1. OBJECTIVES

- To ensure the **confidentiality, integrity, and availability** of TGI S.A. ESP.'s information assets through the implementation of information security directives, policies, regulations, procedures, controls, and other security guidelines.

- To manage information security risks in order to preserve the confidentiality, integrity, and availability of information assets.

- To create and maintain an information security culture through the communication and awareness of directives, policies, regulations, guidelines, and other applicable security and privacy requirements among all stakeholders of the **Information Security and Privacy Framework (ISPF)**.

- To manage information security incidents accurately, promptly, and effectively by following established procedures, controls, and guidelines, with the objective of reducing their impact on TGI S.A. ESP.'s administrative and operational activities.

- To contribute to the continuity of TGI S.A. ESP.'s services and operations by defining an IT disaster recovery and business continuity management plan.

- To comply with the applicable legal and regulatory framework governing privacy and information security matters relevant to TGI S.A. ESP.

2. SCOPE

TGI S.A. ESP establishes and implements the **Information Security and Privacy Model (ISPM)**, which seeks to protect the **Confidentiality, Integrity, and Availability** of information assets for its Administrative Headquarters located at **Carrera 9 No. 73-44, Bogotá**, as well as all other facilities nationwide.

The model is supported by Senior Management to ensure the resources necessary for its continuous improvement and to enforce compliance with the security directives, policies, and guidelines that are established. These requirements must be known, understood, and accepted by all stakeholders of the Information Security and Privacy Model (ISPM).

3. DEFINITIONS

3.1 ASSET: Anything that has value to an individual, organization, or government.
3.2 INFORMATION ASSET: Knowledge or data that has value to an individual or organization.
3.3 RISK ANALYSIS: Process used to understand the nature of risk and determine its level.
3.4 CONFIDENTIALITY: Property that ensures information is not made available or disclosed to unauthorized individuals, entities, or processes.
3.5 AVAILABILITY: Property of being accessible and usable upon demand by an authorized entity.
3.6 INTEGRITY: Property of safeguarding the accuracy and completeness of information and ensuring that its processing methods remain accurate.
3.7 CLASSIFICATION LEVEL: For each information security property (Confidentiality, Integrity, and Availability), specific criteria and guidelines have been established for the proper handling of assets. The levels and criteria for each property are detailed in the Asset Management Guide.
3.8 PRIVACY: The right of all data subjects regarding information that includes personal data and classified information that they have provided or that is held by the organization in connection with its functions and responsibilities.
3.9 PROCEDURE: A specified way of carrying out an activity or process.

3.10 USER: All employees, contractors, legal interns, trainees, SENA apprentices, regulatory authorities, and any other third parties who have access to or use TGI S.A. ESP's information assets.

3.11 VULNERABILITY: A weakness in an asset or control that can be exploited by one or more threats.

3.12 CYBERSECURITY: The protection of information assets through the management of threats that may compromise information processed, stored, or transmitted by interconnected information systems.

4. DEVELOPMENT OF ACTIVITIES

TGI S.A. ESP establishes and implements the **Information Security and Privacy Model (ISPM)**, aligned with its vision, strategy, values, and Integrated Management System. To this end, the Company defines information security and privacy policies and related guidelines aimed at preserving the **integrity, availability, and confidentiality** of information, in accordance with the provisions established within the Integrated Management System. This system is, in turn, aligned with the Quality Management System and supported by a documented structure designed to meet all applicable requirements and mandatory obligations.

In line with the above, the **Information Security and Privacy Management Model**, which is aligned with the Information Security and Cybersecurity Model of the Grupo Energía Bogotá (GEB), adopts the documentary structure and all guidelines established within the Integrated Management System. This approach strengthens TGI S.A. ESP's processes, optimizes resources, ensures compliance with legal requirements, and fulfills all requirements established under the Quality Management System.

At TGI, efforts are focused on delivering quality service and innovation while motivating and guiding employees toward the efficient achievement of objectives. Through transparent management and the continuous pursuit of excellence, the Company contributes to the development of the industry and the growth of the country.

The **Information Security and Privacy Model (ISPM)** provides cross-functional support to the achievement of the Company's strategic objectives, which are framed within the business pillars and supported by strict compliance with the Codes of Ethics and Good Governance that guide TGI's strategy.

