Global

Multifunctional

Policy

RISK CONTROL AND MANAGEMENT POLICY OF ENEL COLOMBIA

INDEX

1. OBJECT

The Risk Control and Management Policy of Enel Colombia S.A. ESP and its subsidiaries (hereinafter "Enel Colombia" or the "Company"), is the set of decisions taken by the company to determine the acceptable framework of action for the levels of risk inherent to its activity, within which the normal development of the business must be circumscribed, and the appropriate measures for the adequate management, monitoring and control of such risks.

In particular, the Risk Control and Management Policy aims to:

- Establish Enel Colombia's model for controlling and managing risks, defining the mission of the bodies related to the same and the competencies assigned for the entire business group of the Company in terms of risks.
- Regulate Enel Colombia's risk control and management model and identify the main functions to be developed in each of them.

The set of actions and measures adopted by Enel Colombia in the execution of the Risk Control and Management Policy (the "Policy") is based on the guidelines of the Enel Group's Internal Control and Risk Management System ("SCIGR").

2. SCOPE

This Policy binds all executives and all Enel Colombia personnel, regardless of the nature of the functions of the respective position. The executives and personnel of Enel Colombia shall adjust their actions to the provisions of this Policy and shall promote the criteria established in it.

In companies in which Enel Colombia directly or indirectly holds 100% of their share capital, this Policy shall be applied directly as the company's own. This Policy shall be subject to the legal regulations in force, to the bylaws and regulations of the different companies in which it is to be implemented, as well as to the respect for the sovereign resolutions of the corporate bodies of the companies.

3. DEFINITIONS

For purposes of this Policy, the following terms have the specific meanings set forth below:

- **Internal Auditing:** is an independent and objective assurance and consulting activity designed to add value and improve an organization's operations.
- **Risk Control:** unit in charge of monitoring the established risk limits or thresholds, generating risk policy proposals, as well as their periodic review and permanent evaluation, and reporting and communicating to the Company's Audit Committee. Report the results of its monitoring and evaluation to the General Manager of Enel Colombia so that he/she may adopt the measures he/she deems appropriate. The Risk Control unit is also responsible for processing or denying requests for exceptions to the established risk limits or thresholds ("waivers"), which shall be processed and managed in accordance with this Policy.
- **Risk Owner:** unit within the organization responsible for risk management in the Company. It usually corresponds to the operational areas of the same, both business and corporate.
- **Risk Map:** a document that makes it possible to inventory, homogenize and group together the main risks that affect the achievement of economic objectives, to define mitigation and follow-up actions.
- **Risk:** uncertainty about future events that could have a negative impact on the Company's financial results or could affect expectations of their evolution over time and, consequently, on the achievement of the objectives set by the Company. Such events may consist of the possibility of unexpected variations in cash flows, EBITDA, results, asset/liability balance sheet items including provisions or planned transactions; or they may consist of events, facts or actions that cause serious damage to the Company.
- **Strategic Risks:** are all those risks that may significantly affect the achievement of the Company's strategic objectives, both in the short and long term. These objectives have been defined by Enel Group management. The strategic risks are: Climate change; Competitive landscape; Innovation; Legislative and regulatory developments; Macroeconomic and geopolitical trends; Strategic planning and capital allocation.
- **Financial Risks:** refers to the probability of occurrence of an event with negative financial consequences for the Company, in relation to: (i) the risks inherent to the financial market, whether arising from the variability and volatility of interest rates and exchange rates; and (ii) to the risks arising from eventual restrictions to access the financial market by the Company or to meet the obligations assumed or the flow needs required in the course of its business, such as liquidity and credit risks. The financial risks are: Capital structure adequacy and access to financing; Commodity; Credit and counterparty; Exchange rate; Interest rate; and Liquidity.

