VALORIZA

INFORMATION SECURITY MANIFESTO

VALORIZA

INDEX

INFORMATION SECURITY MANIFESTO

The Management of VALORIZA SERVICIOS MEDIOAMBIENTALES, SA, hereinafter, "VALORIZA", within the framework of its general and non-delegable competence to determine the general policies and strategies of the organization, and following the guidelines defined in the Information Security Policy, approves the following information security manifesto.

The objective of this Manifesto is to define and establish the principles, criteria and improvement objectives that govern the actions regarding information security of the VALORIZA systems that are subject to the Information Security Management System (hereinafter, SGSI) and in the scope of the National Security Scheme (ENS).

1 Purpose

Establish the guidelines and principles that will govern the way in which VALORIZA and its group of companies will manage and protect their information and services, complying with the objectives and guidelines of the corporate Information Security Policy, through the implementation, maintenance and improvement of an ISMS and applying the requirements and security measures within the legal and current regulatory framework such as Royal Decree 311/2022, of May 3, which regulates the National Security Scheme, which requires the establishment of the principles and requirements for a security policy in the use of electronic media that allows adequate protection of information.

2 Scope

Taking into account the context in which the internal and external issues of the organization are determined, the interested parties that are relevant and their requirements for information security, as well as the interfaces and dependencies between the activities carried out by the entity and the that are carried out by other organizations in compliance. This manifesto is limited to the VALORIZA services and systems included in the scope of the ISMS that covers compliance with the requirements and security measures established in the National Security Scheme.
These services included within the ENS are the following:

- Application of VALORIZA Parking Meters: System for the monitoring and management of the SER

3 Objectives and mission

Through this Manifesto, VALORIZA assumes and promotes the following general principles that must guide all its activities:

a) Guarantee compliance with the objectives and general principles detailed in the Information Security Policy approved and promoted by the VALORIZA Management
b) Ensure the establishment and compliance of this manifesto and the information security objectives, and that these are compatible with VALORIZA's strategy
c) Ensure the integration and compliance with the applicable ISMS/ENS requirements in the company's services and processes.
d) Ensure that the resources necessary for the ISMS/ENS are available.
e) Communicate the importance of effective security management in accordance with the ISMS/ENS requirements.

f) Ensure that the ISMS/ENS achieves the expected results.
g) Direct and support people to contribute to the effectiveness of the ISMS/ENS.
h) Promote continuous improvement.
i) Ensure continuous surveillance
j) Conducting periodic reassessments
k) Support other relevant Management roles, leading their areas of responsibility in information security.

Information security objectives will be established at the relevant functions and levels, focused on improvement and using as a reference framework:

a) Changes in the needs of interested parties that lead to an improvement in the scope of the system.
b) Applicable information security requirements and the results of the assessment and treatment of risks to guarantee the confidentiality, integrity, availability, traceability and authenticity of the information, as well as the protection of personal data.
c) Internal factors such as the application of organizational techniques that improve the monitoring of the processing and resolution of security incidents.
d) External factors such as technological advances, the application of which improves the effectiveness of risk treatment.
e) Improving the effectiveness of training and awareness of personnel who work in the entity and affects their performance in information security.

Likewise, planning to achieve the established information security objectives will be carried out taking into account what is going to be done, the necessary resources, the person responsible and the achievement period.

4 Legal and regulatory framework in which activities are carried out:

a) Royal Decree 311/2022, of May 3, which regulates the National Security Scheme.
b) Resolution of October 13, 2016, of the Secretary of State for Public Administrations, which approves the Technical Security Instruction in accordance with the National Security Scheme.
c) Resolution of March 27, 2018, of the Secretary of State for Public Function, which approves the Technical Security Instruction for the Security Audit of Information Systems.
d) Resolution of April 13, 2018, of the Secretary of State for Public Function, which approves the Technical Security Instruction for Notification of Security Incidents.
e) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and the free circulation of these data and repealing the Directive 95/46/EC (General Data Protection Regulation).
f) Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.
g) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/ EC.
h) Law 6/2020, of November 11, regulating certain aspects of electronic trust services.

i) Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations
j) Law 40/2015, of October 1, on the Legal Regime of the Public Sector
k) Royal Legislative Decree 1/1996, of April 12, which approves the consolidated text of the Intellectual Property Law, regularizing, clarifying and harmonizing the current legal provisions on the matter
l) The SGSI of Valoriza Servicios Medioambientales SA will continue to comply with and respect the Intellectual Property Law with regard to the use of the software, obtaining the corresponding licenses and keeping a record and control of these for the proper use of these in the development of the activities.

