
ALIANDO

Information Security Policy

Version 1.0. | 12 / 02 / 2024

Document Sheet

File Name	Information Security Policy
Typology	Policy
Scope of Dissemination	All employees and external collaborators of ALIANDO
Responsible	Responsible for the Integrated Management System
Sensitivity level	Internal

Version Control

Version	Go to	Review	Approves	Date	Description
1.0	Management System Operating Committee	Management System Operating Committee	Jorge Flores Catalina Jiménez	12/02/2024	Initial Version of the document

Content

Introduction

In an environment that is increasingly interconnected and digitalized, where information has become one of the most valuable assets for our organization, the importance and reliance on ICT (Information and Communication Technologies) systems are growing ever more significant. For this reason, it is increasingly essential to ensure these systems are managed with due diligence, adopting a security strategy aligned with the culture and business requirements. This approach enables us to have the necessary capacity to detect, react to, and recover effectively from threats that may affect the availability, integrity, or confidentiality, as well as the authenticity and traceability of the information processed and the services we provide.

Therefore, at ALIANDO Solutions, S.L. and ALIANDO Security & Innovation S.L. (hereafter referred to as ALIANDO), we consider information security to be one of the main pillars in the development of our activities. Consequently, we allocate the necessary resources and means to implement security measures in compliance with applicable requirements and manage the risks to which the organization is exposed.

Scope

This policy applies to all ICT systems within the organization and to all personnel, both internal and external collaborators, who support the processing of information for which we are responsible and the provision of the services we offer.

Objectives

Our mission is to deliver solutions that best meet our clients' needs by integrating information technology, industrial management, and business management. To achieve this, we aim to be a technological reference that generates long-term trust, led by committed individuals proud to be part of ALIANDO.

With this goal in mind, and aware of the need to provide guarantees for the effective protection of corporate resources and the continuity and proper functioning of our services, we have established the following objectives:

- Establish and maintain an efficient and effective Information Security Management System, aligned with current legislation and international security standards.
- Minimize the risks to which the organization and its information assets are exposed to acceptable risk levels.

- Comply, and ensure compliance in third-party relations, with security requirements and obligations as per the established legal, regulatory, and contractual framework.
- Promote security through training and awareness processes, ensuring that organization employees possess the necessary competencies.
- Ensure the protection of information and the continuity of the organization's critical processes in providing services to our clients.

To achieve these objectives, we establish action and monitoring plans that are periodically evaluated.

Principles

The regulatory development of this policy and decision-making within the management system are based on the following set of basic principles:

- Security as an integral process, constituted by all human, material, technical, legal, and organizational elements related to the information system.
- Risk-based security management, thereby maintaining a controlled environment, minimizing risks to acceptable levels through the proper application of security measures.
- Prevention, detection, response, and preservation, to minimize vulnerabilities and prevent threats from materializing or, if they do, not severely affecting the information handled or the services provided.
- Lines of defense, constituted by organizational, physical, and logical measures, as a layered protection strategy.
- Continuous vigilance for detecting anomalous activities or behaviors and responding promptly.
- Periodic reevaluation of the security status of assets, measuring the evolution of risks, detecting vulnerabilities, and identifying deficiencies and improvement opportunities.
- Security as a distinct function, separating the responsibilities for defining requirements, overseeing security, and operating systems.

Regulatory Framework

At ALIANDO, we comply with all legal, regulatory, and contractual requirements applicable to us, both in terms of information security and privacy. Similarly, we commit to complying with the measures determined in the reference frameworks and international standards we implement, highlighting, among others, the following certifiable references:

- Royal Decree 311/2022, of May 3, regulating the National Security Framework for HIGH level information systems.
- ISO/IEC 27001:2022 Information security management systems.
- ISO/IEC 27701:2019 Privacy Information Management Systems.

For this purpose, at ALIANDO, we develop this policy through a set of documented processes that make up our management system's regulatory body.

This regulation is available to all ALIANDO staff and third parties who need to know it, particularly those who use, operate, or manage information systems.

Security Organization

To facilitate the management and maintenance of the Management System, at ALIANDO, we have determined a defined, approved, and functional structure of roles and responsibilities for the implementation, operation, and management of information security and privacy within the organization, adhering to the principle of security as a distinct function.

Additionally, the attention, supervision, and audit of system security throughout their lifecycle are carried out by duly qualified and trained personnel.

Risk Management

Risk management at ALIANDO is a fundamental process that is conducted across all our information systems, through which we identify, evaluate, and control risks that could affect our service delivery performance, information protection—including those that could impact personal data—or the ability to achieve our goals.

This process is carried out recurrently and continuously, always kept up to date to adapt to new challenges and threats due to constant changes in our environment. However, at a minimum, this evaluation is repeated:

- Regularly, at least once a year.
- When there is a significant change in information systems.
- When a serious security incident occurs.
- When serious vulnerabilities are reported.

Furthermore, to obtain objective, comparable, and reproducible results, aligned with the requirements for our service provision, ALIANDO has and applies a recognized, documented, and formally approved risk analysis and management methodology.

Staff Obligations

All ALIANDO personnel are obligated to know and comply with this Information Security. Policy and the relevant security regulatory framework, as applicable, which develops the measures and protocols to follow for information protection.

Similarly, staff are obligated to train in functions related to the performance of their competencies with professionalism and ethics, especially regarding the use, operation, or administration of ICT systems, and to attend information security and privacy awareness sessions or activities.

The ALIANDO Management provides the necessary means and resources for training and awareness initiatives to be effectively carried out. In this sense, ALIANDO has a continuous training and awareness plan, which is periodically reviewed to meet the needs of all employees according to their roles and responsibilities.

Third Parties

In cases where ALIANDO provides services or handles information from third parties, they are made participants in this Information Security Policy and regulations as required.

To quickly and effectively respond to security incidents that may affect third-party services, we establish reporting channels and coordination, and action protocols.

ALIANDO does not transfer information to third parties, except with prior authorization from those concerned, and provided these third parties offer sufficient guarantees of compliance with the appropriate technical and organizational measures, so that the processing is in accordance with the requirements set out in its Information Security Policy, and with prior authorization from those concerned.

In cases where third-party services are used or information is transferred to third parties, under the aforementioned conditions, we also transmit the applicable security requirements and pursue their compliance. Additionally, when third-party personnel are involved in the operation or administration of our systems, we ensure they are adequately trained and aware of security matters. Appropriate measures will be taken in case of non-compliance with these requirements by a third party.

Approval

This policy has been approved by the Management of ALIANDO Solutions, S.L., and my- CloudDoor Security & Innovation S.L., effective from the date of its approval until it is replaced by the approval of a new version of the same.

Furthermore, in accordance with the continuous improvement process, this policy is regularly reviewed by the Management to assess the timeliness, suitability, completeness, and accuracy of its content, with the aim of adapting it to the circumstances of our environment.

Through this policy, the Management of ALIANDO wishes to record its commitment to complying with the applicable requirements in terms of information security and the conti- nuous improvement of the processes that make up the management system, developing gui- delines for the management and protection of the information handled by ALIANDO and the services it provides.

ALIANDO

Thank You