ENS INFORMATION SECURITY POLICY

REVISION CONTROL

Version	Modified	Reason for Change	Approval Date
1.0	DOCUMENT CREATION	DEFINITION OF THE INFORMATION SECURITY POLICY	20/02/2026

URBAN MANZANA S.L., a company dedicated to the implementation, deployment and management of marketplaces and comprehensive solutions for local commerce, undertakes its commitment to information security, committing to its proper management, in order to offer all its stakeholders the greatest guarantees regarding the security of the information used. Considering the above, Management establishes the following information security objectives:

- Provide a framework to increase resilience capacity to effectively respond to critical security situations.
- Ensure rapid and efficient recovery of services in the event of any physical disaster or contingency that could occur and put 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 information.

To achieve these objectives, it is necessary to:

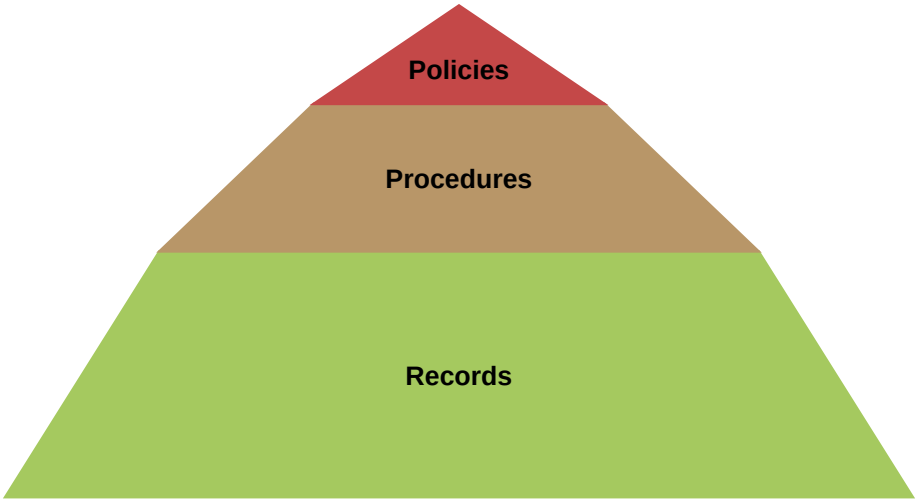
- **Continuously improve** our information security system.
- Comply with applicable legal requirements and any other requirements we subscribe to, in addition to commitments acquired with clients, as well as their continuous updating.

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 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.*
- *Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights.*
- *Royal Legislative Decree 1/1996, of 12 April, Intellectual Property Law.*
- *Royal Decree-Law 2/2018, of 13 April, amending the consolidated text of the Intellectual Property Law.*
- *REGULATION (EU) 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 (European eIDAS Regulation).*
- *Occupational Risk Prevention Law 31/1995 of 8 November and Royal Decree 39/1997 of 17 January, approving the Regulations of the Prevention Services.*
- *Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce (LSSI-CE).*
- *RD-Law 13/2012 of 30 March, Cookies Law.*
- *Royal Legislative Decree 1/1996, of 12 April, approving the consolidated text of the Intellectual Property Law, regularising, clarifying and harmonising the legal provisions in force on the matter.*
- *Resolution of 7 October 2016, of the Secretariat of State for Public Administrations, approving the Technical Security Instruction on the State of Security Report.*
- *Resolution of 13 October 2016, of the Secretariat of State for Public Administrations, approving the Technical Security Instruction on conformity with the National Security Framework.*
- *Resolution of 27 March 2018, of the Secretariat of State for Public Function, approving the Technical Security Instruction on the Auditing of the Security of Information Systems.*
- *Resolution of 13 April 2018, of the Secretariat of State for Public Function, approving the Technical Security Instruction on the Notification of Security Incidents.*
- *Royal Decree 311/2022, of 3 May, regulating the National Security Framework (ENS).*

- Identify potential threats, as well as the impact on business operations that such threats, if they materialise, may cause.
- Preserve the interests of its main stakeholders (clients, shareholders, employees and suppliers), reputation, brand and value-creation activities.
- Work jointly with our suppliers and subcontractors in order to improve the provision of IT services, the continuity of services and information security, which will result in greater efficiency of our activity.
- Evaluate and ensure the technical competence of personnel, as well as ensuring their adequate motivation for their participation in the continuous improvement of our processes, providing the appropriate training and internal communication so that they develop good practices defined in the system.
- Guarantee the correct state of the facilities and adequate equipment, so that they correspond to the activity, objectives and goals of the company.
- Guarantee a continuous analysis of all relevant processes, establishing the pertinent 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 General Director and the system will be available in our information system in a repository, which can be accessed according to the access profiles granted under our access management procedure in force.

These principles are assumed by Management, which provides the necessary means and equips its employees with sufficient resources for their compliance, embodying them and making them publicly known through this Integrated Management Systems Policy.

The security roles or functions defined in ENS are:

Function	Duties and Responsibilities
Information Officer	- Make decisions relating to the information processed
Services Officer	- Coordinate the implementation of the system - Continuously improve the system

Security Officer	- Determine the suitability of technical measures - Provide the best technology for the service
System Officer	- Coordinate the implementation of the system - Continuously improve the system
Company Management	- Provide the necessary resources for the system - Lead the system

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

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

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

The members of the information security committee are:

- Information Officer.
- Services Officer.
- Security Officer.
- System Officer.
- Data Protection Officer.
- Company Management.

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

The security committee is an autonomous, executive body with autonomy for decision-making and 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.

AT VILLANUEVA DEL PARDILLO, 20 FEBRUARY 2026

LUIS MARIO GONZÁLEZ DE LA VEGA

CHIEF EXECUTIVE OFFICER

URBAN MANZANA S.L.