tower

INTERNAL POLICY

Security Information

POL-02

ISO 27001
Sistema de gestión de seguridad de la información

Prepared by Héctor Oliva López

Approved by Security Committee

Control de versiones

Version	Date	Autor	Cambios
1.0	23/03/2023	Rubén Navío	Revisión Inicial
2.0	21/03/2024	Hector Oliva	Cambio y adaptación de termino

Revisión

Responsable	Última revisión	Siguiente revisión	Comentarios

Control de cambios

Version	Date	Resumen de los cambios producidos
2.0	21/03/2024	Se cambia el etiquetado del documento, pasa a ser Confidencial

Table of contents

Purpose

Tower Consultores depends on ICT (Information and Communication Technologies) systems to achieve its business objectives.

These systems must be managed diligently, acting appropriately to protect them against accidental or deliberate damage that may affect the availability, integrity or confidentiality of the information processed or the services provided.

The information security objective is to ensure the quality of information and the provision of services, acting preventively, monitoring daily activity, and reacting promptly to incidents.

ICT systems must be protected against rapidly evolving threats with the potential to impact the confidentiality, integrity, availability, intended use and value of information and services. To defend against these threats, a strategy that adapts to changing environmental conditions is required to ensure the continued delivery of services. This implies that departments must implement the minimum-security measures required by the National Security Scheme (ENS), as well as continuously monitor service delivery levels, track and analyze reported vulnerabilities, and prepare an effective response to incidents to ensure the continuity of the services provided.

Departments must ensure that ICT security is an integral part of every stage of the system's life cycle, from its conception to its decommissioning, through development or procurement decisions and operational activities.

Security requirements and funding needs must be included in planning and bidding documents for ICT projects.

Departments must be prepared to prevent, detect, react and recover from incidents, in accordance with the ENS.

References and annexes

The implementation of this procedure requires consideration of the following documentation:

- **Information security policy.**
- **Security regulations.**
- **UNE-ISO/IEC 27001**
- **UNE-ISO/IEC 27002**
- **Documents and guides of the National Cryptologic Center (CCN-STIC) referred to ENS.**

Prevention

Departments must avoid, or at least prevent as far as possible, that information or services are impaired by security incidents. Departments must implement the minimum-security measures determined by the ENS, as well as any additional controls identified through a threat and risk assessment.

Security controls, roles and staff responsibilities will be clearly identified and documented.

To ensure compliance with the policy, departments must:

- Authorize systems prior going into operation.
- Regularly assess security, including assessments of configuration changes made on a routine basis.
- Request periodic review by third parties to obtain an independent assessment.

Detection

Since services can degrade rapidly due to incidents, ranging from simple slowdowns to shutdowns, services must continuously monitor the operation to detect anomalies in service delivery levels and act accordingly.

Monitoring is especially relevant when establishing lines of defense. Detection, analysis and reporting mechanisms shall be established to reach the responsible parties on a regular basis and when a significant deviation from the parameters that have been pre-established as normal occurs.

Feedback

Departments should:

- Establish mechanisms to respond effectively to security incidents.
- Designate point of contact for communications regarding incidents detected in other departments or other agencies.
- Establish protocols for the exchange of incident-related information. This includes two-way communications with Emergency Response Teams (CERTs)

Recovery

To ensure the availability of critical services, departments should develop ICT systems continuity plans as part of their overall business continuity plan and recovery activities.

Scope

This policy applies to all Tower Consultores ICT systems and to all members of the organization, with no exceptions.

Purpose

In response to a new technological environment where the convergence between computing and communications are facilitating a new paradigm of productivity for companies, Tower Consultores, is highly committed to maintain the promotion of research projects, technological development and innovation, in a quality environment, where the development of good practices in Information Security is essential to achieve the objectives of confidentiality, integrity, availability and legality of all information managed.

Consequently, Tower Consultores defines the following application principles to consider within the framework of the Information Security Management System (ISMS):

Tower Consultores' Management understands its duty to guarantee information security as an essential element for the correct performance of the organization's services and, therefore, supports the following objectives and principles:

- Implement the value of Information Security throughout the Organization.
- To contribute, every person of Tower Consultores, to the protection of Information Security.
- To preserve the confidentiality, integrity, availability and resilience of the information, with the objective of guaranteeing that the legal and regulatory requirements, and those of our clients, related to the security of the information are fulfilled, and specifically with regard to personal data:

  - Data will be processed in a lawful, fair and transparent manner in relation to the data subject (lawfulness, fairness and transparency).
  - Data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes (Purpose limitation).
  - Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Data minimization).
  - Data shall be accurate and, if necessary, kept up to date; all reasonable steps shall be taken to ensure that personal data which are inaccurate in relation to the purposes for which they are processed are promptly deleted or rectified (Accuracy)
  - Data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be kept for longer periods provided that they are processed

exclusively for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Limitation of the storage period).

– Data will be processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, through the implementation of appropriate technical or organizational measures (Integrity and confidentiality).

