Corporate Information Security Policy

Approved by the Board of Directors
of El Corte Inglés, S.A.
on 30 November 2020

Version 3.0 (29 October 2025)

TABLE OF CONTENTS

NOTE: The definitions of the most frequently used terms in this document and in the related regulations of the Information Security Management System, as well as those of the EL CORTE INGLÉS Criminal Compliance Management System, are set out in **Annex 1**.

Annex 2 sets out the main standards and/or regulations related to this Policy in the field of information security.

1. INTRODUCTION

The Board of Directors of El Corte Inglés, S.A. is responsible for defining the Strategy and Corporate Policies of the companies within the El Corte Inglés Group (hereinafter referred to as the Group), as well as for approving compliance programmes and internal control systems.

Since its establishment, the information recorded, generated and managed within the Group has been considered one of its strategic assets and a key element for the sustainability and competitiveness of the Organisation. Accordingly, with the aim of establishing the general principles governing the processing of information across all Group companies, the Board of Directors, following a proposal by the Audit and Control Committee, has approved this Corporate Information Security Policy (hereinafter referred to as the Policy).

This Policy is aligned with the Group's values and reaffirms its strong commitment to contributing to the 17 United Nations Sustainable Development Goals, as well as to maintaining conduct that is respectful of the regulations applicable to its activities and of the ethical standards and other rules and initiatives to which the Group is committed through certification or adherence. These include, among others, UNE-ISO/IEC 27001:2023, the Spanish National Security Scheme (ENS), Directive (EU) 2022/2555 (NIS2) and the Payment Card Industry – Data Security Standard (PCI-DSS), as well as other regulatory frameworks and recognised best practices deemed relevant by the Group in the field of information security.

This Policy constitutes the foundation of the Information Security Management System (hereinafter, the ISMS), upon which the Organisation's information protection strategy and operational framework are based.

2. PURPOSE

The purpose of this Policy is to establish the principles governing Information Security management in the interests of the companies comprising the Group, with a view to laying the foundations for preserving the confidentiality, integrity, availability, authenticity and traceability of the Group's information.

The application of these principles shall enable the Organisation to:

- define appropriate roles and responsibilities;
- control and manage information security risks;
- ensure business continuity;
- comply with applicable legislation;
- safeguard its commercial reputation; and
- manage and monitor relationships with third parties and/or stakeholders.

3. SCOPE OF APPLICATION

This Policy is mandatory and applies globally to all companies comprising the Group, as well as to employees, collaborators and third parties who manage Group information in any format or medium, across all activities related to the value chain, both upstream and downstream, regardless of the country in which such activities are carried out, and to the relevant stakeholder groups concerned.

All Members of the Organisation, particularly those involved in the value chain, are required to comply with the provisions of this Policy, irrespective of their position or the territory from which they operate. This Policy also applies to Business Partners when carrying out their activities within the Group, as well as to all workers involved in the value chain and other stakeholders participating in it.

This commitment shall be formalised as set out in Section 8, 'Awareness and Statement of Compliance', of this Policy.

Furthermore, this Policy applies to risks arising from threats and vulnerabilities affecting the Group's information and communication systems, including any outsourced assets used to carry out operations and/or provide services, as well as to risks associated with the processing of personal data, which are identified, assessed and managed on an ongoing basis throughout the entire data processing lifecycle.

4. PRINCIPLES OF ACTION

The El Corte Inglés Group expects all Members of the Organisation, as well as its Business Partners and other parties identified in Section 3, 'Scope of Application', to comply with the following principles of action in relation to Information Security, which underpin the effective protection of the Group's assets and information:

Principle 1. Compliance with Laws and Regulations.

The Group ensures compliance, at all times, with applicable national and international laws and regulations on Information Security in the territories in which it operates, particularly those relating to personal data protection, system security, accessibility, electronic communications and electronic services.

Principle 2. Implementation of Risk- and Efficiency-Based Information Security Measures.

The Group applies risk- and efficiency-based criteria when defining and implementing security measures to protect information assets and systems, and to prevent fraudulent activities and attacks that could compromise the integrity or reputation of the Organisation.

The control procedures applied by the Group may include, among other measures, the storage and verification of messages, transactions or communications through access to their content, including attachments or links, in order to ensure the confidentiality, availability, integrity, authenticity and traceability of information. As a result, such communications fall outside the scope of personal confidentiality and privacy, and Members of the Organisation must inform the relevant interlocutors accordingly.

