INFORMATION SECURITY POLICY

VILT is a company focused on digital transformation, helping companies around the world to continually improve their customer experience and become more operationally efficient through the adoption of digital solutions, full data integration and advanced analytics. .

VILT, as a provider of professional IT services and consulting for the Administration**,** assumes its commitment to information security, committing itself to an adequate management of it, in order to offer all its stakeholders the best guarantees around the security of the information used. For all the above, the Directorate establishes the following information security objectives:

Provide a framework to increase the capacity for resistance or resilience to provide an effective response.

Ensure the rapid and efficient recovery of services, in the face of any physical disaster or contingency that may occur and that puts the continuity of operations at risk

Prevent information security incidents to the extent that is technically and economically feasible, as well as mitigate the information security risks generated by our activities.

Guarantee the confidentiality, integrity, availability, authenticity and traceability of the information

In order to achieve these objectives it is necessary to:

Continuously improve our information security system

Comply with applicable legal requirements and with any other requirements that we subscribe to in addition to the commitments acquired with the clients, as well as their continuous updating. The legal and regulatory framework in which we develop our activities is:

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016 regarding the protection of natural persons with regard to the processing of personal data and the free circulation of these data
- UNE-EN ISO/IEC 27001:2017
- Organic Law 3/2018, of December 5, Protection of Personal Data and guarantee of digital rights.
- Royal Legislative Decree 1/1996, of April 12, Intellectual Property Law
- Royal Decree-Law 2/2018, of April 13, which modifies the revised text of the Intellectual Property Law
- Royal Decree 3/2010, of January 8, development of the National Security Scheme modified by Royal Decree 951/2015, of October 23.
-

Identify potential threats, as well as the impact on business operations that these threats, if they materialize, may cause.

Preserve the interests of its main stakeholders (customers, shareholders, employees and suppliers), reputation, brand and value creation activities.

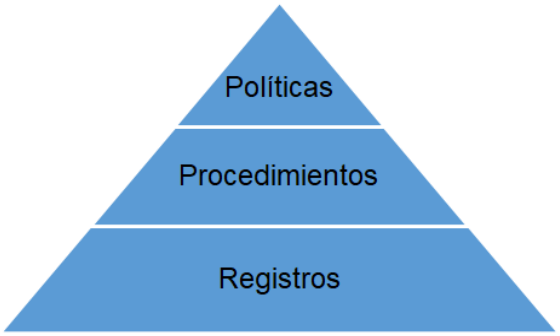
Work together with our suppliers and subcontractors in order to improve the provision of IT services, the continuity of services and information security, which have an impact on a greater efficiency of our activity.

Evaluate and guarantee the **technical competence of the staff**, as well as ensure adequate motivation for them to participate in the continuous improvement of our processes, providing adequate training and internal communication so that they develop good practices defined in the system.

Guarantee the **correct state of the facilities and the equipment** appropriate, in such a way that they are in correspondence with the activity, objectives and goals of the company.

Guarantee a continuous **analysis** of all **relevant processes**, establishing the relevant improvements in each case, based on the results obtained and the established objectives.

Structure our management system in a way that is easy to understand. Our management system has the following structure:



The management of our system is entrusted to the Head of Management and the system will be available in our information system in a repository, which can be accessed according to the access profiles granted according to our current procedure access management.

These principles are assumed by the Management, who has the necessary means and provides its employees with sufficient resources to comply with them, expressing them and making them publicly known through this Integrated Management Systems Policy. The security roles or functions defined in Add4u are:processed

Function	Duties and responsibilities
Responsible for the information	• Make decisions regarding the information
Responsible for the services	• Coordinate the implementation of • the system Continuously improve the system
Responsible for security	• Determine the suitability of technical measures • Provide the best technology for the service
Responsible for the system	• Coordinate the implementation of the system • Improve the system continuously

This definition is completed in the job profiles and in the system documents.

The procedure for their appointment and renewal will be ratification by the security committee.

The committee for the management and coordination of security is the body with the greatest responsibility within the information security management system, so that all the most important decisions related to security are agreed by this committee. The members of the information security committee are:

- Responsible for the information.
- Responsible for the services.
- Responsible for security.
- Responsible for the system.

These members are appointed by the committee, the only body that can appoint, renew and remove them.

The safety committee is an autonomous, executive body with autonomy for decision-making and that does not have to subordinate its activity to any other element of our company.

This policy is complemented by the rest of the policies, procedures and documents in force to develop our management system.

Address

Date: July 01, 2020