



Information Security Policy

The Management of GRUPO INDEA establishes this Information Security Policy as a reference framework to protect information and the systems that manage it, ensuring its appropriate and secure use in the performance of all the organization's activities.

This policy applies to all persons, both internal and subcontracted, as well as to third parties that have access to GRUPO INDEA information, systems or facilities.

Information Security Principles

Information security at GRUPO INDEA is based on the following principles:

- **Confidentiality**
Ensure that information is accessible only by duly authorized persons.
- **Integrity**
Ensure that information and systems remain complete, accurate and protected against unauthorized modifications.
- **Availability**
Ensure that information and services are available when necessary for the proper functioning of business processes.
- **Regulatory and Contractual Compliance**
Comply with the applicable legal, regulatory, contractual and customer requirements regarding information security.
- **Risk Management**
Identify, assess and treat risks that may affect information security.
- **Continuous Improvement**
Continuously improve the effectiveness of information security through the periodic review of risks, controls, incidents and associated processes.

Information Security Approach

Information security at GRUPO INDEA is managed through a risk-based approach, integrated into the organization's processes and aligned with business objectives.

Date: 30/04/2026

Approved by: Mario Sanchez

Manager Name
Manager - INDEA Palencia

Classification: Public

Information Security Policy

Security measures are defined and applied proportionately, depending on the criticality of the information, the identified risks and the applicable customer, legal and regulatory requirements.

This approach makes it possible to prioritize security efforts, optimize available resources and ensure an adequate and sustainable level of protection over time.

Management Commitments

The Management of GRUPO INDEA undertakes to:

- Provide the resources necessary for the implementation, maintenance and improvement of information security.
- Integrate information security into business processes and decisions.
- Promote a culture of security and awareness among all persons in the organization.
- Require compliance with this policy and with the rules, procedures and controls that develop it.

Information Security Objectives

GRUPO INDEA establishes the following information security objectives aligned with business objectives, customer requirements and identified risks:

- Ensure the confidentiality of information
Protect information against unauthorized access, disclosure or use, especially sensitive, industrial, strategic and third-party information.
- Preserve the integrity of information
Ensure that information is accurate, complete and protected against unauthorized or accidental modifications.

Date: 30/04/2026

Approved by: Mario Sanchez

Manager Name
Manager - INDEA Palencia

Classification: Public

Information Security Policy

- Ensure the availability of information and services
Ensure that information and critical systems are available when necessary for plant and business operations.
- Protect information throughout its entire life cycle
Apply security measures from the creation, processing and storage of information through to its transmission and destruction.
- Comply with legal, regulatory and contractual requirements
Ensure compliance with the applicable obligations regarding information security, data protection, customers and industrial partners.
- Reduce information security risks to acceptable levels
Identify, assess and treat risks that may affect information and business processes.
- Protect intellectual property and industrial know-how
Safeguard designs, production processes, technical documentation and any information asset critical to the company's competitiveness.
- Control the use of external technologies and cloud services
Ensure that the use of cloud services and artificial intelligence is carried out securely and in accordance with corporate policies.
- Raise awareness and assign responsibility to personnel
Ensure that employees and third parties understand their responsibilities regarding information security and act securely.
- Detect, manage and respond to security incidents
Establish capabilities to identify, report, analyze and respond effectively to information security incidents.
- Ensure traceability and accountability
Maintain records and evidence that allow the use of information to be audited and demonstrate compliance with security requirements.
- Promote continuous improvement of the information security management system
Continuously review and improve security controls, processes and policies.

These objectives are periodically reviewed by Management.

Responsibilities

All persons who work at GRUPO INDEA, as well as those who act on its behalf, are responsible for knowing and complying with this policy and the information security rules that develop it.

Information security measures shall be applied based on identified risks, whether or not they are formally documented.

Failure to comply with this policy may result in disciplinary measures, without prejudice to any civil or criminal liability that may arise.

Development and Review of the Policy

Date: 30/04/2026

Approved by: Mario Sanchez

Manager Name
Manager - INDEA Palencia

Classification: Public

Information Security Policy

This policy is developed through information security rules, procedures and controls integrated into the organization's management system.

The policy shall be reviewed periodically or whenever relevant changes occur in the organization, in the identified risks, in applicable legislation or in customer requirements.

Date: 30/04/2026

Approved by: Mario Sanchez

Manager Name

Manager - INDEA Palencia

Classification: Public