



**Global
Multifuncional**

Política

**POLÍTICA DE CONTROL Y GESTIÓN DE RIESGOS
DE
ENEL COLOMBIA**



ÍNDICE

1.	OBJETO.....	3
2.	ALCANCE	3
3.	DEFINICIONES.....	4
4.	CONTENIDO.....	7
4.1.	Introducción	7
4.2.	Principios Generales para la Gestión de los Riesgos	7
4.3.	Órganos Vinculados a la Función de Control y Gestión de Riesgos.....	8
4.3.1.	Primera Línea de Defensa: Áreas Operativas o Corporativas.....	8
4.3.2.	Segunda Línea de Defensa: Control de Riesgos	9
4.3.3.	Tercera Línea de Defensa: Auditoría Interna	10
5.	RESPONSABILIDADES.....	11
6.	ENTRADA EN VIGOR Y VIGENCIA.....	11



1. OBJETO

La Política de Control y Gestión de Riesgos de Enel Colombia S.A. ESP y sus filiales (en adelante “Enel Colombia” o la “Compañía”), es el conjunto de decisiones que toma la empresa para determinar cuál es el marco de actuación aceptable para los niveles de riesgo inherentes a su actividad, dentro del cual debe circunscribirse el desarrollo normal del negocio, y las medidas apropiadas para la adecuada gestión, monitoreo y control de dichos riesgos.

En particular, la Política de Control y Gestión de Riesgos tiene por objeto:

- Establecer el modelo de Enel Colombia para controlar y gestionar los riesgos, definiendo la misión de los órganos vinculados al mismo y las competencias asignadas para todo el conjunto empresarial de la Compañía en materia de riesgos.
- Regular el modelo de control y de gestión de riesgos de Enel Colombia e identificar las principales funciones a desarrollar en cada uno de ellos.

El conjunto de acciones y medidas adoptadas por Enel Colombia en la ejecución de la Política de Control y Gestión de Riesgos (la “Política”) se basa en los lineamientos del Sistema de Control Interno y Gestión de Riesgos del Grupo Enel (“SCIGR”).

2. ALCANCE

Esta Política vincula a todos los ejecutivos y a todo el personal de Enel Colombia, con independencia de la naturaleza de las funciones del respectivo cargo. Los ejecutivos y el personal de Enel Colombia ajustarán sus actuaciones a lo dispuesto en esta Política y promoverán los criterios que se establezcan en ella.

En las empresas en que Enel Colombia ostente directa o indirectamente el 100% de su capital social, esta Política se aplicará directamente como propia de la empresa. Esta Política estará supeditada a la normativa legal vigente, a las normas estatutarias y reglamentarias de las distintas sociedades en que deba ser implementada, así como al respeto a las resoluciones soberanas de los órganos societarios de las empresas.



3. DEFINICIONES

Para efectos de lo dispuesto en la presente Política, los siguientes términos tienen el significado específico que a continuación se indica:

