
Technosylva Business Policy

TECHNOSYLVA's priority objective is to achieve and maintain a relevant position in the provision of forestry, wildland fire and environmental consulting services, through the development of software applications and integration of advanced management support techniques (geographic information systems, remote sensing, digital cartography, GNSS).

It is considered, therefore, that the adoption of an Integrated Management System based on continuous improvement is a fundamental element to achieve our objectives.

This policy of the Integrated Management System (IMS) starts from the leadership's concern to guarantee the full satisfaction of the interested parties, as well as the management of the security of their information systems. In addition, our organization feels totally identified with principles oriented to the protection and prevention of the environment and therefore proposes the permanent search for solutions aimed at avoiding or minimizing the environmental impact of its products, activities and services, contributing to a better quality of life of the community.

This commitment is reflected in the following principles:

LEADERSHIP: to become a benchmark for clients that need innovative solutions in the field of Territorial Engineering and the development of services based on geospatial tools.

VOCATION OF SERVICE: maintain and encourage good relations with stakeholders to know and anticipate in the satisfaction of their needs.

INNOVATION: essence of the continuous improvement of our services, driving us in a dynamic and agile way to be able to adapt to the evolution of the needs of our clients and to market changes, guaranteeing quality innovative products.

PERSONAL IMPROVEMENT: we encourage workers and collaborators to optimize their contribution to the organization, and that this provides them with the means to grow as professionals, involving them in the pursuit of excellence and customer service, fostering the training environment and the work environment.

MOTIVATION: we motivate the staff of TECHNOSYLVA to carry out the activities of the innovation tools (monitoring, forecasting, analysis, creativity).

MANAGEMENT IMPROVEMENT: comply with the requirements and continuous improvement of our processes, products and services to increase stakeholder satisfaction, defining individual responsibilities for subsequent measurement and analysis, ensuring, at the same time, that our environmental policy is applied so that the necessary technical and organizational processes are reviewed regularly and continue to be developed and improved.

ENVIRONMENTAL SENSITIVITY: motivating our team and clients to improve their environmental behavior so that they align with our principles of environmental protection, actively cooperating with the competent authorities in the matter, in order to achieve our objectives and goals.

PREVENTION: adopt all measures at our disposal to prevent occupational and environmental risks.

COMPLIANCE OF THE LEGAL FRAMEWORK: ensure compliance with the provisions for the development of our services and the protection of the environment that contemplate environmental impacts, and optimize the consumption of energy and resources.

TRANSFER OF TECHNOLOGY: look for entities of interest to face new R + D + i challenges that allow the development of innovative projects.

EXPANSION: reinvesting the profits obtained to encourage continuous growth and self-financing of the company, ensuring profitability and proper development of the commercial activity and attention to the needs of customers.

RESULTS AND INNOVATION: establish a methodology for the protection and exploitation of results, paying special attention to those successes that are not contemplated in the state of national art.

SECURITY OF INFORMATION: make clear the commitment of management in relation to information security, in line with the business strategy. To do this, we proceed to define, develop and implement the technical and organizational controls that are necessary to ensure the confidentiality, integrity and availability of the information managed by the company. The security of information is understood as a process of continuous improvement, which allows reaching increasingly advanced levels of security.

DATA PROTECTION: ensure compliance with current legislation on the protection of personal data and information society, as well as all applicable legal, regulatory and contractual requirements.

SAFETY CULTURE: create a "safety culture" both internal (in relation to all personnel), and external (in relation to customers and suppliers).

Any violation of this policy or those that develop it, of the rules and procedures, will be considered by the disciplinary procedure, including suppliers and external collaborators that will be processed by its appropriate procedure.

The Management of TECHNOSYLVA undertakes to periodically review this policy, as well as to ensure compliance with the principles established therein by the entire organization. This policy is communicated and made available to all those affected, both internal and external.

Scope

The Integrated Management System of TECHNOSYLVA applies to forestry, wildland fire, and environmental consulting services. These include the development of computer applications and its supporting activities and the supply of solutions based on geotechnologies. In accordance with the Statement of Applicability [dated 07 July 2019](#)

Leadership Commitments

The TECHNOSYLVA leadership is committed to the development and implementation of the Integrated Management System and to the continuous improvement of its effectiveness.

The TECHNOSYLVA leadership is committed to the safety of the company, as well as to his positions, to be part of the Safety Committee, and to be an active part of it.

Leadership:

- Communicates to the organization the importance of satisfying both the client's requirements as well as security, legal, regulatory, and contractual obligations.
- Establishes and communicates the scope of the Integrated Management System (IMS).
- Defines and communicates the Integrated Management System Policy, rules and procedures.
- Communicates the Security Policy and the importance of complying with it to clients and suppliers.
- Ensures the establishment and communication of the objectives of the Integrated Management System.
- Carry out and direct the annual reviews by the Management.
- Ensures that the internal audits of the IMS are carried out annually.

