Cybersecurity & Privacy policy

Rev.0
April 2024

This policy defines the necessary guidelines to implement, operate, maintain and continuously improve the Information Security and Cybersecurity Management System, adjusted to the needs of the business, and the regulatory requirements that apply to its nature.

These guidelines include the adoption of a series of organizational measures whose purpose is to protect the information resources of our organization and the computer systems used for their processing against threats, internal or external, deliberate or accidental, in order to ensure all dimensions of information security. To this end, our organization:

- Guarantees compliance with established legal, regulatory and contractual obligations.
- Verifies that the responsibilities regarding Information Security and Cybersecurity are defined, shared, published and accepted by each of the Collaborators (employees and contractors) or third parties.
- Protects the information created, processed, transmitted or safeguarded by its business processes, in order to minimize financial, operational or legal impacts due to its incorrect use. To this end, it is essential to apply controls according to the classification of the information owned or in custody.
- Protects our information from threats from collaborators (employees and contractors) and third parties.
- Controls the operation of its business processes guaranteeing the security of technological resources and data networks.
- Implements access control to information, systems, and network resources.
- Ensures that security is an integral part of the information systems lifecycle.
- Guarantees adequate management of security and cybersecurity events and weaknesses associated with information systems, to improve the effectiveness of the security and cybersecurity model.
- Guarantees the availability of our business processes and the continuity of our operation based on the impact that events can generate.