- **Auditoría Interna:** es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización.
- **Control de Riesgos (*Risk Control*):** unidad encargada del monitoreo de los límites o umbrales de riesgos establecidos, de la generación de propuestas de políticas de riesgos, así como de su revisión periódica y evaluación permanente, y de reportar y comunicar al Comité de Auditoría de la Compañía. Informar los resultados de su monitoreo y evaluación al Gerente General de Enel Colombia a fin de que éste adopte las medidas que estime pertinente. La unidad de Control de Riesgos es también la encargada de dar curso o denegar las solicitudes de excepciones en el traspaso de los límites o umbrales de riesgo establecidos (“*waivers*”), las que se tramitarán y gestionarán de conformidad con la presente Política.
- **Gestor de Riesgo (*Risk Owner*):** unidad dentro de la organización responsable de la administración del riesgo en la Compañía. Corresponde habitualmente a las áreas operacionales de la misma, tanto del negocio como corporativas.
- **Mapa de Riesgos:** documento que permite inventariar, homogeneizar y agrupar los principales riesgos que influyen en la consecución de los objetivos económicos, para luego definir acciones de mitigación y seguimiento.
- **Riesgo:** incertidumbre ante eventos futuros que puedan influir negativamente en los resultados financieros de la Compañía, o puedan incidir en las expectativas de su evolución en el tiempo y, por consiguiente, en la consecución de los objetivos fijados por la Compañía. Dichos eventos pueden consistir en la posibilidad de variaciones inesperadas en flujos de caja, en el EBITDA, en los resultados, en partidas del activo/pasivo del balance incluidas las provisiones o en las transacciones previstas; o bien, pueden consistir en eventos, hechos o acciones que produzcan daños graves a la Compañía.
- **Riesgos Estratégicos:** son todos aquellos riesgos que puedan afectar de manera significativa el logro de los objetivos estratégicos de la Compañía, tanto en el corto como en el largo plazo. Estos objetivos han sido definidos por la dirección del Grupo Enel. Los riesgos estratégicos son: Cambios climáticos; Panorama competitivo; Innovación; Desarrollo legislativo y regulatorio; Tendencias macroeconómicas y geopolíticas; Planificación estratégica y asignación de capital.
- **Riesgos Financieros:** se refiere a la probabilidad de ocurrencia de un evento que tenga consecuencias financieras negativas para la Compañía, en relación a: (i) los riesgos propios del mercado financiero, ya sea que se deriven de la variabilidad y volatilidad de las tasas de interés y tasas de cambio; y (ii) a los riesgos derivados de las eventuales restricciones para acceder al mercado financiero por parte de la Compañía o para hacer frente a las obligaciones



asumidas o las necesidades de flujo requeridas en el curso de sus negocios, tales como los riesgos de liquidez y de crédito. Los riesgos financieros son: Adecuación de la estructura de capital y acceso a financiamiento; *Commodity*; Crédito y contraparte; Tipo de cambio; Tasa de interés; y Liquidez.

- **Riesgo Financiero de *Commodities*:** dentro de esta tipología está considerada incertidumbre ante eventos futuros de mercado, generados por la volatilidad de los precios y volúmenes de producción, disponibilidad y demanda de *commodities* de energía, tales como gas, petróleo, carbón, o de la variabilidad en factores externos que pueden incidir en los precios o los volúmenes de tales *commodities*, como la hidrología, considerando las peculiaridades locales y las restricciones propias del mercado de que se trate.
- **Riesgo Financiero de Crédito & Contraparte:** riesgo de pérdida económica por el incumplimiento de pago de los clientes o incumplimiento de alguno de los proveedores de la Compañía.
- **Gobernanza y Cultura:** Riesgo de incurrir en sanciones judiciales o administrativas, pérdidas económicas o financieras y daños a la reputación como resultado de la incapacidad de cumplir con las expectativas de los grupos de interés, un ejercicio ineficaz de las funciones de supervisión y/o la ausencia de integridad y transparencia en los procesos de toma de decisiones y/o consecuencia de actitudes y conductas no autorizadas de los empleados y alta dirección, en violación de los valores éticos de la Compañía. Los riesgos de gobernanza y cultura son: Cultura corporativa y ética; Gobierno corporativo; Reputación; y Compromiso de partes interesadas.
- **Riesgo Operacionales:** son aquellos que representan los riesgos de la operación, resultantes de los procesos internos inadecuados, fallas sistémicas en la red, y otros eventos de causas externas, que puedan afectar la calidad del abastecimiento de energía y los indicadores de performance en los principales aspectos identificados. Los riesgos operacionales son: Protección de activos; Interrupción del negocio; Necesidades y satisfacción de clientes; Medio ambiente; Salud y seguridad; Propiedad intelectual; Personas y organización; Eficiencia de procesos; Compras, logística y cadena de suministro; y Gestión de calidad del servicio.
- **Tecnología Digital:** son riesgos intrínsecamente vulnerables a los ataques cibernéticos, que pueden tomar muchas formas, desde el robo de datos y el *ransomware* hasta la invasión de sistemas con consecuencias potencialmente dañinas a gran escala y hasta mismo interrupciones del servicio. Los riesgos de tecnología digital son: Ciberseguridad; Digitalización; Efectividad de Tecnologías de la Información (TI); y Continuidad del servicio.
- **Riesgos de *Compliance*:** son aquellos que representan los riesgos de incumplimiento de una regla o una norma. Por ello, la gestión de riesgos en *compliance* requiere conocer y definir claramente las leyes y regulaciones por las que está regida la Compañía. Los riesgos de *compliance* son: Cumplimiento contable; Cumplimiento antimonopolio y derechos de los consumidores; Corrupción; Protección de Datos; Divulgación externa; Cumplimiento de regulación financiera; Cumplimiento tributario; y Cumplimiento de otras leyes y regulaciones.





