

INFORMATION SECURITY POLICY

Public Disclosure Notice:

This document has been prepared by **Nazaríes Information Technologies, S.L.** for general informational purposes. The information contained herein is provided in good faith and may be freely shared, reproduced, or distributed, provided that proper credit is given to **Nazaríes Information Technologies, S.L.** as the original source. While every effort has been made to ensure the accuracy of the information, **Nazaríes Information Technologies, S.L.** makes no warranties or representations regarding its completeness or reliability. The content of this document is subject to change without notice. ©2026

TABLE OF CONTENTS

APPROVAL AND ENTRY INTO FORCE.	3
INTRODUCTION.	4
PURPOSE.	5
A - The objectives or mission of the organization.	5
B - Legal and Regulatory Framework.....	6
C - Security Roles and Functions	8
D - Structure and Composition of the Committee for the Management and Coordination of Security.....	13
E - Guidelines for Structuring System Security Documentation, Its Management and Access	15
F - Risks Arising from the Processing of Personal Data.	16

APPROVAL AND ENTRY INTO FORCE.

This document has been reviewed and approved by the Security Committee on **July 30, 2026**. From now on, we will refer to the ENS Information Security System using the term ISMS (Information Security Management System), by virtue of its integration and scope within the system.

In accordance with the recommendations of the ICT SECURITY GUIDE (CCN-STIC-801) and considering our resources and scope, the Information Security and ICT Services Committees may operate simultaneously, thanks to their integration and equivalence within **Nazaríes Information Technologies, S.L.**

This Information Security Policy shall enter into force as of this date and shall remain in effect until a new policy is issued to replace it.

INTRODUCTION.

At **Nazaríes Information Technologies, S.L.**, since 2018 an information security policy has been implemented that plays a fundamental role in our management and in the protection of the data and services we manage.

Our security policy has been established following a rigorous process that addresses multiple essential aspects. It has been formally approved and, at a minimum, includes clear guidelines on our objectives as an organization, the relevant regulatory framework that affects us, the responsibilities and roles related to security, the structure of committees responsible for supervising and coordinating security aspects, as well as precise guidelines for managing documentation and the security of our systems.

It is very important that each member of our team knows and complies with these security standards. Our policy complies with minimum security requirements, which vary according to the risks identified in our systems.

Within this framework, information security becomes a fundamental pillar to ensure the integrity, confidentiality and availability of the data and services we handle as a company.

PURPOSE.

At **Nazaríes Information Technologies, S.L.**, the Information Security Policy aims to establish guidelines and principles for the effective management and protection of information and services. We will implement, maintain and continuously improve an Information Security Management System (ISMS) in accordance with the requirements of UNE ISO/IEC 27001:2022, PCI-DSS v4.0 certification and the National Security Framework (Medium Level) and the needs of our interested parties.

This will be carried out in compliance with the applicable regulatory framework, which includes current legal provisions such as Spanish Royal Decree 311/2022, of May 3, regulating the National Security Framework. The application of this policy focuses on ensuring the adequate protection of information within the context of our organization.

The purpose of both the ISMS and the Security Policy is to ensure the protection of information and services, guaranteeing their authenticity, confidentiality, integrity, availability and traceability. This extends to the assets used in the processing, transmission and storage of information.

The dissemination, knowledge and application of this Information Security Policy is the responsibility of all personnel, both internal and external, who have access to the information of **Nazaríes Information Technologies, S.L.** and to the technological resources used in the organization's operations. This includes all levels of the organization, from the Management Committee to the information systems that support the services and processes necessary to achieve business objectives.

A - The objectives or mission of the organization.

The mission of **Nazaríes Information Technologies, S.L.** is to analyze, design, develop, integrate, deploy, roll out, operate and maintain technological solutions—including technology consulting services, software, data, artificial intelligence and IoT—, as well as to provide customer support, help desk and incident management services, with the highest levels of quality, response time and information security, while complying at all times with the customer's requirements.

To this end, the organization maintains the information systems and processes that support these activities and its corporate processes, in accordance with the applicable system categorization and the Statement of Applicability in force.

The main objective of information security is to protect company data. However, this concept is expressed in general terms, since the system will ensure five fundamental aspects: confidentiality,

availability, traceability, authenticity and integrity. To carry out these actions, strategies must be established where policies of action are drafted for each of these cases.

