Corporate Information and Cybersecurity

Policy

GrupoEnergíaBogotá

PURPOSE

This corporate policy provides a framework for acting upon and committing to protecting Grupo Energía Bogotá S.A. E.S.P.'s information, personal data and cyber assets, as well as those of the companies in the business group, in accordance with the regulations of the countries in which they are present, in order to contribute to the development and resilience of the business group.

SCOPE

This Policy applies to Grupo Energía Bogotá S.A. E.S.P., the companies that form part of the business group, and its managers, employees, contractors, and stakeholders who access GEB's information.

STATEMENT OF COMMITMENT

1. To generate a culture that uses information and cyberspace safely in Grupo Energía Bogotá S.A. E.S.P.'s managers, employees and contractors by strengthening their necessary technological competencies, knowledge, skills and capacities.

2. To cooperate with the government bodies and agencies of the countries in which the Company operates, generating adequate communication protocols and channels to contribute to improving cyber and information security with respect to the energy infrastructure.

3. To ensure that the cyber and information security model and policies implemented by subsidiary companies are aligned with Grupo Energía Bogotá S.A. E.S.P.'s strategy.

4. To strengthen the Company's administrative and operational capacity in order to establish efficient and effective models for protecting information and cyber assets that leverage operations and compliance with the strategic objectives.

5. To promote prevention, detection, containment, response, recovery and defense capacity development in terms of information and cybersecurity to ensure information, cyber assets, and the critical infrastructure used in the countries in which it is present is protected.

RESPONSIBLE PARTIES

The following are responsible for the cyber and information security models' proper functioning, as well as compliance with this policy and other documents that develop it: GEB's managers, employees and contractors, as well as other stakeholders that access GEB's information.

GEB's Technology Management will act as an element of the second line of defense of the control architecture through the information security process, and will define and issue guidelines for the first line of defense. It will also rely on the third line of defense to validate the efficacy of the cyber and information security model.

Finally, GEB's Technology Management will be in charge of periodically evaluating this policy in order to establish its pertinence and functionality, making the necessary adjustments in case it is required. To do so, they will consider the regulatory changes that may arise.