Members of the Organisation shall not install any software or software versions on equipment or systems made available by the Group that have not been approved through El Corte Inglés, S.A.'s corporate procurement and service contracting processes. This prohibition includes, in particular, conversational, productivity and/or coding artificial intelligence tools involving corporate data, unless expressly authorised in advance.

Principle 3. Information Security Culture.

The objective of the Information Security culture is to establish a shared set of beliefs, behaviours and practices among users regarding the handling of information, in order to preserve its confidentiality, integrity and availability.

To this end, the Group carries out awareness-raising, training and skills development activities, ensuring the appropriate qualification of all internal and external personnel.

Principle 4. Effective Response to Information Security Incidents.

The Group has established mechanisms for the detection of and response to Information Security incidents that may compromise its information systems or assets, with the aim of responding effectively, minimising impacts on the Organisation and other stakeholders, and reducing recovery times.

For this purpose, the Group maintains collaborative relationships with the competent authorities and bodies responsible for Information Security, in order to ensure regulatory compliance and effective incident response.

Such relationships shall be established in accordance with applicable internal regulations.

Principle 5. Information Security Across the Value Chain

The Group extends these principles to suppliers and other stakeholders as part of its Information Security risk management.

Accordingly, in supplier contracting processes, it must be ensured that the requirements arising from internal regulations applicable to suppliers are duly incorporated, both contractually and through appropriate training.

Principle 6. Responsible Use of Information Systems

All Members of the Organisation and other users of the Group's information systems and IT equipment shall make exclusively professional use of such systems and equipment.

For this purpose, and in order to verify compliance with this Policy and other internal regulations, the Group may monitor internet access and messages, transactions or communications, including any attachments or links, sent or received through the systems and equipment accessed under the user's credentials.

Likewise, the use of work tools made available by the Organisation does not form part of the users' private sphere.

These principles are linked to the management of the specific impacts, risks and opportunities identified in the Purpose of the Policy section of this document. Their application is carried out through an Information Security Management System (ISMS), which is articulated within an organisational structure responsible for its governance, management and operation. For its proper functioning, the ISMS is based on four key components: Information Security Strategy, Information Security Control Framework, Information Security Regulatory Framework and the Information Security Scorecard.

5. ORGANISATIONAL STRUCTURE

The Group's ISMS establishes an organisational structure based on three fundamental pillars: Information Security Governance, Management and Operations.

5.1 Information Security Governance

As a foundation for governance, the Group has established three committees responsible for supervising and monitoring all aspects of Information Security at their respective levels of responsibility, coordination and operation:

- **CSI (Information Security Committee):** a multidisciplinary committee that meets on a regular basis and is responsible for promoting and supervising Information Security across the Organisation, ensuring that good security management practices are applied holistically, effectively and consistently.
- **SCSI (Information Security Subcommittee):** a multidisciplinary committee that meets regularly and is responsible for ensuring the execution and compliance of the Information Security activities promoted and supervised by the CSI.
- **CODES (Delegated Information Security Committee)**: the committee responsible for the operational management and implementation of the Group's Information Security Control Framework.

Effective communication among these three governance committees is ensured, allowing issues to be escalated and addressed in a structured and organised manner. This guarantees that decisions and actions are taken with the necessary coordination, enabling Information Security objectives to be addressed comprehensively and efficiently across the Organisation.

The operation of these committees is governed by their respective internal regulations.

5.2 Information Security Management and Operation

Under the supervision of the above-mentioned committees, Information Security Management and Operation is structured around five functional Information Security management areas, supported by a cross-functional Operations area. In this context, the Information Security and Cybersecurity Department, headed by the Information Security and Cybersecurity Officer (RSIC), leads, coordinates and supervises these functions.

- **Information Security and Cybersecurity Officer (RSIC)**: responsible for leading Information Security management.
- **Information Security Management Areas**: responsible for articulating the different Information Security capabilities, including Governance, Risk and Compliance; Protection; Detection; Response; and Security by Design.
- **Security Operations Centre (COS):** the cross-functional area responsible for providing operational support to the Information Security and Cybersecurity Department.

