Principles of action of the corporate information security policy

[May 2023]

Control version

Version	Date	Control
1	May 2023	✓ Initial version

Content

1. Introduction

1.1 Background

Information and communication technologies (ICT) are currently a key resource for the development and operation of banking services. ICTs are more than enablers in the strategies of the institutions and are part of almost all banking processes and distribution channels, but also execute automated controls on the key information (core) of the business.

Information security must be established around a set of measures and procedures which purpose is to safeguard the Group's information and promote the desire to:

- Ensure adequate protection of information, deploying security measures that the CaixaBank Group must adopt to adequately protect itself against threats and risks that could impact the confidentiality, integrity and availability of its systems, information assets or resources.
- Systematize information security management in such a way that it helps in adequate decision-making, based on risks, in situations related to the preservation of information security.
- Establish the information security function for the entire CaixaBank Group through responsibilities and roles.

1.2 Objective

The CaixaBank Group, aware of the importance that security in the processing of information has for the entire Group, customers, suppliers and, in general, all the institutions with which it maintains a relationship, considers it essential to establish the type of treatment that must be given to the information it manages, throughout its life cycle and to guarantee its confidentiality, integrity and availability.

The objective of the Corporate Information Security Policy (hereinafter the Policy) is to have the corporate principles on which the actions to be carried out in the field of information security must be based, all aimed at:

- Define the technical and organizational measures necessary to mitigate the risk on the security of the CaixaBank Group's information.
- Ensure the evaluation of decisions regarding information security to preserve the balance between profitability and risks.
- Maintain adequate management of this risk, in line with the Risk Appetite Framework, the result of which must be within the medium-low risk profile determined by the Board of Directors for the Group.
- Meet regulatory requirements and supervisory expectations.

The Policy to which these Principles refer is updated in line with current regulatory references and best practices in information security management, both nationally and internationally.

2. Applicability

The Policy to which these Principles refer is corporate and is aligned with the Corporate Technology Risk Management Policy. Its scope includes CaixaBank and all its subsidiaries (those in which the parent company exercises a position of control).

3. Corporate strategy / General principles of information security risk management

The information security strategy obeys the need to preserve the confidentiality, availability, and integrity of the information to achieve the strategic objectives of the business. With this premise, a strategy based on analysis and periodic monitoring of risks is adopted which, in accordance with the established risk thresholds, will determine their treatment.

Periodic risk analysis and monitoring is especially relevant in an environment in which new technologies are emerging that are quickly adopted by business and society. Likewise, this approach is justified by the incessant number of threats that appear daily on technology and information, either linked to new techniques or using either obsolescence or inadequate maintenance of environments.

The development of this strategy is inconceivable without the availability of a properly trained team. And, given the complexity of the Group, the development of the strategy cannot be conceived without the constant updating of knowledge acquired through both suppliers and participation in national and international forums and the adoption or alignment with international standards of recognized prestige.

3.1. Information security principles

One of the priority objectives of the Group is to guarantee transparency, independence, and good governance in order to safeguard the interests of all interest groups and have their trust.

The general principles are fundamental guidelines related to information security and must always be present in any activity related to the information and systems owned by the Group. The general principles are listed below:

a) Strategic alignment. The information security approach will always remain aligned with the Group's strategic objectives.

b) Risk management. Through integration with the corporate risk management framework, risks will be identified, monitored, and treated to place them at the acceptable levels defined by the Group.

c) Proportionality. The deployment of protection, detection and recovery measures will be proportional to the risks, their criticality, the value of the information and the cost of the defined security measures.

d) Security measures at various levels or layers. There will be a protection strategy made up of several security layers of organizational, logical and physical origin, arranged in such a way among them that when one fails, it allows gaining time for an adequate reaction against materialized incidents, reducing the probability that the system can be compromised as a whole and the final impact on systems and information is minimized.

e) Fundamental characteristics of information security. Due to the strategic nature of the Group's information and the mission to achieve business objectives, it is necessary to guarantee its protection

based on the pillars of confidentiality, integrity and availability. The confidentiality of the information must be guaranteed according to its categorization, in such a way that only authorized users have access to it. The integrity of the information must be ensured, guaranteeing that the data has not been manipulated and, therefore, is reliable. Finally, the availability of the information must be guaranteed, which will be the ability to remain accessible at the location, at the time and in the manner in which authorized users require it.

