Table of Contents

Date	*Revision*	*Description / Modifications*
May 6, 2025	00	Initial edition
September 1,2025	01	Update
January 8, 2026	02	Update

Prepared by:	**Reviewed by:**	**Approved by:**
Security Officer	System Owner	Management

1. Approval

This Information Security Policy is approved by the Management on July 7, 2025, and is effective from that date until it is replaced by a new Policy.

2. Introduction

ABANCE INGENIERÍA Y SERVICIOS, S.L. depends on ICT systems (Information and Communication Technologies) to achieve its objectives. These systems must be diligently managed, taking appropriate measures to protect them from accidental or deliberate damage that may affect the availability, integrity, or confidentiality of the processed information or services provided.

The goal of information security is to ensure the quality of information and the continued delivery of services, by acting preventively, monitoring daily activity, and responding quickly to incidents.

ICT systems must be protected against rapidly evolving threats that could impact the confidentiality, integrity, availability, intended use, and value of the information and services. To defend against these threats, a strategy is required that adapts to changing environmental conditions to ensure the continuous delivery of services.

This means departments must apply the minimum-security measures required by the National Security Scheme (ENS), continuously monitor service performance levels, track and analyse reported vulnerabilities, and prepare effective incident responses to guarantee service continuity.

Departments must ensure that ICT security is an integral part of every stage of the system's life cycle—from its conception to decommissioning—covering development/acquisition decisions and operational activities. Security requirements and funding needs must be identified and included in planning, procurement requests, and tender specifications for ICT projects.

Departments must be prepared to prevent, detect, respond to, and recover from incidents, in accordance with Article 7 of the ENS.

in this document, the set of basic principles and lines of action to which the organization commits itself are set out, within the current and applicable legal regulatory framework, namely Royal Decree 311/2022, of 3 May, which regulates the National Security Framework (ENS), and the ISO 27001 standard. Likewise, this Policy is aligned with the European cybersecurity guidelines established in Directive (EU) 2022/2555 (NIS2) and its national transposition regulations, insofar as they are applicable to ABANCE INGENIERÍA Y SERVICIOS, S.L., reinforcing the approach to risk management, resilience, and incident response.

The Management of ABANCE INGENIERÍA Y SERVICIOS, S.L. focuses the Information Security System on continuous improvement and commits to promoting active compliance with this policy among all to meet all regulatory and business requirements and ensure the highest level of protection for all our information assets, whether from intentional attacks or accidental exposure, ensuring at all times the absolute confidentiality, integrity, availability, authenticity, and traceability of the information..

3. Definitions

- Information System: An organized set of resources that allows information to be collected, stored, processed or treated, maintained, used, shared, distributed, made available, presented, or transmitted.
- Risk: An estimate of the degree of exposure to the materialization of a threat over one or more assets causing harm or damage to the organization.
- Risk Management: Coordinated activities to direct and control an organization with respect to risks.
- Information Security Management System (ISMS): A management system based on the study of risks, established to create, implement, operate, monitor, review, maintain, and improve information security. The management system includes the organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources.
- Availability: Guarantee that system resources are operational when needed, especially those related to critical information.

- Integrity: Assurance that the system information remains as it was stored by an authorized agent.
- Confidentiality: Assurance that information is only accessible to authorized agents.
- Authenticity (ENS): Guarantee of the identity or origin of the information.
- Traceability (ENS): Guarantee for certain data of who did what and when.

4. Purpose

The purpose of this Information Security Policy is to protect Abance's information assets by ensuring the availability, integrity, confidentiality, authenticity, and traceability of both the information and the facilities, systems, and resources that process, manage, transmit, and store it — all in accordance with the organization's requirements and applicable legislation.

5. Scope

The scope of the Information Security Management System covers the information systems that support the ship engineering and naval systems services provided by Abance.

This Policy applies to all individuals, systems, and devices or media that access, process, store, transmit, or use information that is known, managed, or owned by the organization as part of the processes described.