- Protect Tower Consultores' information assets from threats, whether internal or external, deliberate or accidental, to ensure the continuity of the service offered to our customers and information security.
- Establish an information security plan that integrates the activities of prevention and minimization of the risk of security incidents based on the risk management criteria established by Tower Consultores.
- To provide the necessary means to be able to conduct the pertinent actions to manage the identified risks.
- Assume responsibility for awareness and training in information security to ensure compliance with this policy.
- Extend our commitment to information security to our employees and suppliers.
- Continually improve security by establishing and regularly monitoring information security objectives.

This Policy shall be updated and adequate for the organization's purposes, aligned with the organization's risk management context. To this end, it shall be reviewed at planned intervals or whenever significant changes occur, to ensure that its suitability, adequacy and effectiveness are maintained.

Regulatory framework

The management of Tower Consultores ensures that the documentation of external origin that is of interest for the operation of the company is known by the employees of the company who need it and is always kept updated and available.

For this purpose, Tower uses the means and procedures defined in this document.

The following international standards are followed to formalize the different security procedures established:

- Information Technology. Security techniques. Information Security Management Systems (ISMS). Requirements. UNE-ISO/IEC 27001
- Information Technology. Security techniques. Code of Good Practices for Information Security Management. UNE-ISO/IEC 27002
- Requirements of interested parties

- In addition, Tower has created the Register of Applicable Regulations to provide all the information, links of interest and information related to the Regulations applied.

Appointments ang organization of managers

Tower Consultores' management is responsible for making appointments to designate roles and responsibilities, as well as the necessary committees, to ensure compliance with this policy.

This documentation will be accessible to all interested parties and internal staff to the organization.

Roles: Functions and responsibilities

The internal document REG-02_Roles and Responsibilities Tower Consultants_v2.0 details all the roles and responsibilities of the organization.

Nomination procedure

Tower Consultores' management will appoint the Information Security Officer upon proposal of the Security Committee. The appointment will be reviewed every 2 years or when the position becomes vacant.

The Department responsible for a service that is provided electronically in accordance with Law 11/2007 shall designate the person responsible for the System, specifying his/her functions and responsibilities within the framework established by this Policy.

Personal data

Tower Consultores processes personal data. The corporate drive (located in the EU), to which only authorized persons will have access, contains the affected files and the corresponding responsible persons.

All Tower Consultores information systems will be adjusted to the security levels required by the regulations for the nature and purpose of the personal data collected in the mentioned Security Document.

Information classification

Tower Consultores has an internal system for classifying information according to its criticality. Sensitive information with a relevant level of criticality is encrypted and treated before being sent or leaving the organization.

This system is described and proceduralized in the internal system of the organization.

Risk management

All systems subject to this Policy shall perform a risk analysis, assessing the threats and risks to which they are exposed. The analysis shall be repeated:

- at least once a year
- if the information managed changes
- if the services provided change
- if a serious security incident occurs
- if severe vulnerabilities are reported

To harmonize risk analyses, the ICT Security Committee will establish a reference assessment for the diverse types of information managed and the different services provided.

The ICT Security Committee will streamline the availability of resources to meet the security needs of the different systems, promoting investments of a horizontal nature.

It may be necessary to increase the measures proposed by the ENS itself due to the protection of personal data.

Information security policy development

This policy will be developed by means of security regulations that will address specific aspects in the operation of the organization's IT users.

The security policy will be available to all members of the organization who need to know it, in particular to those who use, operate or administer the information and communications systems.

The security policy will be available on the web site https://towerconsultores.com, on the data repository "SharePoint" and on the corporate intranet.:

https://towerconsultoressl.sharepoint.com/:w:/r/documentacion/ESQUEMA NACIONAL DE SEGURIDAD/ENS - COMITÉ SEGURIDAD/OFICIALES/POLITICAS/POL_01 Política de seguridad de la información_v1.0.docx?d=w94987b9dfc14439eb23e2ac820ff67b6&csf=1&web=1&e=n96vcv

Staff responsibilities

All members of Tower Consultores have the obligation to know and comply with this Information Security Policy and the Security Regulations, being the responsibility of the ICT Security Committee to provide the necessary means to ensure that the information reaches those affected.

All Tower Consultants members will attend an ICT security awareness session at least once a year.

A continuous awareness program will be established to deal with all members of the organization, particularly new members.

Persons with responsibility for the use, operation or administration of ICT systems shall be trained in the safe operation of the systems to the extent that they need it to perform their work.

Training shall be mandatory before taking on a responsibility, whether it is their first assignment or a change of job or job responsibilities.

External parties

When Tower Consultores provides services to other organizations or manages information from other organizations, they will be informed of this Information Security Policy, channels will be established for reporting and coordination of the respective ICT Security Committees and procedures will be established to react to security incidents.

When Tower Consultores uses third party services or transfers information to third parties, they will be informed of this Security Policy and of the Security Regulations applicable to such services or information.

Such third party shall be subject to the obligations established in such regulations and may develop its own operating procedures to satisfy them.

Specific incident reporting and resolution procedures will be established.

It shall be ensured that third party personnel are adequately security-aware to at least the same level as that set out in this Policy.

Where any aspect of the Policy cannot be satisfied by a third party as required in the preceding paragraphs, a report from the Security Manager will be required, outlining the risks involved and how they will be addressed.

Approval of this report by those responsible for the information and services concerned will be required before proceeding further.

Management signature

Madrid, March 21, 2024