Within the framework of its non-delegable competence, OHLA Group's Corporate Resources Management has approved this **Information Security Policy** that sets out the general policies of the management system in the areas of the organization, human resources, general services, transformation, innovation, and information systems of the Group.

This Policy aims to define and establish information security principles, criteria, and objectives for all of the organization's business processes and systems.

OHLA is responsible for the security of the information associated with its services as part of its strategy and as a determining factor in the performance of its activities to ensure the confidentiality, integrity, availability of information, and privacy of personal data, protecting data and information systems against unauthorized access, unauthorized modifications, and loss of connectivity.

OHLA's strategy includes developing and optimizing an Information Security Management System to identify, detect, and respond to threats, incidents, and vulnerabilities that put data at risk and protect and recover information systems. To this end, OHLA Group's Corporate Resources Department is committed to providing the human and financial resources to achieve this goal and to carry out regular annual reviews to ensure that information security is included in the organization's continuous improvement processes.

By employing this Policy, OHLA promotes the following general principles, which serve as a guide for the definition and execution of business activities:

1. Guaranteeing the confidentiality, integrity, availability of information, and privacy of personal data, protecting data and systems against improper access, cyber-attacks, and unauthorized modifications.
2. Ensuring that the organization complies with client requirements and the regulatory frameworks of the countries where OHLA operates, emphasizing the conditions set out in information security.
3. Encouraging the participation of employees to achieve the goals established by the organization to ensure safety, which will benefit the safety of customers and stakeholders.
4. Focusing efforts on error prevention from the design phases of processes and activities, and on the management and correction of possible incidents.
5. Promoting continuous training and awareness among information security employees.
6. Establishing the procedures and implementing the tools that allow the organization to adapt with agility and security to the business's changing conditions.
7. Ensuring business continuity, in terms of information security, protecting critical processes against failures or disasters that cause a significant impact on the organization's operations.
8. Performing an adequate assessment, management, and treatment of information security risks to achieve a high level of maturity that allows minimizing those risks, prioritizing the measures and controls to be implemented according to the identified risks and business goals.
9. Acting in an appropriate and coordinated manner to prevent, detect, and respond to cyber incidents that could affect the security of information systems and business processes.
10. Improving the efficiency of the information security controls implemented to adapt the organization to the evolution of risks, business operations, and technological environments.
11. Establishing regular actions to control, monitor, and prevent security incidents in information systems.

12. Regularly reviewing and updating the Information Security Management System, taking the appropriate measures to correct any possible deviations.

Tomás José Ruiz González
General Manager of OHLA Group