- **Sistema de Control Interno y Gestión de Riesgos (SCIGR):** consiste en un set de reglas, procedimientos y entidades organizacionales enfocadas en permitir que los principales riesgos corporativos dentro del grupo sean identificados, medidos, administrados y monitoreados. El SCIGR es una parte integral de las estructuras corporativas generales adoptadas por la Compañía y está basado en las mejores prácticas locales e internacionales.

4. CONTENIDO

4.1. Introducción

El riesgo es algo inherente a la empresa, forma parte de ella, de su estrategia y de su día a día; y así como es necesario gestionar y conducir la Compañía, también es necesario gestionar el riesgo al que ésta se encuentra sometida en cada momento, controlarlo y mitigarlo.

El control y gestión de los riesgos, forma parte de las estructuras del gobierno corporativo de la Compañía. Para que el control y gestión de los riesgos sea eficaz, el riesgo debe ser considerado como un elemento más de los planes operativos de la Compañía; siendo preciso identificar y analizar qué factores pueden afectar a la consecución de los objetivos empresariales, detectar cuantificadamente sus eventuales consecuencias, así como estimar cuantitativamente su probabilidad de ocurrencia, con el fin de determinar las acciones necesarias para que dichos objetivos puedan ser alcanzados con mayor certidumbre.

4.2. Principios Generales para la Gestión de los Riesgos

El SCIGR de Enel Colombia se fundamenta y recoge los principios elaborados en el documento "*Guidelines of the Enel Group's Internal Control and Risk Management System*" del Grupo Enel.

En particular, la presente Política de Control de Riesgos de Enel Colombia se inspira en los siguientes principios recogidos por las *Guidelines of the Enel Group's Internal Control and Risk Management System*:

- El establecimiento de estrategias globales de riesgo, desarrolladas a nivel táctico y operativo, que servirán para orientar la definición y despliegue de los diferentes niveles y tipos de riesgo dentro de la Compañía, en coherencia con los objetivos de negocio y estratégicos de la misma.
- El establecimiento y la implementación de una adecuada separación de obligaciones y responsabilidades entre las distintas unidades organizacionales, para prevenir incompatibilidad de funciones de tareas y la concentración de funciones en una misma responsabilidad. En especial, la presente Política, contempla una necesaria separación entre las funciones de operación y control de los riesgos inherentes a ella.
- La función de Control de Riesgos será única para Enel Colombia y estará integrada jerárquicamente. Su responsabilidad será verificar el cumplimiento de la Política de Control y Gestión de Riesgos en la que se enmarcan las actuaciones relacionadas con el riesgo.



- La función de Gestión de Riesgos será propia de cada línea de negocio o área corporativa (*Risk Owners*). Su responsabilidad será dirigir la gestión de los riesgos en su ámbito de competencia. Asimismo, se responsabilizará de implementar los controles de riesgos que aseguren el cumplimiento de las directrices y límites definidos por Control de Riesgos.
- Esta Política busca contribuir a que la toma de decisiones sea informada y consistente con la propensión al riesgo de la Compañía. Está desarrollada tomando en consideración las recomendaciones internacionales respecto de los modelos de gobierno de los riesgos, y provee un lenguaje común a toda la organización, facilitando la interpretación y comprensión de los alcances de este marco de actuación.