This Policy shall apply to the information systems of **Nazaríes Information Technologies, S.L.** related to the exercise of its competencies and to all users with authorized access to them, whether or not they are public employees and regardless of the nature of their legal relationship with the company.

All employees are required to know and comply with this Information Security Policy and its derived Security Regulations, and it is the responsibility of the Information Security Committee to provide the necessary means so that the information reaches the affected personnel.

In this context, personal computers individually financed and not inventoried are not considered IT resources of **Nazaríes Information Technologies, S.L.**, even if they may occasionally be used for research tasks. However, if access to the corporate network is made through such personal computers, they shall be subject to the obligations established in this information security policy and its implementing regulations.

Specifically, this security policy applies to the following services:

- Customer Success
- Engineering
- DevOps
- Ticketing & SaaS

B - Legal and Regulatory Framework

The responsibilities of the departments of **Nazaríes Information Technologies, S.L.** towards their clients is reflected in the contracts signed by both parties. Likewise, this department requires from its suppliers the services and products acquired under the terms, services, and obligations set forth in the contracts signed for such purpose.

The applicable legislation in the event of conflict between the parties is also specified in the service provision contracts signed by both parties.

The applicable regulations and standards include, among others:

(ES) Law 34/2002, of July 11, on Information Society Services and Electronic Commerce
(LSSICE): Ensures that our company complies with the obligation to provide clear and

accessible information to users regarding the services offered and the terms of use, in addition to regulating advertising and content liability.

UNE-ISO/IEC 27002:2022 Code of Practice for Information Security Management: Provides a reference framework for establishing effective security policies in information management, helping us protect our assets and mitigate risks associated with information security.

UNE-ISO/IEC 27001:2022 Specifications for Information Security Management Systems: Requires us to implement an Information Security Management System (ISMS), enhancing our ability to manage risks and comply with regulatory requirements, thereby increasing customer trust.

Regulation (EU) No 910/2014 (eIDAS): Facilitates the use of trust services, such as electronic signatures, enabling our company to carry out electronic transactions securely and legally, improving efficiency and security in our operations.

(ES) Royal Decree 311/2022, of May 3, regulating the National Security Framework: Requires us to comply with security standards to protect information systems, especially if we work with public sector data, which may influence our risk management practices.

(ES) Law 9/2014, of May 9, General Telecommunications Law: Modernizes telecommunications regulation in Spain, promoting competition, improving user rights, and facilitating the deployment of advanced infrastructures.

PCI-DSS (PCI Security Standards Council): Establishes requirements for the protection of payment card data, directly affecting our security management if we process card transactions, ensuring that we properly handle sensitive information.

Regulation (EU) 2019/881 (Cybersecurity Act): Establishes a cybersecurity framework within the EU, affecting our company by requiring the implementation of measures to protect our systems and data against cyber threats.

Regulation (EU) 2024/1689 (IA Act): Establishes a harmonised legal framework for the development, marketing and use of artificial intelligence systems in the EU based on risk, affecting our company by requiring us to classify our AI systems according to their level of risk and to comply with the applicable transparency, human oversight, risk management and data quality requirements for each category.

(ES) Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights: Requires us to ensure the protection of personal data of our clients and employees, establishing protocols for the processing, storage, and security of personal information.

(SP) Law 22/2019, of December 6, amending the Intellectual Property Law: Affects our ability to protect and enforce our rights over the software and other digital products we develop, as well as the management of the use of third-party works in our services.

(ES) Law 31/1995, of November 8, on the Prevention of Occupational Risks: Requires us to ensure the safety and health of our employees in the workplace by implementing policies and measures to prevent risks and promote a safe working environment.

(ES) State Collective Agreement for Consulting Companies, Information Technologies and Market and Public Opinion Research (agreement code 99001355011983) – April 13, 2023, Applicable Collective Agreement: Regulates specific employment conditions, including aspects related to salaries, working hours, and labor rights, directly impacting the management of human resources within our organization.

C - Security Roles and Functions

In application of the criteria set out in the CCN-STIC-801 Guide ([Guía ENS. Responsabilidades y Funciones](#)), the following roles are distinguished within the ISMS of **Nazaríes Information Technologies, S.L.**:

- Information Owner
- Service Owners
- System Owner
- Information Security Officer
- Data Protection Officer

As permitted by the aforementioned Guide, the Security Committee, as a collegiate body, performs the functions of “Information Owner.” There is an Information Security Officer. The Data Protection Officer is internal company personnel, and their appointment is recorded in minutes signed by the CEO.