Additionally, VALORIZA has a detailed record of all the legislation that is applicable to the services of the Management System and the ENS.

5 Security organization

The management of each of the companies included within the scope of the ENS has the fundamental responsibility of leading and committing to it.

5.1.- Coordination mechanisms and Committees

The Information Security Committee is designated as the body responsible for the system and has the following functions:

- Ensure that the processes necessary for ISMS and ENS compliance are established, implemented and maintained.
- Ensure that awareness of the requirements of the client and other Interested Parties is promoted at all levels of the organization.

The composition of the Information Security Committee (CSI) and its relationship with other elements of the organization is included in Annex 5 of Information Security of the Management System Manual.

5.2.- Security functions and responsibilities

- **Responsible for information:**
  - Determines the requirements of the information processed
  - You have ultimate responsibility for the use made of the information and, therefore, for its protection. The Information Controller is ultimately responsible for any error or negligence that leads to an incident of confidentiality or integrity (in terms of data protection) and availability (in terms of information security). The ENS assigns to the Information Manager the power to establish the requirements and security levels necessary for security information.
  - The Information Manager approves the System Assessment document
  - The Information Manager approves, as part of the risk analysis, the residual risks
  - You must accept your position profile and functions

- **Responsable of the service:**
  - Determines the requirements of the services provided, including security specifications in the life cycle of services and systems
  - The ENS assigns to the Service Manager the power to establish the service requirements in terms of security. Or, in ENS terminology, the power to determine the security levels of the services, which may be a specific natural person or a collegiate body.
  - The Service Manager also approves the System Assessment document
  - The Service Manager approves, as part of the risk analysis, the residual risks
  - You must accept your position profile and functions
- **System Manager:**
  - Develop, operate and maintain the information system throughout its life cycle, including its specifications, installation and verification of its correct operation.
  - Define the topology and management of the information system, establishing the use criteria and the services available therein.
  - Ensure that security measures are properly integrated into the overall security framework.
  - Proposes the evaluation of the system
  - You must adopt corrective measures derived from the audits (PAC)
  - You must accept your position profile and functions

- **Security Manager:**
  - Determine decisions to satisfy information and service security requirements, supervise the implementation of the necessary measures to ensure that the requirements are met, and report on these matters.
  - Ensure compliance with security policies
  - Manage and develop information security risk analyzes
  - Develop, promote, coordinate and implement the Information Security Policy
  - Prepare and implement procedures and technical instructions regarding information security.
  - Recommend security controls applicable to information systems to reduce risk.
  - Recommend the design, evaluation, selection and implementation activities of Information Security solutions.
  - Promote training and awareness regarding the security of information systems and the communications networks that support them, both in logical, physical and organizational aspects.
  - Investigate information security incidents.
  - Notify the CSI of security incidents that have an impact on the provision of services
  - Direct the Information Security activity, which will have the necessary technical and human means to assume all the functions assigned to it, both organizational and technical. Any other functions that are included in the current legislation on the matter.
  - Proposes the evaluation of the system
  - Determining System Category
  - Approval of the Statement of Applicability (SoA)
  - Approval of Risk Analysis
  - You must accept your position profile and functions

- **POC (Point or Person of Contact)**for the security of the information processed and the service provided, has the support of the management bodies, and channels and supervises both compliance with the security requirements of the service it provides or solution it provides, as well as communications related to the information security and incident management for the scope of said service. The security POC is the organization's own Security Manager and will be part of the ICT Management Area. All this without prejudice to the fact that the ultimate responsibility resides in the public sector entity recipient of the aforementioned services.
    - You must accept your position profile and functions
- **ISMS Manager:**Ensure compliance with security policies
- **System administrator:** Compliance with technical information security procedures
- **Functional application managers:** Registration, cancellation and management of privileges in applications
- **Security Manager for personal data protection:** Ensure compliance with the requirements regarding the protection of personal data

5.3.- Designation of functions

The Management ensures, with the collaboration of the RSGSI, that the staff has the necessary theoretical and practical training in information security for the efficient performance of their functions.

