE REVISIÓN Y APROBACIÓN

Elaborador por:	Revisado por:	Aprobado por:
FIRMADO EN ORIGINAL	**FIRMADO EN ORIGINAL**	**FIRMADO EN ORIGINAL**
ASISTENTE DE PROCESOS	**DIRECTOR DE RIESGOS**	**VICEPRESIDENTE FINANCIERA Y ADMINISTRATIVA**
LILIAN ALEXANDRA ARRIERO	MARGARITA RAMÍREZ HERRERA	VANESSA GARAY GUZMÁN