6. ISMS COMPONENTS

For the effective application of the ISMS, the Group has defined four fundamental components:

- **Information Security Strategy:** Information Security Strategy: a high-level approach defined by the Group to ensure the proper management of Information Security risks through a set of strategic initiatives aimed at their mitigation.
- **Information Security Control Framework:** the framework that underpins both the Information Security strategy and operational security activities, based on the requirements set out in applicable regulations, reference frameworks and recognised best practices relevant to the Group.
- **Information Security Regulatory Framework:** a set of policies, standards and general and specific procedures that cover the requirements identified in the Control Framework and applicable regulations.
- **Information Security Scorecard:** a tool used to measure and evaluate the performance of Information Security-related actions and processes across the Group.

These four components are maintained and updated by the Information Security and Cybersecurity Department in accordance with the Organisation's context and needs.

7. DUE DILIGENCE

Due diligence processes refer to the management and monitoring of relationships with third parties, whether suppliers, customers, business partners or any other third party with whom a contractual relationship exists and who have, or may potentially have, access to the Organisation's sensitive information.

The third-party due diligence process is based on the following pillars:

- Before entering into a relationship with a third party, the impact of the agreement on Information Security shall be assessed and, where such impact exists, the corresponding risk analysis shall be carried out.
- The Organisation shall establish a standardised and systematic framework of controls and measures to manage the Information Security risks associated with collaboration with or the engagement of third parties.
- The third party shall be contractually required to comply with the Information Security Policy and to implement the technical and organisational measures necessary to ensure the adequate protection of the Organisation's information assets.
- On a periodic basis, and depending on the level of risk associated with the agreement, monitoring and audit processes shall be carried out to ensure that the third party maintains a security ecosystem equivalent to that contractually committed.
- Upon termination of the contractual relationship, the Organisation shall ensure the return of assets, the destruction of information and the revocation of the third party's access to information.

8. AWARENESS AND STATEMENT OF COMPLIANCE

Compliance with ethical rules and standards represents both a corporate commitment and a strategic objective for the Organisation. Therefore, all Members of the Organisation are expected to be familiar with and adhere to the contents of this Policy. Likewise, all Business Partners are expected to act in accordance with its principles.

This commitment shall be formalised through:

i. Statements of compliance with the principles set out herein by Members of the Organisation, through their adherence to the **High Ethical Standards.**

ii. **Compliance clauses included in contracts** with Business Partners

iii. **Formal agreements or acknowledgement** by the governing bodies of the companies within the El Corte Inglés Group, in accordance with applicable internal regulations.

Such agreements and their renewals shall be notified to the El Corte Inglés Group's Compliance and Risk Control Department.

In the event of significant changes to this Policy (i.e. changes that require formal approval from the Board of Directors of El Corte Inglés, S.A.), the preceding commitments shall be formally renewed.

As compliance with ethical rules and standards is a corporate commitment and a strategic goal for the Organisation, all Members of the Organisation are expected to know and respect the contents of this Policy. Likewise, all Business Partners are expected to act in accordance with its principles.

The Organisation shall respond promptly to any breach of the provisions set out in this Policy, in accordance with its internal regulations and in compliance with all applicable legislation.

9. REPORTING OF NON-COMPLIANCE

9.1 Non-Compliance with Information Security Regulations

Any Member of the Organisation, Business Partner or Third Party with a direct relationship and legitimate commercial or professional interest, or any other interested party, who becomes aware of a breach of this Policy or who has doubts as to whether an observed practice may constitute an unlawful act, whether in the public or private sector, shall immediately contact the Compliance and Risk Control Department of the El Corte Inglés Group. This shall be done via the Ethics Channel, using any of the available means of communication:

- **Digital Channel:**

  The El Corte Inglés Group's digital channel can be accessed via the following website:

  https://www.elcorteingles.es/informacioncorporativa/es/gobierno-corporativo/etica- and-compliance/

  This access is available on the corporate website and additionally on the NEXO intranet for Members of the Organisation.

- **Postal address:**

  El Corte Inglés, S.A.
  Compliance and Risk Control
  Hermosilla, 112
  28009 Madrid

- **Compliance and Risk Control Department – Phone number:** 91 401 85 00

- **Request for a face-to-face or remote meeting**

The information communicated through this Channel is confidential, as is the identity of reporting persons acting in good faith, whose cooperation the Organisation appreciates and in respect of whom it guarantees the absence of retaliation of any kind.

In addition, the Compliance and Risk Control Department may act on its own initiative by investigating any indication of non-compliance with this Policy.