4.3. Órganos Vinculados a la Función de Control y Gestión de Riesgos

El aseguramiento de la efectividad del SCIGR la entrega el modelo de tres niveles de acción, denominado “Tres Líneas de Defensa”, el cual segrega funciones según los niveles de:

- Primera Línea de Defensa: Unidades de Negocio/Front Office “*Risk Owners*”. Son los responsables de gestionar los riesgos y, por tanto, deben contar con mecanismos de control.
- Segunda Línea de Defensa: Control y Monitoreo de Riesgos “*Risk Control*”. Deben asegurar el cumplimiento de los límites, criterios y principios en los que se enmarcan las actuaciones relacionadas con el ámbito de riesgo.
- Tercera Línea de Defensa: Auditoría Interna provee aseguramiento sobre la efectividad de las medidas dispuestas en la estructura de gobierno corporativo, la gestión de riesgos y el control interno, incluyendo la manera en que la primera y segunda línea de defensa alcanzan sus objetivos de control y gestión de riesgos.

Las dos primeras líneas de defensa y contención reportan a la administración de la Compañía, de acuerdo con su estructura corporativa u organizacional, mientras que la tercera línea de defensa lo hace a la Junta Directiva, de acuerdo con las mejores prácticas internacionales de gobierno corporativo.

4.3.1. Primera Línea de Defensa: Áreas Operativas o Corporativas

Como primera línea de defensa, las Gerencias, Áreas Operativas o Corporativas son las responsables primarias de los riesgos emanados de su quehacer diario y los gestionan en su ámbito de competencia. Las Gerencias, Áreas Operativas o Corporativas también son responsables de la implementación de acciones correctivas para hacer frente a deficiencias de proceso y control.

Las Gerencias, Áreas Operativas o Corporativas son responsables de mantener un control interno efectivo y de ejecutar procedimientos de control sobre los riesgos de manera constante en el día a día. Cada Gerencia, Área Operativa o Corporativa identifica, evalúa, controla y mitiga los riesgos, guiando el desarrollo e implementación de políticas y procedimientos internos que aseguren que las



actividades efectuadas son consistentes con las metas y objetivos propios de cada una.

A través de una estructura de responsabilidad distribuida en cascada, los ejecutivos y los responsables directos de cada Gerencia, Área Operativa o Corporativa diseñan e implementan procedimientos detallados que sirven como controles y supervisan la ejecución de tales procedimientos por parte de sus empleados. Las Gerencias, Áreas Operativas o Corporativas son responsables de implementar adecuados controles de gestión y supervisión para asegurar el cumplimiento de los procedimientos trazados, así como para detectar oportunamente brechas de control, procesos inadecuados y eventos inesperados. Las Gerencias, Áreas Operativas o Corporativas sirven naturalmente como primera línea de defensa ante los riesgos de la Compañía, porque los controles están diseñados y operan insertos dentro de los sistemas y procesos que se encuentran y desarrollan bajo la dirección de cada Gerencia, Área Operativa o Corporativa, como una medida más de administración operacional.

Asimismo, las Gerencias, Áreas Operativas o Corporativas serán responsables de implementar los controles en coherencia con las directrices y límites aprobados por la Junta Directiva de Enel Colombia.

4.3.2. Segunda Línea de Defensa: Control de Riesgos

El control de riesgos es responsabilidad del Área de Control de Riesgos y tiene por objeto definir la estructura y procesos de control de los riesgos de la Compañía.

El Área de Control de Riesgos es responsable de detectar, cuantificar, monitorear y comunicar los riesgos relevantes a los que está expuesta la Compañía al Comité de Auditoría. Para ello, tendrá las siguientes funciones:

- Definir las metodologías y herramientas que permitan identificar, medir y controlar los riesgos.
- Someter anualmente a la aprobación de Gerente General de Enel Colombia los límites y umbrales de Riesgos de *Commodities* y Riesgos Financieros.
- Hacer seguimiento, al menos trimestralmente, de los Riesgos Financieros de *Commodities* y de Crédito y Contraparte, y analizar el cumplimiento de los límites.
- El Área de Control de Riesgos es la encargada de dar curso o denegar las solicitudes de excepciones en el traspaso de los límites de riesgo establecidos (“*waivers*”), cualquier actuación que supere los umbrales de riesgos aprobados, debe contar con la aprobación del Gerente General de Enel Colombia.
- Apoyar a los *Risk Owners* en la definición de los planes de mitigación de los riesgos, como también hacer el seguimiento de estos planes y proponer acciones correctivas en caso de ser necesario.
- Analizar el impacto en los riesgos de las operaciones relevantes.
- Informar, al menos anualmente al Comité de Auditoría el Mapa de Riesgos de Enel Colombia, incluyendo tanto los riesgos directos como aquellos indirectos.