TGI Business Pillars

4.1 STAKEHOLDERS

TGI S.A. E.S.P. creates and provides comprehensive low-emission midstream hydrocarbon industry solutions (natural gas and potentially LPG and/or biogas, and other gases in the future such as hydrogen) to large users, producers, and energy market developers, connecting supply sources with consumption centers through long-term relationships and capital-intensive businesses.

TGI S.A. E.S.P., committed to delivering high-quality services through the implementation of best practices, promotes the development of new and improved information and communication channels with its stakeholders.

The Investor Relations Office of Grupo Energía Bogotá aims to disclose information regarding the commercial, financial, and operational performance of the Group's companies, as well as the economic environment in which they operate, to shareholders, investors, regulators, stock exchanges, and credit rating agencies.

4.2 GENERAL INFORMATION SECURITY AND PRIVACY MODEL (ISPM) POLICY

TGI S.A. E.S.P., seeking to establish a framework of trust for reliable, efficient, and transparent operations, recognizes the importance of establishing, implementing, maintaining, and continuously improving the Information Security and Privacy Model (ISPM) in order to protect its information assets (regardless of the medium in which they are stored), ensuring their availability, confidentiality, and integrity, in compliance with applicable regulations and aligned with the corporate policy, operating model, and pillars of excellence.

4.3 INFORMATION SECURITY ORGANIZATION

Each individual understands their role in fulfilling information security responsibilities, collaborating with other members of TGI S.A. E.S.P. to achieve the objectives of the ISPM while fostering skill development within a continuous learning environment.

Accordingly, it is necessary to define roles and their corresponding responsibilities, which are described in the document **"TGI Information Security Organization"**, in compliance with clause **5.3 Roles, Responsibilities and Authorities in the Organization** and the associated control **"Information Security Roles and Responsibilities"** established in the **ISO/IEC 27001:2013** standard.

4.4 METHODOLOGICAL DESCRIPTION

The following section describes each phase of TGI's Information Security Model:

4.4.1. Phase 1: Planning

During this phase, the context is established and the inventory of assets is identified, classified, and labeled in order to protect them against threats that may affect the confidentiality, integrity, and availability of information.

At this stage, an analysis is conducted of all risks affecting the identified assets. Once the risks have been identified, the corresponding controls must be defined. The output of this phase is a properly structured asset inventory, which should remain subject to continuous updating throughout the entire life cycle of the Information Security Model.

Information Classification: Based on the information security risk context and the information classification and labeling methodology, employees, contractors, legal trainees, interns, SENA apprentices, and regulatory authorities shall consult the asset inventory to verify the classification and labeling of information assets in order to ensure their protection.

Risk Identification, Assessment, and Treatment: The process owner shall update the risk treatment plan and the Statement of Applicability (SoA) to reflect the current status of controls.

As a key aspect of risk management, TGI adopts the cybersecurity risk management best practices proposed by GEB, particularly regarding risks associated with:

- Loss of availability, integrity, or confidentiality of operational assets and cyber assets.
- Loss of confidentiality, integrity, or availability of the Company's information assets and/or cyber assets.

Communication Plan: Information security policies, guidelines, and procedures shall be communicated through various mechanisms to promote an organizational security culture. These mechanisms include the implementation of an information security awareness plan that incorporates training sessions and communication campaigns on information security topics.

4.4.2. Phase 2: Implementation

Once the assets have been identified, the next step is to plan and implement the controls defined in the risk treatment plan in order to mitigate the potential consequences of the threats identified against asset vulnerabilities.

Implementation of the Risk Treatment Plan: Process owners shall periodically implement the controls defined in the risk treatment plan based on the corresponding risk treatment actions.

Management Indicators: Process owners shall periodically implement and evaluate metrics and management indicators related to the implemented controls, the risk treatment plan, and the Statement of Applicability (SoA), in order to reflect the status and effectiveness of the controls.

Communication Plan: Information security policies, guidelines, and procedures shall be communicated through various mechanisms to foster an organizational culture of information security.

As part of the risk treatment plan, a **Disaster Recovery Plan (DRP)** is established, and periodic testing is conducted to ensure the effectiveness of information system recovery in the event of a disaster affecting the technological infrastructure.

TGI also maintains an **Information Security Incident Management** process that defines the actions necessary to ensure the identification, analysis, containment, eradication, and post-incident activities required for the timely response to information security incidents. This process aims to minimize the risk of information theft, loss, or unauthorized disclosure.