9.2 Reporting of Information security incidents

Any Member of the Organisation, Business Partner or Third Party with a direct relationship and legitimate commercial or professional interest who identifies a security event that could result in an incident affecting the Group's information systems shall immediately contact the Security Operations Centre (COS) of the El Corte Inglés Group through the following communication channels:

- **Mailbox:**

  The Security Operations Centre (COS) of the El Corte Inglés Group has the following mailbox:

  cos_notificaciones@elcorteingles.es

- **COS Phone number:** 636 10 27 32 (78570)

10. APPROVAL, EFFECTIVE DATE AND UPDATING

This Policy shall become effective on the date of its approval by the Board of Directors of El Corte Inglés, S.A.

This Policy shall be kept up to date over time. To this end, it shall be reviewed regularly, on an annual basis, and on an extraordinary basis where necessary, and in any event as promptly as possible in the event of changes to the Group's strategic objectives or to internal or external regulatory requirements that require its update or amendment.

Any proposed amendments shall be submitted to the Audit and Control Committee by the Information Security Committee, following prior validation by the Legal Advisory Department and the Compliance and Risk Control Department, and with the corresponding supervision by the internal control body entrusted with this function.

Where such changes are significant, they shall be submitted for approval to the Board of Directors, following a proposal from the Audit and Control Committee.

11. DISSEMINATION AND IMPLEMENTATION

Once approved by the Board of Directors of El Corte Inglés, S.A., this Policy shall be made available on NEXO for all Members of the Organisation and on the corporate website for all ECI Group stakeholders.

Likewise, the Information Security Committee shall be responsible for promoting the actions necessary to ensure the appropriate dissemination of and awareness of this Policy.

12. CONTROL, MONITORING AND SUPERVISION

12.1 Control and Monitoring

The Sub-Committee on Information Security shall periodically assess compliance with and the effectiveness of this Policy through internal and external reviews, controls and audits coordinated by the Information Security and Cybersecurity Department, and shall report the results to the Information Security Committee.

The Information Security Committee shall be responsible for the ongoing supervision of the implementation of the provisions of this Policy by the Group companies.

12.2 Supervision

The Internal Audit Function shall review the adequacy and effectiveness of the measures implemented within the ISMS to supervise compliance with the regulations applicable to the different activities of the Organisation, to the extent that the Annual Audit Plan approved by the Audit and Control Committee includes work related to this System, and, on an extraordinary basis, as a result of the occurrence of incidents or the identification of irregularities. As a result of such audits, the Internal Audit Function shall issue the corresponding report, including recommendations where opportunities for improvement are identified.

Any opportunities for improvement that may be identified as a result of these reviews shall be considered as part of the continuous improvement process of the System.

The assessment of any potential breach of the Corporate Information Security Policy shall be determined in accordance with the applicable procedure and the provisions in force, without prejudice to any legal responsibilities, including disciplinary measures in the employment sphere, that may be applicable to the infringing party.

VERSION HISTORY

Version 3.0 approved by the Board of Directors on 29/Oct/2025

Version	Date of amendment	Purpose of the amendment	Sections affected
1.1	28/Jun/2023	- Include communication channels	Reporting of Non-Compliance
2.0	30/Oct/2024	- Adapt to the new strategic and regulatory framework - Align Policy with the requirements of the Corporate Sustainability Reporting Directive. - Include Due diligence process. - Include a reference to the new internal rules governing the Group companies' compliance with the Corporate Policies. - Update digital channels for reporting non-compliance. - Include 'Dissemination' section	- All
3.0	29/Oct/2025	- Align with the requirements of the National Security Scheme - Incorporate an addendum for verification of compliance with the National Security Scheme.	- All

Last revision, 29 October 2025

Annexes

Annex 1 - Definitions

Below are the definitions of the terms most frequently used in this document.

Authenticity: The property or characteristic whereby an entity is who it claims to be, or which guarantees the source from which the data originates.

Availability: The ability of a service, system or process to be accessible and usable by authorised users or processes when required.

Confidentiality: The protection of data and systems to prevent threats such as unauthorised access or data leakage, which could result in the disclosure, alteration or destruction of sensitive information.

Information Asset: Any information or information processing system that has value for the organisation, including business processes, data, applications, IT equipment, personnel, information media, networks, auxiliary equipment or facilities.

Information Security: The set of technologies, practices and measures designed to protect the confidentiality, integrity and availability of information.

Information Security Policy: A high-level executive document through which a company establishes its guidelines, decisions and security measures regarding the protection of its information systems, following an assessment of the value of its assets and the risks to which they are exposed.