All individuals with access to such information—regardless of whether it resides on automated or non-automated media, and regardless of whether they are employees of Abance or not—are subject to this Policy. Therefore, it also applies to contractors, interns, or any third parties with access to the organization's information or systems.

All such individuals will be considered users for the purposes of this document.

To ensure that the security process is continuously updated and improved, an Information Security Management System will be implemented and documented. In this way, the content of the Information Security Policy will be further developed through complementary security standards and procedures.

6. Mission

Mission: To deliver naval engineering, detailed design, production engineering, and systems engineering services.

Vision: To be a global company offering naval engineering services supported by fully digitized processes.

Values: We are driven by honesty, responsibility, innovation, commitment, teamwork, and balance.

7. Objectives

To comply with Royal Decree 311/2022 of May 3, which regulates the National Security Framework (ENS) and establishes its basic principles and minimum requirements, Abance has implemented a set of proportional security measures based on the nature of the information and services to be protected, and taking into account the category of the affected systems.

a) Security as a Comprehensive Approach and Principle of Least Privilege

Security is understood as a comprehensive approach encompassing all human, material, technical, legal, and organizational elements related to the information system. The handling of information shall be governed by this principle, which excludes any isolated or circumstantial actions.

Maximum attention shall be given to raising awareness among the individuals involved in the process, as well as their supervisors and managers, to prevent ignorance, lack of organization or coordination, or inadequate instructions from becoming sources of security risk.

Information systems must be designed and configured by granting only the minimum privileges necessary for their proper operation, which involves incorporating the following aspects:

a. The system shall provide only the essential functionality required for the organization to fulfill its statutory or contractual objectives.
b. Operation, administration, and activity logging functions shall be limited to the strict minimum necessary and carried out exclusively by authorized personnel, from equally authorized locations or equipment; access restrictions by schedule or authorized access points may be enforced where applicable.
c. In a production system, unnecessary or unsuitable functions shall be removed or disabled through configuration management. The regular use of the system must be simple and secure, such that insecure use would require a conscious action by the user.
d. Security configuration guides shall be applied for each technology, adapted to the system's categorization, to eliminate or disable any functions that are unnecessary or inadequate.

b) Risk-based security management.

Risk analysis and management are essential parts of the security process and must be conducted as ongoing and continuously updated activities. Managing risks effectively allows for the maintenance of a controlled environment by reducing them to acceptable levels.
This reduction shall be achieved through the appropriate implementation of security measures, applied in a balanced and proportionate way according to the nature of the information processed, the services provided, and the risks involved.

c) Prevention, detection, response, and recovery.

The system's security strategy must address prevention, detection, and response actions to minimize vulnerabilities and ensure that threats do not materialize—or, if they do, that they do not seriously impact the information handled or the services delivered.

Preventive measures—potentially including deterrence mechanisms or strategies to reduce the attack surface—should aim to eliminate or lower the likelihood of threats materializing. Detection measures shall focus on identifying the presence of a cyber incident. Response measures, which must be managed promptly, shall aim to restore the information and services potentially affected by a security incident.

Without prejudice to the remaining basic principles and minimum requirements, the information system shall ensure the preservation of data and electronic information. Likewise, it shall guarantee the availability of services throughout the full life cycle of digital information, based on a design and procedures that support the preservation of digital assets.

To ensure the availability of critical services, departments must develop ICT continuity plans as part of their overarching business continuity and recovery framework.

d) Defence-in-Depth Strategy

The information system must incorporate a protection strategy based on multiple layers of security. This layered approach shall ensure that, if one layer is compromised:

- The organization can respond appropriately to incidents that could not be prevented, reducing the likelihood of a full system compromise.
- The final impact on the system is minimized.

These defence layers must include organizational, physical, and logical security controls.

e) Continuous Monitoring and Periodic Reassessment

The system must support the detection of anomalous activities or behaviours and enable a timely response.

Ongoing assessment of asset security status shall allow tracking their progress, detecting vulnerabilities, and identifying configuration deficiencies.

