INFORMATION SECURITY POLICY

OPENSISTEMAS is an internationally oriented company specializing in providing support, services, and solutions based on open-source technologies. Its service provision in the field of open-source information technology is specialized in technological consultancy, solution development and integration, and support services. These services are offered in three lines of business: Solutions, Managed Services, and Support. OPENSISTEMAS acknowledges that Information Security is indispensable for the competitiveness and survival of the company. Therefore, it has implemented an Information Security System based on the ISO 27001:2017 standard.

This Policy is established as the framework within which all company activities must be conducted. Its scope covers **"Information systems that support services related to the development, support, and maintenance of open-source software products and those based on intensive data usage, as well as support services applicable to platforms, infrastructures, and hours banks for corrective or evolutionary interventions provided by the support area to end customers, in accordance with the current applicability statement."** This ensures the commitment made to customers and other stakeholders.

For the annual setting of objectives, OPENSISTEMAS takes into account the following pillars:

- Protection of personal data and individuals' privacy.
- Protection of the organisation's records.
- Compliance with legislative and contractual requirements applicable to the company's security activities.
- Mandatory training on information security as defined in the human resources security policy.
- Compliance with security policies' controls and measures, with potential application of the disciplinary process defined in the Workers' Statute, Chapter IV (Offenses and sanctions of workers), in case of intentional security breaches.

- Reporting of detected security incidents based on established policies.
- Ensuring availability, confidentiality, integrity, traceability, and authenticity of information.
- Establishing a continuous improvement approach.

To achieve compliance with the above principles, it is necessary to implement a set of security measures that ensure the effectiveness of the efforts made. All measures adopted have been established following a thorough risk analysis of OPENSISTEMAS' information assets, with special attention to compliance with legal aspects related to data processing. The requirements of the current Spanish Data Protection Act and the General Data Protection Regulation (GDPR) will be considered in all aspects involving our business activities.

All members of the organization must comply with and ensure compliance with what is established in OPENSISTEMAS' ISMS. To ensure compliance with what is established by the ISMS, the Management delegates the responsibility for supervision, verification, and monitoring of the system to the Security Coordinator and the Security Officer, who have the necessary authority and independence and will have the appropriate resources to ensure the correct operation of the ISMS.

Finally, the Management commits to providing the necessary means and adopting appropriate improvements throughout the Organization to promote the prevention of risks and damages to assets, thus improving the efficiency and effectiveness of the ISMS.

Madrid, November 17, 2023

Luis Alberto Flores Porras