- Ensures that audit results are reviewed to identify opportunities for improvement.
- Ensures the provision and availability of resources.
- Ensures that information security risks are managed and evaluated at planned intervals.
- Defines the approach to take for the management of information security risks and the criteria to assume the risks.
- Approves acceptable levels of risk for the organization.
- Establishes roles and responsibilities in security matters.
- Determines external and internal issues that are relevant to the purpose of the organization and its strategic direction.

The commitment of the Management is reflected in the following policies.

Security policy

The purpose of the Security Policy is to protect the information assets of the TECHNOSYLVA information system, as well as the information assets of our clients with which there is a contractual agreement, before any threat, whether internal or external, deliberate or accidental. It seeks to guarantee the quality of information and the continued provision of services, acting preventively, supervising daily activity to detect any incident and reacting urgently to incidents to recover as soon as possible and minimize the impact.

TECHNOSYLVA has implemented, and continuously improves, an Information Security Management System in accordance with the UNE-ISO / IEC 27001: 2013 standard.

The Security Policy is applicable to all TECHNOSYLVA personnel, including their contractors and the staff hired temporarily; affects any type of information, both that which is owned by TECHNOSYLVA and that which comes from customers, regardless of the media or medium in which it is found, type or category; and applies to any information asset owned by TECHNOSYLVA that affects the system.

Information Security is implicit in each of the points of this Policy, and integrated into business processes as a key tool to achieve the business objectives of TECHNOSYLVA. This policy is fully aligned with the business objectives and integrated into the TECHNOSYLVA'S strategy.

SCOPES

The scopes of the Information Security Management System (ISMS) of TECHNOSYLVA are:

- Maintain an adequate management of the ISMS in accordance with the safety standards and good practices of the sector, carrying out all this in a way that ensures competitive advantages for the organization.
- Protect internal information related to the provision of services, considering the dimensions of:
 - Confidentiality to ensure that information is only accessed by those who have the corresponding authorization. All information will be protected in a way that will not be made available or disclosed to individuals, entities or processes, not previously authorized.
 - Integrity to preserve the veracity and completeness of information and processing methods. All information will be protected so that it can be ensured that it has not been altered in an unauthorized manner. The alteration will be understood in all its contexts, that is, the creation, modification or elimination.
 - Availability to ensure that authorized users have access to the information and processes, systems and networks that support it, when required. The information will be accessible to those users or processes that require it and when they require it. It will be the basic principle of the organization, the restriction of access to the minimum necessary.
- Establish annually specific objectives in relation to Information Security, which guarantee the continuous improvement of the ISMS, being these consistent with the present objectives.

- Develop a risk analysis process and, according to its result, implement the corresponding actions in order to treat the risks that are considered unacceptable, according to the established criteria.
- Establish the necessary means to guarantee the continuity of the organization's business.
- Comply with business requirements, legal obligations and contractual security obligations.
- Ensure that the assets of the organization are only used by authorized users in the exercise of their functions, their defined profiles or according to extraordinary assignments.
- Establish and disseminate the roles and responsibilities related to Information Security.
- Sensitize and conscientiously and permanently raise awareness among all the personnel of the organization regarding the security of information.
- Encourage and maintain the good name of the organization in relation to the services developed, knowledge and active response (reactive and proactive) to security incidents, maintaining the image and reputation.
- Reflect in the Declaration of Applicability of the ISMS the control objectives defined for the ISMS of TECHNOSYLVA, based on the controls included in Annex A of the standard 27001: 2013.
- Sanction any violation of this policy, as well as any policy or procedure of the ISMS.

Applicable legislation and contractual requirements

The following legal obligations applicable to TECHNOSYLVA in relation to information security are identified:

- Copyright:
 - Applicability: Software License.

The following business obligations established by the organization are identified:

ISO / IEC 27001: 2013 - Information Security Management Systems (ISMS).

- Applicability: scope of the ISMS.

UNE EN ISO 9001: 2015 - Quality Management Systems (QMS).

- Applicability: scope of the SGC.

UNE EN ISO 14001: 2015 - Environmental Management Systems (EMS).

- Applicability: scope of the EMS.

In addition, the contractual requirements established in contracts of clients or suppliers that require specific security requirements are considered.

Security structure

Security roles are established, I defend for each, the duties and responsibilities of his position, as well as the procedure for its designation and renewal.

In addition, the structure of the Security Committee for the management and coordination of security is established, detailing its scope of responsibility, the members and the relationship with other elements of TECHNOSYLVA.

The roles and responsibilities in relation to the ISMS are communicated to the new incorporations and periodically reminded to all the personnel of TECHNOSYLVA.

System security documentation

The documentation generated within the ISMS is controlled and approved by the Security Committee.

This documentation is located in a restricted access directory, only making public the documents that are considered to be known by all through the TECHNOSYLVA Intranet.

This Policy is the property of TECHNOSYLVA, S.L. Its total or partial reproduction is limited to express authorization by the Manager of the company. The content of this Policy does not suppose for TECHNOSYLVA, S.L. obligations or rights different from those agreed contractually.

APROBED BY



Joaquín Ramírez Cisneros
CEO

León 7/25/2019