Security measures shall be periodically reviewed and updated, ensuring their effectiveness evolves in line with new risks and protection mechanisms—potentially requiring a full revision of the security strategy when necessary.

Any inclusion or modification of physical or logical components in the system's asset inventory shall require prior formal authorization.

Continuous evaluation and monitoring shall ensure that system security reflects current vulnerabilities, configuration issues, and updates, while enabling early detection of incidents.

The implemented comprehensive security process shall be continuously updated and improved, applying recognized national and international best practices and methodologies for information security management.

f) Differentiation of responsibilities.

Information systems must clearly distinguish between roles and responsibilities. Specifically:

- The Information Owner defines the security requirements for the information being processed.
- The Service Owner determines the security requirements for the services provided.
- The System Owner is accountable for the delivery and operation of those services.
- The Information Security Officer is responsible for taking decisions to ensure that the defined security requirements are fulfilled.

In cases involving the processing of personal data, the Data Controller must also be identified, as well as the Data Processor, where applicable.

8. Security Requirements

8.1. Security organization and process implementation

Information security applies to all individuals within the scope of this document (users).
Abance identifies the responsible parties and defines their responsibilities in the sections “Roles, Responsibilities and Duties” and “Third Parties” of this document.
This Security Policy and the related regulations must be made known to all individuals within its scope.

8.2. Risk analysis and management

Identifying and understanding risks, and developing a strategy to manage them effectively, is essential for the organization. Only by understanding the security posture can appropriate decisions be made to mitigate the risks faced.

When an information system processes personal data, the provisions of the GDPR and the LOPDGDD, or where applicable, Organic Law 7/2021 of May 26 on the processing of personal data for the purpose of preventing, detecting, investigating, and prosecuting criminal offenses and executing criminal penalties, shall apply. The Data Controller or Processor, advised by the Data Protection Officer (DPO), shall conduct a risk analysis in accordance with Article 24 of the GDPR, and a Data Protection Impact Assessment as required under Article 35. Additional security measures may be required as a result.

Abance uses the ISO 31000 methodology to analyse risks, conducting a detailed assessment of risks affecting assets recorded in the Asset Inventory. These results are documented in the Risk Analysis Report.

The organization defines risk thresholds from which it adopts appropriate treatment measures. A risk is considered acceptable when implementing further controls would consume more resources than the potential impact of the risk.

This analysis shall be repeated:

- Regularly, at least once per year.

- When the information or services involved change significantly.
- When a serious security incident occurs or major vulnerabilities are identified.

Once the risk evaluation has been completed, senior management is responsible for approving the residual risks and the associated risk treatment plans.
If the risk analysis identifies the need for stricter controls than those required by the ENS, these additional measures will be implemented accordingly.

8.3. Personnel management

All Abance personnel must be trained and informed of their duties and obligations regarding information security, particularly in the relevant procedures applicable to their roles. Their actions are monitored in accordance with assigned responsibilities to ensure adherence to established procedures.

Staff awareness and training are reinforced through the regular distribution of concise security awareness capsules.

Each user is assigned a unique login, and their access rights and related activities are periodically reviewed to correct inconsistencies or enforce accountability when necessary.

8.4. Professionalism, awareness, and training

The security of Abance's systems is managed by qualified internal personnel and specialized external staff, who receive and regularly update the training necessary to ensure information security.

All policies, standards, and procedures related to this Information Security Policy must be clearly communicated and made known to all relevant individuals, companies, and institutions.

Awareness and training activities shall be conducted on a regular basis, and users will be provided with copies of the relevant policies.

8.5. Access control and authorization

Access to information systems is controlled, monitored, and restricted to users, processes, devices, and systems with only the minimum required or explicitly authorized functionalities.

8.6. Physical security

Systems are located in protected areas equipped with appropriate physical, redundancy, continuity, and environmental security measures, and governed by formal access control procedures.

8.7. Procurement of security products and services

Security products and information and communication technology (ICT) security services to be used in information systems shall be procured in proportion to the system's classification and the required security level.