El Mapa de Riesgos incluirá los riesgos financieros, regulatorios, fiscales, legales, operacionales y tecnológicos, así como los de sostenibilidad, económicos, sociales y ambientales.

- Promover y planificar la capacitación permanente del personal atingente de la Compañía, independientemente del vínculo contractual que lo una a ella, respecto de las políticas, procedimientos, controles y reglamentos o cuerpos normativos internos implementados para la gestión de riesgos.
- Verificar que las operaciones se realicen dentro del marco de actuación definido por esta Política.
- Cualquier actuación que pueda suponer niveles de riesgo superiores a los establecidos debe contar con la revisión del Área de Control de Riesgos y la aprobación del Gerente General de Enel Colombia.

Será responsabilidad de las Gerencias o Áreas Operativas o Corporativas entregar oportunamente al Área de Control de Riesgos la información solicitada y necesaria para desarrollar el proceso de detección, cuantificación y monitoreo de los riesgos.

4.3.3. Tercera Línea de Defensa: Auditoría Interna

El Área de Auditoría Interna se encarga de la supervisión general de la estructura y la funcionalidad del SCIGR de la Compañía.

En concreto, el responsable de la función de Auditoría Interna:

- Prepara, al menos anualmente, el plan de auditoría –basado en un proceso estructurado de análisis e identificación de los principales riesgos– el cual debe ser presentado a, y aprobado por la Junta Directiva de la Compañía.
- Monitorea, de acuerdo con las normas internacionales de auditoría interna, el funcionamiento y la eficacia del SCIGR a través del plan de auditoría y la realización de trabajos especiales.
- Realiza controles en funciones u operaciones societarias específicas cuando él lo considere oportuno o a petición de la Junta Directiva.
- Reporta directamente a la Junta Directiva y no es responsable ni dependiente de ningún área operativa.
- Tiene acceso directo a toda la información útil para la realización de sus funciones.
- Prepara informes periódicos que contengan información adecuada sobre sus acciones y los procedimientos para el control y gestión de riesgos, así como el cumplimiento de los planes establecidos. Los informes periódicos contienen una evaluación de la idoneidad del SCIGR.
- Reporta el resultado de la actividad realizada a los órganos corporativos según lo previsto en la normativa local vigente y la normativa extranjera aplicable



(como es el caso de la emanada de la Ley Sarbanes-Oxley, de 2002, y la normativa complementaria de la *Securities and Exchange Commission* y la *New York Stock Exchange* de los Estados Unidos de América).

- Prepara oportunamente informes sobre acontecimientos particularmente significativos.
- Revisa, como parte del plan de auditoría, la fiabilidad de los sistemas de información.
- Monitorea la implementación y la efectividad de los programas de cumplimiento de la Compañía inherentes a los riesgos penales para la persona jurídica, de acuerdo con lo establecido en la normativa aplicable.

5. RESPONSABILIDADES

- Es responsabilidad del Área de Control de Riesgos elaborar las modificaciones de esta Política.
- Es responsabilidad del Área de Auditoría Interna la supervisión general de la estructura y la funcionalidad del SCIGR de la Compañía y asegurar la efectividad de su gobierno corporativo en la gestión de riesgos y el control interno, incluyendo la manera en que la primera y segunda líneas de defensa alcanzan sus objetivos de control y gestión de riesgos.

6. ENTRADA EN VIGOR Y VIGENCIA

La aplicación de la presente Política será a partir del siguiente día hábil después de la fecha de su aprobación por parte del Comité de Auditoría. Su vigencia se mantendrá mientras no sea modificada o derogada por otro acuerdo del Comité de Auditoría.