Any conflicts between the roles involved in the ISMS that may arise during the normal course of company activities or in security crisis situations shall be resolved within the Security Committee. In case of conflicts between roles, the company CEO shall be invited to the Committee. Decisions regarding such conflicts shall be taken unanimously; failing unanimity, the CEO shall issue a binding decision.

The main functions of each of these roles, in the field of information security, are as follows:

Public Disclosure Notice:

This document has been prepared by **Nazaríes Information Technologies, S.L.** for general informational purposes. The information contained herein is provided in good faith and may be freely shared, reproduced, or distributed, provided that proper credit is given to **Nazaríes Information Technologies, S.L.** as the original source. While every effort has been made to ensure the accuracy of the information, **Nazaríes Information Technologies, S.L.** makes no warranties or representations regarding its completeness or reliability. The content of this document is subject to change without notice. ©2026

Information Owner

The responsibilities of the Information and Service Owner include:

- Establishing the necessary security levels for each aspect that constitutes the system categorization.
- Accepting responsibility for the residual risk associated with the information and services.
- Assuming ultimate responsibility in the event of any error or negligence resulting in a confidentiality or integrity incident (within the scope of data protection) or an availability incident (within the scope of information security), without exempting Senior Management from its corresponding responsibility.

Service Owners

The responsibilities of the Service Owners are as follows:

- Determining the necessary security requirements to ensure adequate protection of the services provided by these applications and technological platforms, considering the relevant interests and needs.
- Assuming responsibility for both the use and the protection of shared services and therefore being accountable for any error or negligence in the use of these services that may result in a security incident.
- Playing an active role in the Security Committee.

System Owner

The responsibilities of the System Owner include:

- Developing, operating, and maintaining the information system throughout its entire lifecycle, including specifications, installation, and verification of proper operation.
- Defining the topology and management of the information system, establishing usage criteria and available services.
- Ensuring the proper integration of security measures within the overall security framework.

-
- Developing, maintaining, and ensuring compliance with operational security procedures.
 - Preparing security improvement plans and continuity plans.
 - Committing to the implementation and monitoring of continuity plans.
 - Avoiding the temporary suspension of services, prioritizing maximum system availability whenever possible.
 - Supervising and planning the implementation of safeguards within the system.
 - Deciding to suspend information processing in the event of detecting serious deficiencies, although the final decision rests with Senior Management.
 - Applying the security configuration approved by the Information Security Officer.
 - Monitoring the security status of the systems.
 - Recording, tracking, and managing security incidents within the systems under their responsibility.
 - Isolating incidents to prevent their spread to elements outside the risk situation.
 - Making immediate decisions if information is compromised in a way that may have serious consequences.
 - Ensuring the integrity of critical system elements if their availability is affected.
 - Maintaining and recovering information stored by the System and its related services.
 - Investigating incidents, determining their nature, means, motivations, and origin.
 - Planning the implementation of safeguards within the system.
 - Executing the approved security plan.

Information Security Officer

The Information Security Officer is appointed by the Management Committee. Unless their function is revoked by another decision of the Management Committee, they shall continue to perform this role.

The responsibilities of the Information Security Officer include:

- Promoting and participating in the creation and implementation of information security policies, regulations, procedures, and guidelines in accordance with the requirements of the applicable security standards.

Public Disclosure Notice:

This document has been prepared by **Nazaríes Information Technologies, S.L.** for general informational purposes. The information contained herein is provided in good faith and may be freely shared, reproduced, or distributed, provided that proper credit is given to **Nazaríes Information Technologies, S.L.** as the original source. While every effort has been made to ensure the accuracy of the information, **Nazaríes Information Technologies, S.L.** makes no warranties or representations regarding its completeness or reliability. The content of this document is subject to change without notice. ©2026