Whenever possible, products and services must hold the corresponding security certification. In this regard, Spain's National Cryptologic Center (CCN), through its Certification Body within the National Evaluation and Certification Scheme for IT Security, will determine the following, based on recognized national and international evaluation criteria and methodologies, and considering the intended use of the product or service:

- The security functionality and assurance requirements applicable to certification.
- Any additional mandatory security certifications required by regulation.
- In exceptional cases, the criteria to follow when no certified products or services are available.

The procurement of security services shall be subject to the provisions outlined in the previous sections and in the "Third Parties" section of this document.

8.8. Least privilege and security by design

At Abance, systems are always designed and configured with *security by default* principles in mind. Systems provide only the minimum necessary functionality, with operational, administrative, and logging features restricted to the essential minimum and accessible solely by authorized personnel, from authorized locations or devices.

This approach is particularly critical in production systems, where unused or unnecessary functions are removed, disabled, or explicitly recommended for deactivation, as appropriate.

All projects involving or impacting information systems must include a security requirements assessment and define a security model in coordination with the Information Security Officer.

Security by design, secure coding practices, and appropriate security controls and measures shall be integrated throughout the design, development, installation, and operation of information systems and projects, in accordance with the Statement of Applicability approved by the organization.

To support this, security configuration guides tailored to the system's classification shall be applied to disable or remove any unnecessary or inadequate functionalities.

8.9. System integrity and updates

Abance regularly verifies the integrity and update status of its systems to maintain full awareness of their security posture. This process takes into account vendor specifications, identified vulnerabilities, and applicable updates, thereby ensuring proper system integrity management.

All system components must receive prior authorization before installation.

8.10. Information protection (stored and in transit)

Information is classified according to its required sensitivity and the applicable levels of security and protection.
Abance pays special attention to information that is stored or transmitted through untrusted environments. This includes data handled or processed on portable devices, tablets, smartphones, peripheral devices, storage media, and communications over open or weakly encrypted networks. Appropriate technical and procedural safeguards are implemented to ensure that all information is processed in accordance with its classification.
Procedures are in place to guarantee the long-term preservation and recoverability of electronic documents generated by information systems.
Any non-electronic information that is either a cause or a direct result of digital information must be protected to the same security level. Security measures will be applied according to the medium's characteristics and relevant regulations.

8.11. Prevention of risks from interconnected systems

Abance protects the perimeter of its information systems—particularly at Internet connection points—by continuously assessing the risks associated with interconnecting with other systems and implementing the necessary measures to ensure the required level of security.

8.12. Activity logging

In compliance with the provisions of this Royal Decree, and with full guarantees of the rights to honour, personal and family privacy, and personal image—as well as in accordance with applicable regulations on personal data protection and labour law—Abance logs user activity, retaining only the information strictly necessary to monitor, analyse, investigate, and document any improper or unauthorized actions. This enables the identification of the individual responsible at all times.

To preserve the security of information systems and in line with the General Data Protection Regulation (GDPR)—including the principles of purpose limitation, data minimization, and storage limitation—the organization may, strictly when necessary and proportionate, analyse incoming and outgoing communications solely for information security purposes. These include preventing unauthorized access to networks and systems, blocking denial-of-service (DoS) attacks, and stopping the dissemination of malicious code or other threats to the integrity of these systems.

To ensure accountability, each user accessing the information system must be uniquely identified. This ensures that it is always possible to determine who has been granted access rights, the nature of those rights, and who performed specific activities

8.13. Security Incidents and Malware Detection

Any compromise of the confidentiality, integrity, availability, authenticity, or traceability of information is considered a security incident.

Abance has established procedures for the management of security incidents, supported by systems for their detection and response. All incidents are classified, managed, and resolved while ensuring the collection of relevant evidence. This process supports incident reporting and post-incident analysis to foster continuous improvement.

Systems are in place to detect and respond to malicious code, and intrusion detection and prevention mechanisms are implemented. Technical security audits are conducted to verify the effectiveness of protection measures.

