INFORMATION SECURITY POLICY

OPENSISTEMAS is a company with an international scope specialised in providing support, services and solutions based on open source technologies. Its activity of providing services related to information technologies in open source environments is specialised in technological consultancy, development and integration of solutions and support, services that it offers in three business lines: Solutions line, Managed Services line and Support line. OPENSISTEMAS is aware that Information Security is essential for the competitiveness of the company and, therefore, for its survival, so 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.

In order to achieve compliance with the above principles, it is necessary to implement a set of security measures that guarantee the effectiveness of the efforts made. All the measures adopted have been established after the appropriate risk analysis of the information assets of OPENSISTEMAS, taking special care to comply with the legal aspects associated with the processing of personal data. The requirements of the Spanish Data Protection Act in force and the General Data Protection Regulation (GDPR), as well as other regulations in force and applicable in the countries where OPENSISTEMAS is present, will be taken into account in all aspects involving the activities of our business.

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, April 29, 2024

Luis Alberto Flores Porras