- **Financial Risk of Commodities:** within this typology is considered uncertainty regarding future market events, generated by the volatility of prices and production volumes, availability and demand of energy commodities, such as gas, oil, carbon, or the variability in external factors that may affect the prices or volumes of such commodities, such as hydrology, considering local peculiarities and the restrictions of the market in question.
- **Credit & Counterparty Financial Risk:** risk of economic loss as a result to non-payment by customers or non-compliance by any of the Company's suppliers.
- **Governance and Culture:** Risk of incurring judicial or administrative sanctions, economic or financial losses and reputational damage because of the inability to meet stakeholder expectations, ineffective exercise of oversight functions and/or the absence of integrity and transparency in decision-making processes and/or because of unauthorized attitudes and behaviors of employees and senior management, in violation of the Company's ethical values. Governance and culture risks are: Corporate culture and ethics; Corporate governance; Reputation; and Stakeholder engagement.
- **Operational Risk:** are those that represent operational risks, resulting from inadequate internal processes, systemic failures in the network, and other events of external causes, which may affect the quality of energy supply and performance indicators in the main aspects identified. The operational risks are: Asset protection; Business interruption; Customer needs and satisfaction; Environment; Health and safety; Intellectual property; People and organization; Process efficiency; Procurement, logistics and supply chain; and Service quality management.
- **Digital Technology:** are inherently vulnerable to cyber-attacks, which can take many forms, from data theft and ransomware to system invasion with potentially damaging large-scale consequences and even service interruptions. Digital technology risks are: Cybersecurity; Digitization; Information Technology (IT) Effectiveness; and Service Continuity.
- **Compliance Risk:** are those that represent the risks of non-compliance with a rule or standard. Therefore, compliance risk management requires knowing and clearly defining the laws and regulations by which the company is governed. The compliance risks are: Accounting Compliance; Antitrust and Consumer Rights Compliance; Corruption; Data Protection; External Disclosure; Financial Regulatory Compliance; Tax Compliance; and Compliance with other laws and regulations.
- **Internal Control and Risk Management System (ICRMS)**: consists of a set of rules, procedures and organizational entities focused on enabling the main corporate risks within the group to be identified, measured, managed and monitored. The SCIGR is an integral part of the overall corporate structures adopted by the Company and is based on local and international best practices.

4. CONTENT

4.1. Introduction

Risk is inherent to the company, it is part of it, of its strategy and of its day-to-day operations; and just as it is necessary to manage and lead the Company, it is also necessary to manage the risk to which it is always subject, to control and mitigate it.

Risk control and management is part of the Company's corporate governance structures. For risk control and management to be effective, risk must be considered as one more element of the Company's operating plans; it is necessary to identify and analyze which factors may affect the achievement of business objectives, quantitatively detect their possible consequences, as well as quantitatively estimate their probability of occurrence, to determine the necessary actions so that these objectives can be achieved with greater certainty.

4.2. General Principles for Risk Management

Enel Colombia's ICRMS is based on and reflects the principles elaborated in the Enel Group's "Guidelines of the Enel Group's Internal Control and Risk Management System" document.

In particular, this Risk Control Policy of Enel Colombia is inspired by the following principles contained in the Guidelines of the Enel Group's Internal Control and Risk Management System:

- The establishment of global risk strategies, developed at a tactical and operational level, which will serve to guide the definition and deployment of the different levels and types of risk within the Company, in coherence with the Company's business and strategic objectives.

- The establishment and implementation of an adequate separation of duties and responsibilities among the different organizational units, to prevent incompatibility of functions and tasks and the concentration of functions in the same responsibility. In particular, this Policy contemplates a necessary separation between the functions of operation and control of the risks inherent to it.

- The Risk Control function will be unique for Enel Colombia and will be hierarchically integrated. Its responsibility will be to verify compliance with the Risk Control and Management Policy in which the actions related to risk are framed.
- The Risk Management function will be specific to each business line or corporate area (Risk Owners). Its responsibility will be to direct the management of risks in its area of competence. It will also be responsible for implementing risk controls to ensure compliance with the guidelines and limits defined by Risk Control.

- This Policy seeks to contribute to informed decision making consistent with the Company's risk propensity. It has been developed taking into consideration international recommendations regarding risk governance models, and provides a common language for the entire organization, facilitating the interpretation and understanding of the scope of this framework.

4.3. Bodies Related to Risk Management and Control Function

Ensuring the effectiveness of the ICRMS is provided by the three-level model of action, called "Three Lines of Defense", which segregates functions according to the levels of:

i. First Line of Defense: Business Units/Front Office "Risk Owners". They are responsible for risk management and, therefore, must have control mechanisms in place.

ii. Second Line of Defense: Risk Control and Monitoring "Risk Control". They must ensure compliance with the limits, criteria and principles in which the actions related to the risk area are framed.

iii. Third Line of Defense: Internal Audit provides assurance on the effectiveness of the measures set forth in the corporate governance structure, risk management and internal control, including the way the first and second line of defense achieve their risk management and control objectives.

The first two lines of defense and containment report to the Company's management, in accordance with its corporate or organizational structure, while the third line of defense reports to the Board of Directors, in accordance with international corporate governance best practices.

4.3.1. First Line of Defense: Operational or Corporate Areas

As the first line of defense, the Management, Operational or Corporate Areas are primarily responsible for the risks arising from their daily activities and manage them within their scope of competence. Management, Operational or Corporate Areas are also responsible for the implementation of corrective actions to address process and control deficiencies.

Management, Operational or Corporate Areas are responsible for maintaining effective internal control and executing risk control procedures on an ongoing day-to-day basis. Each Management, Operating or Corporate Area identifies, evaluates, controls and mitigates risks, guiding the development and implementation of internal policies and procedures to ensure that the activities carried out are consistent with the company's goals and objectives. activities carried out are consistent with the goals and objectives of each.