Designated communication channels are available for users to promptly report any detected incident or anomaly

8.14. Business continuity

Abance performs regular backups to ensure information recovery and implements appropriate measures to guarantee the continuity of operations in the event of a disruption or loss of primary working resources.

8.15. Continuous improvement

The implemented Information Security Management System (ISMS) is continuously updated and enhanced in accordance with the requirements of ISO/IEC 27001 and the National Security Framework (ENS).

9. Legal Requirements and Regulatory Framework

ABANCE operates within the following legal and regulatory framework for information security:

- Organic Law 3/2018 of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (Spain).
- Royal Decree 311/2022 of May 3, which regulates the National Security Framework (ENS) in the field of electronic administration.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (General Data Protection Regulation - GDPR), applicable to the fully or partially automated processing of personal data, as well as to the non-automated processing of personal data contained in or intended to be part of a filing system.
- CCN-STIC Security Guidelines issued by the National Cryptologic Center (CCN).
- The applicable collective bargaining agreement.
- Standards: UNE-EN-ISO 9001, UNE-EN-ISO 14001, UNE-ISO/IEC 27001, and UNE-EN-ISO 45001.

10. Roles, Responsibilities, and Duties

The Management of Abance assigns, renews, and communicates the responsibilities, authorities, and roles associated with information security. These appointments are reviewed every four years or whenever a position becomes vacant.

Management also ensures that users are aware of, accept, and perform their assigned responsibilities, authorities, and roles, and resolves any conflicts that may arise concerning information security responsibilities.

As part of this Information Security Policy, the main roles are documented in the *Role Designation Record* and include:

- **Information and Service Owner**
- **Data Protection Officer (DPO)**
- **Security Officer**
- **System Owner**
- **System Security Administrator**

The following sections define the specific duties assigned to each of these roles.

10.1. Users

Users are responsible for their conduct when accessing information or using the organization's information systems. Each user is accountable for all actions carried out using their personal identifiers or credentials.

Users are required to:

- Comply with the Information Security Policy, as well as all related rules, procedures, and guidelines.
- Protect and safeguard organizational information, preventing its disclosure, external transmission, modification, deletion, accidental or unauthorized destruction, or misuse—regardless of the medium through which it was accessed or became known.
- Familiarize themselves with and apply the Information Security Policy, the Acceptable Use Policy for Information Systems, and all applicable policies, procedures, and security measures.

Users who violate the Information Security Policy or any associated policies or procedures may be subject to disciplinary action in accordance with Abance's internal regulations, without prejudice to any applicable civil or criminal liability.

10.2. Information Owner (ENS)

The Information Owner is ultimately accountable for any error or negligence that results in a breach of confidentiality or integrity (in the context of data protection), or of availability (in the context of information security).

Key responsibilities include:

- Ensuring the appropriate use and protection of information by approving the relevant security policies and standards.
- Defining the information security requirements.
- Determining the appropriate security classification levels of the information processed, by assessing the potential impact of adverse events.
- Formally accepting residual risk levels that may affect the service.

10.3. Service Owner (ENS)

The Service Owner is accountable for the assets associated with the service.

General responsibilities include:

- Defining the service's security requirements—including interoperability, accessibility, and availability—by approving the relevant policies and security standards.

- Establishing the appropriate security controls for the service in coordination with the Security Officer and the System Owner, as defined in the Statement of Applicability.
- Ensuring the ongoing protection of information and continuity of services provided by the information systems under their responsibility.
- Formally accepting residual risks that may impact the service.

10.4. Management

Management is fully committed to the policy outlined in this document and is aware of the value of information and the serious economic and reputational consequences that a security incident may entail.

Within the framework of the ENS, Management assumes the responsibilities assigned to both the Information Owner and the Service Owner. It is therefore the owner of its own information assets and accountable for the associated risks.

