Digital security

A new three-year master plan

Information security is a great priority at Bankinter. In 2021, in order to fulfil this commitment, the projects agreed within the Security Master Plan were performed. The objective is to guarantee high levels of confidentiality, integrity and availability for customers, employees, shareholders and suppliers. In addition, during the financial year Bankinter decided to rename the Information Security area Digital Security and drew up a new Master Plan, which sets out the entity's information security strategy and objectives for the next three years.

The model for the fight against cybercriminals is based around three lines of defence: the first line is technology, business, operations, etc.; the second line comprises risk control and regulatory compliance bodies; and the third line is the Internal Audit department.

From an organisational viewpoint, a new model was implemented in the first line in 2018 within the Data Security Department consisting of three management areas: technological risk, cybersecurity and security monitoring, and prevention of electronic fraud. In 2021, a new department was created to enhance continuity and response to incidents.

Based on this new reinforced structure, Bankinter has undertaken a set of projects with a higher level of maturity where the main focus has been on the vectors of greatest threat. Not only is it necessary to protect the entity's assets; it is also necessary to ensure security within the supply chain to guarantee the proper functioning of business processes.

Awareness

The activity of the area is completed by the development of awareness plans for users, who are the weakest link in the security chain. The Bank provides online training programmes for employees and carries out simulations to obtain confidential information (passwords, personal details, etc.) through emails, text messages (smishing) or telephone calls. (vishing), etc. The aim is to discover their reaction in situations that can be exploited by cybercriminals. The awareness-raising exercise includes external staff.

The growing importance of information security highlights the rapid expansion of cybercrime, the activities of which have evolved and become much more dangerous. Initially it involved the actions of individual hackers, who were not only motivated by money. Nowadays, cybercrime has created large and sophisticated business structures that are capable of attacking entire economic sectors.

The theft of confidential big data from companies, the denial-of-service attacks and phishing (using the identity of companies or public bodies in order to obtain confidential information from the victim), access to Swift or ransomware, are the main strategies used by cybercriminals.

Financial institutions are particularly exposed to this kind of manipulation and fraud as a result of their permanent contact with the public and the nature of their business, part of which involves payment systems.