- Overseeing information security in accordance with the general guidelines established in the Security Policy.
- Preparing the Statement of Applicability document.
- Ensuring that the Information Security Management System complies with the security standards selected by the Information Security Committee.
- Conducting periodic evaluations to analyze security and proposing changes to security controls as necessary.
- Identifying relevant laws, regulations, and standards that may impact information security and proposing applicable measures, seeking external advice when necessary.
- Actively collaborating in the development of the Information Security Management System.
- Documenting the authorized uses of the organization's information systems for approval by the Security Committee.
- Contributing to the design of security awareness and training initiatives for all personnel.
- Regularly evaluating the effectiveness of controls implemented within the technological infrastructure.
- Establishing communication channels with the various stakeholders involved in information security, including system administrators, security specialists, and physical security managers.
- Collaborating in the initiation of information security projects and promoting solutions aligned with the organization's needs.
- Referring to the Information Security Committee any unresolved conflicts affecting multiple areas or departments.
- Serving as the specialized point of contact for coordination with the designated CSIRT.
- Conducting periodic risk analyses to assess the organization's exposure to vulnerabilities and threats, identifying possible mitigation measures.
- Contributing to the definition of a risk analysis methodology.
- Collaborating in the development of a risk management plan for the continuous improvement of information security.
- Making recommendations to the Information Security Committee within their area of responsibility.

- Reporting to Management on the performance of the Information Security Management System.
- Communicating audit results to Management.
- Verifying the consistency of information security efforts across the organization, identifying duplications or uncovered areas.
- Evaluating the effectiveness of information security awareness and training plans.
- Acting as the primary point of contact of **Nazaríes Information Technologies, S.L.** in matters related to information security.
- Presenting the results of risk analyses to the Information Security Committee.
- Notifying the Security Committee of relevant incidents that may affect the information security of **Nazaríes Information Technologies, S.L.**
- Analyzing and proposing safeguards to prevent similar incidents in the future.

Data Protection Officer

The responsibilities of the Data Protection Officer include:

- Ensuring compliance with the principles related to data processing.
- Identifying the legal bases for data processing activities.
- Evaluating the compatibility of purposes other than those that motivated the initial data collection.
- Determining whether sector-specific regulations establish processing conditions different from those set out in the GDPR.
- Designing and implementing information measures for individuals affected by data processing activities.
- Establishing mechanisms to receive and manage data subject rights requests.
- Assessing data subject rights requests.
- Managing the engagement of data processors, including the details of contracts or legal agreements governing the relationship between the controller and the processor.
- Identifying appropriate international data transfer mechanisms suited to the organization's needs and characteristics, along with the corresponding justifications.

Public Disclosure Notice:

This document has been prepared by **Nazaríes Information Technologies, S.L.** for general informational purposes. The information contained herein is provided in good faith and may be freely shared, reproduced, or distributed, provided that proper credit is given to **Nazaríes Information Technologies, S.L.** as the original source. While every effort has been made to ensure the accuracy of the information, **Nazaríes Information Technologies, S.L.** makes no warranties or representations regarding its completeness or reliability. The content of this document is subject to change without notice. © 2026

-
- Designing and implementing data protection policies.
 - Establishing and maintaining records of processing activities.
 - Integrating data protection measures from the design stage and ensuring data protection by default, adapted to the risks and nature of the processing activities.
 - Implementing security measures appropriate to the risks and nature of the processing activities.
 - Establishing procedures to manage data security incidents, including assessing risks to the rights and freedoms of individuals.
 - Determining whether data protection impact assessments are required.
 - Conducting data protection impact assessments.
 - Managing relationships with supervisory authorities.
 - Implementing training and awareness programs for personnel on data protection matters.

Appointment and Renewal Procedures

All roles are appointed by the CEO of the company.

Any change to the person assigned to a role may occur at the initiative of the CEO or due to the departure of the employee from the company, in which case the CEO must appoint a successor to that role.

Such changes must be notified to the Security Committee, which shall be responsible for providing the necessary information, training, and resources to ensure that the role is carried out effectively.

D - Structure and Composition of the Committee for the Management and Coordination of Security

This Committee is responsible for the definition, implementation, and monitoring of all matters related to Information Security at **Nazaríes Information Technologies, S.L.** Within our organization, general responsibility for information security lies with the Information Security Officer, while ultimate responsibility rests with Management as the highest authority of the ISMS.