Additional responsibilities include:

- Demonstrating leadership and commitment to the Information Security Management System (ISMS).
- Ensuring that the Information Security Policy and objectives are established and aligned with the organization's strategic direction.
- Approving and communicating the Information Security Policy, the Information Systems Usage Rules, and the importance of compliance to all users—internal, external, clients, and suppliers.
- Fostering a strong corporate culture of information security.
- Supporting the continuous improvement of information security processes.
- Ensuring the availability of necessary resources to comply with the security policy, usage rules, and ISMS operation.
- Ensuring that information security audits are conducted and their findings reviewed to identify opportunities for improvement.
- Defining and managing the information security budget.
- Approving documentation up to the second level (standards and procedures).
- Determining disciplinary or other measures applicable to individuals responsible for security breaches.

10.5. Security Officer (ENS)

The Security Officer shall assume the following responsibilities:

- Promote the security of the information managed and of the electronic services provided by the information systems, with the authority and responsibility to ensure that the Information Security Management System (ISMS) complies with ENS requirements.
- Supervise compliance with this Policy, related standards, derived procedures, and the secure configuration of systems.
- Implement the security measures established by the Information and Service Owners, in full alignment with the provisions of Annex II of the ENS.
- Promote awareness and training activities related to security within their scope of responsibility.
- Coordinate and monitor the implementation of compliance projects (e.g., ISO 27001 and ENS) in collaboration with the System Owner.
- Carry out risk analyses—together with the System Owner—select appropriate safeguards, and oversee the risk management process.
- Promote periodic audits to verify compliance with information security requirements, analyze audit reports, and present conclusions to the System Owner to enable appropriate corrective actions.
- Coordinate Security Management in collaboration with the System Owner.
- Prepare annual security reports that include the most relevant incidents for each period, in coordination with the System Owner.
- Determine the system categorization in accordance with Annex I of the ENS, and the corresponding security measures in line with Annex II.
- Verify that security measures are adequate to protect both information and services.
  Ensure the execution—directly or by delegation—of security-related decisions made by Management.

Regarding documentation, and in collaboration with the System Owner:

- Propose second-level security documentation (ICT Security Standards and General ISMS Procedures) for approval by Management and the System Owner, and sign such documents.
- Approve third-level documentation (Operational ICT Procedures and ICT Technical Instructions).
- Maintain all documentation organized and up to date, and manage access control mechanisms to such documents.

The Security Officer may request the collaboration of the System Owner to carry out any of these responsibilities.

10.6. Data Protection Officer (DPO)

In accordance with the GDPR and the LOPDGDD, the Data Protection Officer shall perform, at a minimum, the following duties:

- Inform and advise the data controller and employees on their obligations under the GDPR and other applicable data protection legislation.
- Monitor compliance with the GDPR, Union and Member State data protection provisions, and the internal policies of the controller or processor, including the assignment of responsibilities, awareness-raising, staff training involved in processing operations, and related audits.
- Provide advice, upon request, regarding data protection impact assessments and monitor their execution.
- Cooperate with the supervisory authority.
- Act as the contact point for the supervisory authority on matters relating to processing activities, including prior consultations, and consult on any other issue as needed.

10.7. System Owner

The System Owner is responsible for the following functions:

- Developing, operating, and maintaining the Information System throughout its entire lifecycle, including its specifications, installation, and verification of proper functioning.
- Defining the system's topology and management model, establishing usage criteria and available services.
- Ensuring that specific security measures are properly integrated within the overarching security framework.
- Conducting drills and tests of operational security procedures and existing continuity plans.
- Monitoring all phases of the system lifecycle: specification, architecture, development, operation, and change management.
- Implementing the necessary measures to ensure system security throughout its lifecycle, in coordination with the Security Officer.
- Approving any substantial configuration changes to system components, in agreement with the Security Officer and Management.
- Suspending information processing or electronic services if serious security deficiencies are detected, subject to agreement with the Security Officer and Management.
- Performing required risk analyses, selecting appropriate safeguards, and reviewing the risk management process, in collaboration with the Security Officer.
- Preparing third-level security documentation (ICT Operational Procedures and ICT Technical Instructions) jointly with the Security Officer.