In the same way and due to legal and ethical requirements, the Group must protect in the same terms the information under its responsibility regarding clients, third parties and official bodies.

f) Delivery of value and continuous improvement. Through continuous monitoring of risks and controls, their effectiveness will be measured to optimize investments and spending on security. Continuous monitoring will allow the capture of emerging security risks, both motivated by technological evolution and by the Group's own evolution.

g) Security by default of the systems. The systems and their data must be designed and configured in order to guarantee a sufficient degree of security aligned with the strategic objectives of the business.

h) Management of human and technical resources. The information security process must be considered as a process made up of people, technical, material and organizational elements. The personnel using the systems and information must receive the necessary training and awareness and be informed of their duties and obligations in terms of information security. Said personnel must apply security principles in the performance of their duties.

i) Professionalism. The team in charge of managing information security will be duly trained and trained for the performance of their functions, under a process of updating and continuous training in the matter.

j) Classification of information and assets. The assets will be classified based on information security criteria and will be assigned according to the functions to be performed and applying the appropriate security measures.

k) Privileges, segregation and delegation of functions. The risks derived from the absence of segregation of functions or incompatibilities of functions with specific roles and the dependence or single-person overload in critical functions must be minimized.

l) Security incidents. Mechanisms for detection and reaction to security incidents that may compromise the Group's information systems or assets will be established. These procedures will cover detection mechanisms, classification criteria, analysis and resolution procedures, and communication to interested parties.

m) Disciplinary sanctions and breaches. In the workplace, non-compliance with the Security Policy may be considered a breach of the contractual good faith duty, punishable with the disciplinary measures provided for in the labor legislation and regulations in force at any time, and without prejudice to compensation for damages. that the Group may claim.

3.2. Information security principles in relation to providers

In the contracting of providers, it must be ensured that the requirements arising from corporate policies and supplier relationship frameworks are transferred, among which the following stand out:

a) Comply with current legislation on information security at all times in the territories in which or from which the provider provides services to the Group and favor free market practices, as well as regularly review and improve security practices. government.

b) Establish the necessary measures to prevent and avoid as far as possible that the Group's information and systems may be used for the practice of illegal conduct and review them periodically, actively collaborate with regulators and security forces and communicate all activities suspicious that are detected.

c) Promote responsible practices in terms of security among suppliers and their supply chain, through contractual clauses and the implementation of supervision mechanisms.

The Group will propagate the principles of the Corporate Information Security Policy to suppliers, both at a contractual level and through their training and disclosure.

4. Governance framework

The pillars on which the risk governance framework associated with information security in the CaixaBank Group is based are:

- Compliance with the principles contained in the Policy to which these Principles refer by the CaixaBank Group companies within their scope of application.
- Corporate supervision of the parent entity.
- Alignment of strategies among Group companies, and in turn alignment with best practices, supervisory expectations, and current regulations.
- Maximum involvement of the governing and management bodies of the Group companies.
- Internal control framework based on the Three Lines of Defense model that guarantees strict segregation of functions and the existence of several layers of independent control.

The Policy on which these Principles refer will be submitted for review by the Board of Directors.

5. Information and reporting framework

Establishing an appropriate reporting framework is critical to managing security risks.

The main objectives of the information framework are:

- Provide the Governing Bodies and Senior Management, sufficiently in advance, accurate, clear and sufficient information that facilitates decision-making and allows verification that it is operating within the established risk tolerance.
- Satisfy the information requirements of supervisory bodies.
- Provide those responsible for the different areas, especially the management areas and control areas, with the necessary data to be able to control compliance with the strategy defined for the Group in relation to security.

The information will be provided periodically to the Governing Bodies. Additionally, at the request of the Governing Bodies, they will be provided with any monograph or information requested on a one-off or recurring basis in relation to cybersecurity in the CaixaBank Group.