The Committee is composed of:

- Chair of the committee
- Information Officer
- Service Owners
- System Owner
- Security Officer
- Data Protection Officer

The functions of the **Security Committee** are as follows:

- Drafting the Corporate Security Policy, which must be approved by the entity's Management.
- Coordinating all security functions within the organization.
- Ensuring compliance with applicable legal and sector-specific regulations.
- Ensuring that security activities are aligned with the organization's objectives.
- Coordinating the Business Continuity Plans of the different areas to ensure seamless action if they need to be activated.
- Coordinating and, where appropriate, approving project proposals received from the different security domains, managing oversight and regular reporting of project progress and announcing any deviations.
- Receiving security-related concerns from Management and conveying them to the relevant departmental managers, obtaining corresponding responses and solutions which, once coordinated, must be communicated back to Management.
- Requesting regular reports from departmental security managers regarding the status of the organization's security and possible incidents. These reports are consolidated and summarized for communication to Management.
- Defining, within the Corporate Security Policy, the assignment of roles and the criteria for achieving appropriate guarantees regarding segregation of duties.

There is a documentary repository of ENS and complementary measures, which are approved in Security Committee sessions and subsequently by Management (who signs the documents). Certain ISO 27001 documents may eventually form part of the ENS measures framework.

ENS measures are considered approved when they bear the signature of the General Director and the Information Security Officer and are uploaded to the documentary repository in Microsoft OneDrive or an alternative system. Minutes are not required. It is also contemplated that the General Director may carry out a general approval of measures in formal minutes indicating the name of the measure and the approved version.

Furthermore, the Management Committee, with the collaboration of external legal advisors where appropriate, reviews once a year changes in applicable legislation and their potential impact on the company's business within scope. This review is carried out primarily through consultations of the Spanish BOE, INCIBE, and CCN organizations.

The Committee may regularly request relevant information from internal or external technical staff to make decisions.

This Committee shall be convened when serious security incidents arise and specifically when new security needs emerge.

The Committee shall meet at least once a year on an ordinary basis and extraordinarily whenever necessary, with prior notice of at least three working days, issued by Management via email. The Committee may be requested by the Information Security Officer, in which case Management must convene it within a maximum period of 15 working days.

E - Guidelines for Structuring System Security Documentation, Its Management and Access

Documentation related to system security is organized and managed in accordance with the current internal guidelines.

If a substantial change occurs in the structure or operation that impacts this policy, a corresponding review and update shall be carried out.

These modifications shall be recorded in a new edition of the document and documented in the change control section. This will serve as evidence of the update process carried out and will allow tracking of the different versions.

The person responsible for Information Security is responsible for maintaining and sharing the approved version of this document both in the information security policy available on our website,

accessible to the public, and in the internal version available on the corporate intranet for all employees.

F - Risks Arising from the Processing of Personal Data.

Risk analysis and management must be considered as an essential part of the security process.

Risk management will contribute to maintaining a controlled environment by reducing risks to acceptable levels. To achieve this reduction, security measures will be implemented that balance the nature of the data and processes, the impact and likelihood of associated risks, together with the effectiveness and cost of such measures.

When assessing risks related to data security, particular attention shall be paid to risks arising from the processing of personal data, such as:

Risk of Unauthorized Access: The possibility that unauthorized persons may access personal data, which could result in a breach of confidentiality.

- Personal information could be modified or altered without authorization, threatening its integrity.
- Personal data could become inaccessible due to technical failures, cyberattacks, or other disruptions, affecting the availability of the information.
- The lack of adequate security measures could lead to security breaches, such as cyberattacks or the loss of devices containing personal data.
- Inadequate processing of personal data may result in non-compliance with data protection legislation, potentially leading to legal sanctions.
- Unauthorized disclosure of personal data could result in harmful information leaks.
- Employees or third parties could misuse personal data for unauthorized purposes.
- Granting unnecessary or excessive permission to access personal data may increase the risk of misuse.
- Vulnerabilities in software used for processing personal data may be exploited by malicious actors.
- The outsourcing of services involving personal data may entail risks if third parties do not comply with required security standards.

- A lack of early detection and an inadequate response to security incidents may aggravate the impact of personal data breach.

Currently, the personal data of employees of **Nazaríes Information Technologies, S.L.** is managed by Management and the Administration Department.

Employees of both departments have signed a confidentiality and non-disclosure agreement specifying what information must under no circumstances be disclosed during the term of the contract, as well as other provisions agreed upon by both parties.

The legal and regulatory framework under which the organization's activities are carried out has been identified (Cybersecurity Law Code, edition 02-04-2025).

With regard to client data, its management is carried out in accordance with the guidelines that (as with personal data) have been established in the confidentiality agreement signed between the employee and the company.

Specialized external advisory services are received to ensure compliance with data protection regulations.

Minimum Security Requirements (ES - Art. 12 ENS)

This security policy is developed by applying the following minimum requirements:

a) Organization and implementation of the security process.

