Corporate Information Security Policy

At **bicg**, information is a fundamental asset for the provision of its services and efficient decision making, which is why there is an express commitment to protect it as part of a strategy aimed at business continuity, risk management and the consolidation of a culture of security, based on the three fundamental pillars of information security:

- **Confidentiality**: is the guarantee of access to information for authorized users.
- **Integrity**: the preservation of complete and accurate information.
- **Availability**: is the guarantee that the user has access to the information he/she needs at that precise moment.

These pillars ensure information security in the areas of physical, logical and institutional security.

Understanding the confidentiality, integrity and availability of information as a frame of reference, and aligning these with business requirements, **bicg** establishes the following security objectives:

- Ensure that information assets receive an adequate level of protection.
- Classify information to indicate its sensitivity and criticality.
- Define levels of protection and special treatment measures according to their classification.

In order to achieve these objectives, **bicg** shall comply with the following Information Security requirements:

- Security in Human Resource Management, before, during and after employment.
- Proper asset management involving the classification of information and the handling of media
- Establishing robust logical access control to your systems and applications, managing user permissions and privileges.
- The protection of facilities and the physical environment, through the design of safe working areas and the security of equipment.
- Ensuring the security of operations by protecting against malware, backing up, logging and monitoring. monitoring the software in operation. managing technical vulnerabilities and choosing - appropriate techniques for auditing the systems.
- Communications security, protecting networks and the exchange of information.
- Ensure information security in the acquisition and maintenance of systems, limiting and managing change.
- The realization of safe software development, separating development and production environments, and performing appropriate functional acceptance testing.
- The control of relations with suppliers, contractually demanding compliance with the relevant security measures and acceptable levels in the provision of their services.
- Effectiveness in the management of security incidents, establishing appropriate channels for timely reporting, response and learning.
- The realization of a business continuity plan that protects the availability of services during a crisis or disaster.
- Identification of and compliance with applicable regulations, with special emphasis on intellectual property and the protection of personal data.
- The review of the present information security requirements to ensure compliance and effectiveness.

bicg's Management, by means of this Security Policy, undertakes to manage information security in order to meet the security objectives set, carrying out risk treatment plans that have been the result of the corresponding analysis to which the organization's information systems will be subjected.

To this end, **bicg** management has appointed a Security Committee**,** whose main function will be to determine the security requirements associated with the services and to measure the security objectives with predetermined metrics that provide objective and comparable results, and which will make it possible to determine their effectiveness in order to be able to identify possible improvements.