

INFORMATION SECURITY POLICY

Proximity, service quality, and results orientation are our hallmarks, which is why, aware of the importance of information security and in line with the path set by our identity, ELECTRANS has promoted the establishment of an Information Security Management System in accordance with ISO 27001 requirements. This aims to identify, evaluate, and minimize the risks to which your information and that of your clients are exposed, and to ensure the achievement of established objectives.

The main goal of this Security Policy is to establish a model of conduct that allows us to develop a company culture, a way of working and making decisions at **ELECTRANS**, and to ensure that information security and respect for personal data are a constant:

- Preserving the **confidentiality** of our clients' information, avoiding disclosure and access by unauthorized persons.
- Maintaining the **integrity** of our clients' information, ensuring its accuracy and preventing deterioration.
- Ensuring the **availability** of our clients' information, in all formats and whenever needed.

The Management, for its part, particularly values and sets as the main criterion for risk estimation the evaluation of the availability and confidentiality of its information, and even more so that of its clients. Thus, it is committed to developing, implementing, maintaining, and continuously improving its Information Security Management System (ISMS) with the goal of continuous improvement in how we provide our services and handle our clients' information. Therefore, it is ELECTRANS' policy that:

- Information Security objectives be set annually.
- Legal, contractual, and business requirements be met.
- Information Security training and awareness activities be conducted for all personnel.
- A process of risk analysis, management, and treatment of information assets be developed.
- Control objectives and corresponding controls to mitigate identified risks be established.
- Employees be held responsible for reporting security breaches and complying with the policies and procedures inherent to the Information Security Management System.

The Security Officer will be directly responsible for maintaining this policy, providing advice and guidance for its implementation, and making corrections in case of deviations in its compliance.

This Information Security Policy will always be aligned with the company's general policies and those that provide the framework for other internal management systems, such as quality and environmental policies.

July 22, 2024

Management