The functions and responsibilities inherent to each job position within the ISMS, as well as the necessary training and experience requirements, are included in the job profiles.

Modifications to security roles and functions will be approved by the management of Valoriza Servicios Medioambientales.

5.4.- Conflict resolution

Conflict resolution will be the responsibility of the Management.

6 Awareness and training

The training plans will include awareness-raising actions aimed at staff so that awareness is raised regarding, among others, the following aspects:

- Information security policy.
- Security of the information.
- Risks, vulnerabilities and threats of information systems.
- Necessity of compliance with current legislation

7 Risk management

All systems subject to this Manifesto must carry out a risk analysis, evaluating the threats and risks to which they are exposed. This analysis will be repeated:

- regularly, at least once a year
- when the information handled changes
- when the services provided change
- when a serious security incident occurs

- when serious vulnerabilities are reported

To harmonize risk analyses, the Information Security Committee will establish a reference assessment for the different types of information handled and the different services provided. The Information Security Committee will boost the availability of resources to meet the security needs of the different systems, promoting horizontal investments.

8 Personal data

The processing of personal data will be based on the "VALORIZA Code of Ethics", which establishes the guidelines that must be followed in the Company to guarantee the privacy of the data of clients, suppliers, employees and, in general. , of all the data groups involved, identifying the most appropriate basis of legitimation for the processing of personal data carried out in accordance with current legislation.

9 Determination of the category and level of security required for the systems

The security category of information systems within the scope of the National Security Scheme will be determined based on the assessment of the impact that an incident that affects the security of information or services with detriment to the security would have. availability, authenticity, integrity, confidentiality or traceability.

The assessment of the consequences of the impact will be carried out taking into account its impact on the organization's ability to achieve its objectives, the protection of its assets, the fulfillment of its service obligations, respect for the law and the rights of the users. citizens.

The power to determine the category of a system corresponds to the person responsible for the service and the person responsible for the information; and will apply to all systems used to provide the services included in the scope of the National Security Scheme.

The systems categorization process will be carried out through the following activities:

- Identification of the level corresponding to each service/information, based on the security dimensions.
- Determination of the category of the system, taking into account that when a system handles different information and provides different services, the level of the system in each dimension will be the highest of those established for each information and services.

The identification of the level corresponding to each service/information in the dimensions availability, authenticity, integrity, confidentiality or traceability will be carried out considering the following criteria defined in the National Security Scheme:

- LOW level (B). It will be used when the consequences of a security incident that affects any of the security dimensions entail limited damage to the functions of the organization, its assets or the affected individuals.
- MEDIUM level (M). It will be used when the consequences of a security incident that affects any of the security dimensions pose serious damage to the organization's functions, its assets or the affected individuals.

- HIGH level (A). It will be used when the consequences of a security incident that affects any of the security dimensions entail very serious damage to the organization's functions, its assets or the affected individuals.

The classification will be made based on the following categories: BASIC (B), MEDIUM (M) and HIGH (A).

- An information system will be of HIGH (A) category if any of its security dimensions reaches the HIGH (A) level.
- An information system will be of MEDIUM (M) category if any of its security dimensions reaches the MEDIUM (M) level, and none reaches a higher level.
- An information system will be of BASIC category (B) if any of its security dimensions reaches the LOW (B) level, and none reaches a higher level.

The classification of the information will be carried out by the person responsible for the information considering what is legally established regarding the nature of the information. Those responsible for the information and each service will be designated by management and will be identified in the "List of Functions vs Responsible Persons" document.

The assessment of the information system and the determination of the system category will be documented in the Declaration of Applicability, with the person responsible for the information and the service being responsible for its documentation and both, together with the Security Manager, for its formal approval. . Furthermore, at any time you will have the exclusive power to modify the required security level, according to the criteria described in this document.

Considering the category of the system and the levels associated with each security dimension, the measures that must be applied to said system will be determined.