Security involves the entire organization, with the relevant functions within the ISMS clearly defined in the Security Policy document itself.

b) Risk analysis and management.

Each year, a risk analysis is conducted following a methodology based on ISO 27005, resulting in a Risk Treatment Plan with measures tailored to the identified risks.

c) Personnel management.

Users who access the system are identified and are aware of the company's security regulations. There is an annual training plan for all personnel within scope. Additionally, freely available awareness tools provided by INCIBE are implemented.

d) Professionalism.

Personnel selection is carried out through interviews and a thorough review of the candidate's CV. Newly hired employees receive training on the company's ISMS upon joining, as well as periodic refresher actions.

System security shall be managed, reviewed, and audited by qualified, dedicated, and trained personnel at all stages of its lifecycle: installation, maintenance, incident management, and decommissioning.

e) Authorization and access control.

Access to the system is regulated by permissions, which are audited periodically. The granting and withdrawal of temporary permissions is also provided for.

f) Protection of facilities.

The company's facilities are located in an office building with restricted hours. The company's offices are equipped with RFID key access issued to each employee, with records maintained. There are no production servers or data storage servers located in the offices of **Nazaríes Information Technologies, S.L.**

Information systems shall be located in secure areas protected by physical access controls appropriate to their classification as critical services. Systems and the information assets they contain shall be adequately protected against physical or environmental threats, whether intentional or accidental. Servers hosting production applications or containing production data are housed in companies certified under the ENS at medium or high level.

g) Acquisition of security products and contracting security services.

The procurement of products and services shall prioritize those holding valid ENS certifications, preferably at medium or high categories, considering CCN-CERT specific certifications as a secondary criterion.

h) Least privilege.

The system shall provide the minimum functionality required for the organization to achieve its objectives. Operational, administrative, and activity logging functions shall be limited to what is strictly necessary, ensuring access only by authorized persons or from authorized locations or equipment, with possible time and access point restrictions if required. In production systems, unnecessary or inappropriate functions shall be removed or disabled through configuration control. Finally, ordinary system use must be simple and secure, so that insecure use requires a conscious act by the user.

i) System integrity and updating.

Any physical or logical component shall require formal authorization prior to installation in the system. The security status of systems must be known at all times in relation to manufacturer specifications, vulnerabilities, and applicable updates, responding diligently to manage risk according to their security status.

j) Protection of stored and transmitted information.

Equipment used is encrypted. The use of personal removable devices is not permitted. Paper information is limited to contracts, and printing or disposal of paper information is not allowed without authorization.

Nazaríes Information Technologies, S.L. has implemented mechanisms to protect information stored or transmitted, especially when located in insecure environments (laptops, mobile phones, tablets, storage media, open networks, etc.).

k) Protection against interconnected information systems.

The system protects its perimeter, particularly when connected to public networks. A public communications network is understood as an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public, in accordance with the definition established in section 32 of Annex II of Law 9/2014, of May 9, General Telecommunications Law. In any case, risks arising from system interconnection through networks with other systems shall be analyzed and their connection points controlled.

i) Activity logging and malicious code detection.

User activity is recorded and analyzed to identify and prevent unlawful actions or those likely to generate security risks.

m) Security incidents.

There is a procedure for the identification and management of security incidents. Employees are informed accordingly.

n) Business continuity.

Backup activities are outsourced to providers certified under the ENS at medium or high level.

ñ) Continuous improvement of the security process.

Periodically, every two years, the system is audited—both by internal technical staff and subsequently by an entity accredited by ENAC - CCN. In addition, security committees are regularly held to address the evolution of the Risk Treatment Plan, indicators, and other actions aimed at improving the ISMS.

The comprehensive security process implemented shall be continuously updated and improved. To this end, nationally and internationally recognized criteria and methods related to information technology management shall be applied.

Security Committee

Nazaríes Information Technologies, S.L.

Public Disclosure Notice:

This document has been prepared by **Nazaríes Information Technologies, S.L.** for general informational purposes. The information contained herein is provided in good faith and may be freely shared, reproduced, or distributed, provided that proper credit is given to **Nazaríes Information Technologies, S.L.** as the original source. While every effort has been made to ensure the accuracy of the information, **Nazaríes Information Technologies, S.L.** makes no warranties or representations regarding its completeness or reliability. The content of this document is subject to change without notice. ©2026