4.4.3. Phase 3: Performance Evaluation

Process owners review the assessment of residual risk levels after the implementation of controls and administrative measures.

Process owners monitor the scheduling and execution of internal and external audit activities.
They also measure and evaluate information security management indicators.

Auditing:

Independent planned audits and reviews shall be conducted at scheduled intervals to determine whether the Information Security and Privacy Model (ISPM):

- Complies with TGI's established requirements;
- Has been properly implemented; and
- Is being effectively maintained.

4.4.4. Phase 4: Continuous Improvement

Using the inputs obtained from the previous phases, process owners may make adjustments to deliverables, controls, and procedures.

These inputs will result in an **Improvement Plan** and a **Continuous Improvement Communication Plan**, both reviewed and approved by Senior Management.

The **Management Review** refers to the decisions, changes, priorities, and other actions established through management committees that may impact the Information Security and Privacy Model (ISPM), the Risk Treatment Plan, and the Statement of Applicability (SoA), ensuring that they accurately reflect the status and effectiveness of the implemented controls.

4.4 INFORMATION SECURITY PRINCIPLES

The following information security principles support the Information Security and Privacy Model (ISPM) of TGI S.A. E.S.P.:

- **Availability:** Information assets shall be available whenever required by authorized users.
- **Integrity:** Unauthorized modification of information shall be prevented, ensuring its accuracy, completeness, and reliability.
- **Confidentiality:** Access to information assets shall be restricted exclusively to authorized users.
- **Authentication:** Access to assets, according to their classification level, shall be granted through mechanisms with varying levels of complexity, ensuring that the individual accessing the asset is who they claim to be and is properly authorized.
- **Authorization:** Following successful authentication, the resources that a user may access or use shall be determined based on their identity. Access rights shall be limited to the minimum privileges necessary for the performance of their duties.
- **Information Security Risks:** Continuous identification, assessment, and treatment of information security risks associated with information assets are essential, along with ongoing monitoring to verify the effectiveness and compliance of risk treatment plans.
- **Regulatory Compliance:** TGI S.A. E.S.P. complies with all applicable legal, regulatory, and contractual obligations related to information security and privacy.

- **Responsibility:** All employees and third parties are responsible for complying with their information security responsibilities.
- **Information Protection:** Information generated, processed, or stored through operational processes, technological infrastructure, processing facilities, and other information assets shall be protected against potential risks by applying the necessary controls according to the information classification level.
- **Secure Information Systems:** Security requirements shall be incorporated into all phases of the software development and maintenance lifecycle. These requirements must be validated and fulfilled prior to deployment into production and maintained throughout the system's useful life.
- **Event and Incident Management:** Security events, incidents, and associated weaknesses affecting information assets shall be identified and reported in a timely manner to enable an effective and prompt response, mitigate impacts, and improve the Information Security and Privacy Model (ISPM) through lessons learned.
- **Audit:** Security controls shall be periodically reviewed to verify that the ISPM is properly implemented and effectively maintained.
- **Traceability:** Records and evidence shall be maintained to demonstrate compliance with the ISPM and to identify deviations or non-conformities, enabling the definition and implementation of corrective actions and continuous improvements to the ISPM.

4.5 DOCUMENTED INFORMATION

TGI S.A. E.S.P. documents all information necessary to ensure conformity with the Information Security and Privacy Model (ISPM), taking into account applicable regulatory requirements. In accordance with the documented information requirements established by **ISO/IEC 27001:2013**, the following documents form part of the ISPM:

- Information Security Policy and Regulations.
- Integrated Risk Management System Manual.
- Information Security Risk Management Form.
- Information Asset Classification and Acceptable Use Guide.
- Statement of Applicability (SoA) – ISO 27001 Annex A Controls.
- Information Security Indicators Sheet.
- Information Security Regulatory Matrix.
- Copyright Compliance Verification Procedure.
- Digital Evidence Collection Procedure.
- Remote Connection Management Procedure.
- Secure Information Disposal Procedure.
- Secure Areas Working Procedure.
- Software Installation Procedure for Operating Systems.
- Roles and Privileges Management Procedure.
- Removable Media Management Procedure.
- Information Security Incident Management Procedure.
- User Account Management Procedure.
- Information Security Continuity Procedure.
- Encryption Procedure.
- Internal Audit Execution Procedure.
- Secure Software Development Guideline.
- Contact with Authorities and Stakeholders Procedure.