10.8. System Security Administrator

The System Security Administrator is responsible for:

- Implementing, managing, and maintaining the security measures applicable to the information system.
- Managing, configuring, and updating (as applicable) the hardware and software that support the system's security mechanisms and services.
- Managing user authorizations, particularly privileged access rights, and monitoring system activity to ensure compliance with granted permissions.
- Applying operational security procedures.
- Applying configuration changes to the information system.
- Ensuring strict enforcement of established security controls and the application of approved procedures for system operation.
- Supervising hardware and software installations, modifications, and enhancements to ensure that security is not compromised and that changes conform to proper authorizations.
- Monitoring the system's security posture using security event management tools and technical audit mechanisms implemented in the system.
- Promptly notifying the designated responsible parties of any security anomaly, compromise, or vulnerability detected.
- Participating in the investigation and resolution of security incidents, from initial detection through to closure.

11. Conflict Resolution

In the event of a conflict between designated Responsible roles, the issue shall be resolved by Management.

12. Personal Data

The organization will only collect and process personal data when it is adequate, relevant, and not excessive, and when it is related to the scope and purposes for which it was obtained.

Likewise, it will adopt the necessary technical and organizational measures to always comply with the applicable data protection regulations.

In compliance with the GDPR and the LOPDGDD, measures have been adopted such as: legal legitimacy analysis of each personal data processing activity carried out, risk analysis, impact assessment when the risk is high, the record of processing activities, and the appointment of the Data Protection Officer.

From the risk analyses performed, additional measures may arise that overlap with those already adopted in compliance with the ENS, depending on the system categorization.

13. Third Parties

When Abance provides services to other organizations or handles their information, such organizations shall be informed of this Information Security Policy.

Abance shall define and approve the appropriate communication channels for coordinating information exchange and procedures for responding to security incidents.

When Abance makes use of third-party services or transfers information to third parties, they shall also be informed of this Security Policy and any applicable security standards related to the services or information involved. Such third parties shall be bound by the obligations established in the relevant security policies, and may develop their own operational procedures to ensure compliance.

Specific procedures will be established for communication and incident resolution. Abance shall ensure that third-party personnel are appropriately trained and made aware of security requirements, at a level at least equivalent to that set out in this Security Policy.

Furthermore, third parties must be able to present a valid Statement of Conformity with the ENS for services involving BASIC category systems, or a valid Certification of Conformity with the ENS for services involving MEDIUM or HIGH category systems.

In cases where a third party is unable to comply with any aspect of this Security Policy, the Security Officer shall issue a report identifying the associated risks and proposing mitigation measures. This report must be approved by the relevant Information and Service Owners.

13.1. Third Parties as Outsourced Security Services

In the case of outsourced security services, the service provider must designate a Point of Contact (POC) for the security of the processed information and the services delivered.

This POC must have the endorsement of the provider's senior management and shall be responsible for overseeing compliance with the security requirements applicable to the contracted service or solution, as well as for coordinating all communications related to information security and incident management within the scope of said service.

The appointed POC shall be either the provider's own Security Officer, a member of the security department, or a person with direct reporting lines to it.

14. Review and Audits

The Security Officer shall review this policy at least annually, or whenever significant changes occur that justify its revision, and will submit the updated version for Management approval, if necessary.

The purpose of the review is to assess the effectiveness of the policy, considering technological developments, changes in organizational activity, and updates to guidelines issued by the National Cryptologic Center (CCN) regarding security measures and controls.

Management shall be responsible for approving any modifications to this document when changes arise that affect the defined risk scenarios.

The Information Security Management System (ISMS) will be audited annually, in accordance with the requirements of ISO/IEC 27001, and audited every two years to maintain compliance with the National Security Scheme (ENS).

31339791Z CARLOS CAMPOY (R: B11324456)

Firmado digitalmente por 31339791Z CARLOS CAMPOY (R: B11324456)
Fecha: 2026.01.09 13:41:49 +01'00'

CARLOS CAMPOY ZUASTI

CEO