

The OHLA Group, within the framework of its general policies and strategies of the organization, has approved this **Information Security Policy**.

This Policy, of a global nature, is aimed at all the stakeholders of the OHLA Group as a reference in terms of information security.

### Objective

The objective of this Policy is to define and establish the principles, criteria and objectives of information security for all business processes and systems of the organization, providing the necessary framework for the establishment, monitoring and review of information security objectives aligned with the strategy and context of the OHLA Group.

### Scope of Application

This Policy applies to all companies, organizational units, processes and systems of the OHLA Group, as well as to companies whose information systems are under OHLA's responsibility.

It is mandatory for all employees, managers and collaborators of the OHLA Group, as well as for third parties who, within the framework of their contractual or professional relationship, access, process or support information of the organization.

The OHLA Group considers information security as a fundamental element of its strategy, ensuring the protection of information in terms of confidentiality, integrity, availability, authenticity and traceability, as well as the privacy of personal data.

The General Management of the OHLA Group undertakes to provide human and economic resources to achieve this and to carry out periodic annual reviews so that information security is included in the organization's continuous improvement processes.

The OHLA Group's Global CISO (Chief Information Security Officer), as the person responsible for the Information Security strategy, will ensure its alignment with the corporate vision and mission, actively promoting its dissemination and ensuring compliance with this Policy.

### Reference Framework and Management System

The OHLA Group develops and maintains an Information Security Management System aimed at protecting the information of the systems that support it, the prevention, detection, response and recovery from security incidents and the continuous improvement of security processes, controls and measures.

This system is aligned with the NIST CSF, ISO/IEC 27001 standard and with the National Security Scheme (Royal Decree 311/2022); as well as the legislation and regulations applicable in each area of action.

This Policy is complemented by an Information Security Regulatory Framework, through which its application in the different areas of the organization is specified.

### General Principles

The OHLA Group promotes the following principles as a basis for the protection of information and the development of its business activities:

1. Guarantee confidentiality, integrity, availability, authenticity and traceability of information, as well as the protection of personal data against improper access, cyberattacks and unauthorized modifications.
2. Ensure compliance with customer requirements and the regulatory frameworks of the countries where

OHLA operates, emphasizing those established in terms of information security.

3. Encourage employee participation in achieving the objectives established by the organization to ensure security, through the appropriate definition of roles and lines of defense for information security management.
4. Integrate security into the design of processes, systems and services, considering security criteria throughout the information life cycle and in change management.
5. To promote continuous training and awareness of employees in information security.
6. Guarantee business continuity, in terms of information security, protecting critical processes against failures or disasters that cause a significant impact on the organization's operations.
7. Identify, assess, manage, and address information security risks by prioritizing the implementation of controls based on their impact and likelihood.
8. Prevent, detect, manage and respond in a coordinated way to security incidents.
9. Periodically evaluate the effectiveness of the information security controls implemented to adapt the organization to the evolution of risks, business operations and technological environments.
10. Establish mechanisms for control, supervision, monitoring and prevention of security incidents in information systems, evaluating the effectiveness of the measures and controls applied for their adjustment in the processes of managing cyber incidents.
11. Establish the procedures and implement the tools that allow the organization to adapt with agility and security to the changing conditions of the business.
12. Periodically review and update the Information Security Management System, adopting the necessary measures to correct deviations and improve its effectiveness.

This Information Security Policy has been approved by the OHLA Group Management Committee on 21 July 2026.

**Tomás José Ruiz González**  
CEO of the OHLA Group