10 Documentation.

The documented information associated with the ENS is organized, codified and approved in accordance with the general requirements of the VALORIZA Management System that are included in the document "VALORIZA SERVICIOS ENVIRONMENTALES MANUAL OF THE MANAGEMENT SYSTEM".

All documented information related to the Management Systems, including the treatment of the ENS, is housed in the VALORIZA Information Systems.

11 Establishment, implementation, maintenance and improvement of the ISMS and guidelines for documentation management

Security controls must be implemented, maintained and continually improved, and made available as documented information that must be reviewed and approved by management.

In compliance with article 12 of the Royal Decree of the ENS, this Security Policy will be developed applying the following minimum requirements that are included in the system documentation:

a) Organization and implementation of the security process.

Considering the guidelines developed in the Information Security Policy and the Information Security Manifesto, a set of operational procedures will be developed to guarantee the implementation of said guidelines, and the achievement of the organization's objectives in terms of security of the information.

b) Risk analysis and management.

The risk analysis and management process will be carried out in accordance with the following activities:

- Asset identification.
- Analysis and assessment.
- Risk calculation.
- Determination of acceptable risk.

The development of these activities is included in the risk analysis methodology.

c) Personnel management.

Management will ensure that personnel have the necessary theoretical and practical training in information security for the efficient performance of their duties.

To achieve the information security objectives, all personnel must be involved in the processing and know how they can contribute to its achievement.

These measures are developed in the security procedure related to human resources.

d) Professionalism.

Management must guarantee that personnel have the knowledge and skills necessary for the proper performance of their duties. In addition, it must provide the necessary training when deficiencies are detected in the fulfillment of activities.

e) Authorization and access control.

Information systems must have an access control mechanism that limits their access to users and devices that are duly authorized, restricting access to the functions that are allowed.

The security measures applied are described in the access control procedure.

f) Protection of facilities.

The organization must have a set of physical access controls to the facilities, which allows limiting access only to authorized persons to the storage and/or processing areas of confidential information.

The protection measures are described in the physical and environmental security procedure.

g) Acquisition of security products and contracting of security services.

The acquisition of products and services must consider and guarantee compliance with the security requirements established by the Management, as detailed in the acquisition, development and maintenance procedure.

h) Minimum privilege.

Systems must be configured according to defined security policies and procedures. The operations security procedure develops the security measures that must be applied to information systems in which the principle of least privilege is always considered.

i) System integrity and updating.

Measures must be applied that make it possible to know the security status of the systems, and that allow them to identify and manage their security risks. These measures are developed in the operations security procedure.

j) Protection of information stored and in transit.

Security measures must be applied to guarantee an adequate level of protection of the information stored and in transit. These measures are detailed in the asset management procedure.

k) Prevention against other interconnected information systems.

The risks derived from the connections of information systems with public networks must be analyzed and managed, and the necessary protection measures applied according to the level of security required by the system.

l) Activity log and detection of harmful code.

Information systems must have user activity records that allow the custody of the information necessary to monitor, analyze, investigate and document improper or unauthorized activities. In addition, systems must be available that allow the detection of harmful code.

m) Security incidents.

Information systems must have a system for detecting and reacting to harmful code. In addition, there will be a record of security incidents that will allow tracking their resolution and applying improvements through lessons learned.

n) Continuity of activity.

The necessary mechanisms must be established, to the extent possible and according to the level of associated risk, to guarantee the recovery of information and the continuity of operations.

o) Continuous improvement of the security process.

Management must carry out a periodic review of the system to ensure its suitability, adequacy and continued effectiveness. In the event of any deviation from the expected results, the process of treating it must begin using the established processes.

This Policy will be developed through security regulations and procedures that address specific aspects. The security regulations will be available to all members of the organization within the scope of need to know them, in particular to those who use, operate or manage information and communications systems.

Documented information on security controls must be communicated to the personnel working in the entity (internal and external personnel), who will have the obligation to apply it in the performance of their work activities.

The documented information will be classified into: information for public use, information for internal use and confidential information, giving appropriate use in accordance with said classification and according to the criteria established in the Asset Management Policy.

This Information Security Manifesto has been approved and reviewed, for the last time, by the Chief Executive Officer on November 23, 2023