Through a cascading structure of distributed responsibility, executives and line managers of each Management, Operating or Corporate Area design and implement detailed procedures that serve as controls and supervise the execution of such procedures by their employees. Management, Operating or Corporate Areas are responsible for implementing adequate management and supervisory controls to ensure compliance with the procedures outlined, as well as to detect control gaps, inadequate processes and unexpected events in a timely manner. Management, Operating or Corporate Areas naturally serve as the first line of defense against the

Company's risks, because the controls are designed and operate within the systems and processes that are located and developed under the direction of each Management, Operating or Corporate Area, as a further measure of operational management.

Likewise, the Management, Operational or Corporate Areas will be responsible for implementing the controls in coherence with the guidelines and limits approved by the Board of Directors of Enel Colombia.

4.3.2. Second Line of Defense: Risk Control

Risk control is the responsibility of the Risk Control Area, and its purpose is to define the Company's risk control structure and processes.

The Risk Control Area is responsible for detecting, quantifying, monitoring and communicating the relevant risks to which the Company is exposed to the Audit Committee. To this end, it shall have the following functions:

- Define methodologies and tools to identify, measure and control risks.
- Submit annually to the approval of the General Manager of Enel Colombia the limits and thresholds of Commodity Risks and Financial Risks.
- To monitor, at least quarterly, the Commodities and Credit and Counterparty Financial Risks, and analyze compliance with the limits.
- The Risk Control Area is responsible for granting or denying requests for exceptions to the established risk limits ("waivers"); any action that exceeds the approved risk thresholds must be approved by the General Manager of Enel Colombia.
- Support Risk Owners in defining risk mitigation plans, as well as monitoring these plans and proposing corrective actions if necessary.
- Analyze the impact on the risks of the relevant operations.
- Report, at least annually to the Audit Committee, Enel Colombia's Risk Map, including both direct and indirect risks.

- The Risk Map will include financial, regulatory, fiscal, legal, operational and technological risks, as well as sustainability, economic, social and environmental risks.
- Promote and plan the permanent training of the Company's personnel, regardless of their contractual relationship with the Company, regarding the policies, procedures, controls and regulations or internal normative bodies implemented for risk management.
- Verify that operations are carried out within the framework defined by this Policy.
- Any action that may involve higher risk levels than those established must be reviewed by the Risk Control Area and approved by the General Manager of Enel Colombia.

It will be the responsibility of the Management or Operational or Corporate Areas to timely deliver to the Risk Control Area the information requested and necessary to develop the process of detection, quantification and monitoring of risks.

4.3.3. Third Line of Defense: Internal Auditing

The Internal Audit Area is responsible for the overall supervision of the structure and functionality of the Company's ICRMS.

Specifically, the head of the Internal Audit function:

- Prepares, at least annually, the audit plan - based on a structured process of analysis and identification of the main risks - which must be submitted to and approved by the Company's Board of Directors.
- Monitors, in accordance with international internal auditing standards, the operation and effectiveness of the ICRMS through the audit plan and the performance of special work.
- Performs controls on specific corporate functions or operations when he deems it appropriate or at the request of the Board of Directors.
- He reports directly to the Board of Directors and is not responsible for or dependent on any operational area.
- It has direct access to all the information useful for the performance of its functions.
- Prepares periodic reports containing adequate information on its actions and procedures for risk control and management, as well as compliance with established plans. The periodic reports contain an assessment of the adequacy of the ICRMS.

- It reports the results of the activities carried out to the corporate bodies in accordance with local and foreign regulations (such as the Sarbanes-Oxley Act of 2002 and the complementary regulations of the Securities and Exchange Commission and the New York Stock Exchange of the United States of America). (Such as the Sarbanes-Oxley Act of 2002 and the complementary regulations of the Securities and Exchange Commission and the New York Stock Exchange of the United States of America).

- Prepares timely reports on particularly significant events.

- Reviews, as part of the audit plan, the reliability of information systems.

- Monitors the implementation and effectiveness of the Company's compliance programs inherent to criminal risks for the legal entity, in accordance with the provisions of the applicable regulations.

5. RESPONSABILITIES

- It is the responsibility of the Risk Control Area to prepare modifications to this Policy.
- The Internal Audit Area is responsible for the overall supervision of the structure and functionality of the Company's SCIGR and for ensuring the effectiveness of its corporate governance in risk management and internal control, including the way the first and second lines of defense achieve their risk management and control objectives.

6. ENTRY INTO FORCE AND EFFECT

The application of this Policy shall be effective as of the next business day following the date of its approval by the Audit Committee. It shall remain in effect as long as it is not modified or repealed by another resolution of the Audit Committee.