Integrity: The property of information that guarantees the accuracy of data during transmission or storage, ensuring that it has not been altered or lost.

Resilience: The ability of an organisation to build, ensure and review its operational integrity and reliability in order to sustain the continuous delivery of services.

Risk: The possibility that incidents or events may occur that compromise the confidentiality, integrity or availability of the Organisation's data and systems.

Security Incident: Any event that affects the confidentiality, integrity or availability of the company's information assets, including unauthorised or attempted access to systems, or the unauthorised use, disclosure, modification or destruction of information.

Threat: An unfavourable circumstance that may occur and which, if it materialises, has negative consequences for assets or resources, causing their unavailability, malfunction or loss of value.

Traceability: The property or characteristic whereby the actions of an entity (person or process) can be unequivocally traced back to that entity.

Annex 2 - Related Regulation and Standards

The following are the main regulations and standards related to this document:

- Royal Decree 311/2022, of 3 May, regulating the Spanish National Security Scheme (*Esquema Nacional de Seguridad* – ENS).
- Directive (EU) 2022/2555 (NIS2) on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS Directive).
- Organic Law 3/2018, of 5 December, on Personal Data Protection and the Guarantee of Digital Rights (LOPDGDD).
- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation – GDPR).
- Royal Legislative Decree 1/1996, of 12 April, approving the consolidated text of the Intellectual Property Law, regulating, clarifying and harmonising the legal provisions in force in this field.
- Law 1/2019, of 20 February, on Trade Secrets.
- Law 5/2014, of 4 April, on Private Security.
- Copyright and Related Rights Code (Decree-Law 63/85).
- Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce (LSSICE).
- Law No. 27/2021, of 17 May (Portugal) – Portuguese Charter of Human Rights in the Digital Era.
- Law No. 58/2019, of 8 August (Portugal) – Portuguese national implementation of the GDPR.
- Decree-Law No. 65/2021, of 30 July (Portugal).
- Law No. 109/2009, of 15 September (Portugal) – Portuguese Cybercrime Law.

Annex 3 – Assurance of Compliance with the National Security Scheme (ENS)

As a supplement to the Corporate Information Security Policy currently in force for the companies of the El Corte Inglés Group (hereinafter, the Group), this addendum aims to ensure compliance with and to explicitly articulate the requirements, roles, responsibilities and key organisational structures relating to information security, in strict alignment with Royal Decree 311/2022, of 3 May, regulating the National Security Scheme (ENS).

This addendum has been developed taking into account the guidelines issued by the National Cryptologic Centre (CCN), in particular *CCN-STIC-805 Guidelines*, *Information Security Policy, and CCN-STIC-801, Responsibilities and Functions*, among others.

A. Review of the Corporate Information Security Policy in accordance with the requirements of Royal Decree 311/2022, regulating the National Security Scheme (ENS).

The current Corporate Information Security Policy has been formally approved by the Board of Directors of El Corte Inglés, S.A., which is responsible for defining the Group's strategy and corporate policies, as well as for approving compliance programmes and internal control systems. This institutional endorsement provides the Policy with a solid foundation of governance, legitimacy and strategic coherence.

The Policy has been developed in accordance with the guidelines of UNE-ISO/IEC 27001:2023 and, through the drafting and approval of this addendum, ensures compliance with the requirements set out in *Chapter III of the ENS, which establishes the Security Policy and the minimum requirements necessary to provide adequate protection of information and services.* ENS Requirements (Articles 12 to 27):

a. *Organisation and implementation of the security process.*
b. *Risk analysis and management.*
c. *Personnel management.*
d. *Professional competence.*
e. *Access authorisation and control.*
f. *Protection of facilities.*
g. *Acquisition of security products and contracting of security services.*
h. *Principle of least privilege.*
i. *System integrity and updating.*
j. *Protection of stored and transmitted information.*
k. *Prevention in relation to interconnected information systems.*
l. *Activity logging and malware detection.*
m. *Security incidents.*
n. *Business continuity.*
o. *Continuous improvement of the security process.*

The Group has a Corporate Information Security Regulatory Framework that complements the Corporate Information Security Policy, ensuring full compliance with ENS requirements and establishing mechanisms to support ongoing review and continuous improvement.

Corporate Regulatory Framework Policies and Standards Ensuring ENS Compliance:

- Corporate Data Protection Policy
- Corporate Cyber-Resilience Policy
- Corporate Information Security Governance Standard
- Corporate Asset Management Standard
- Corporate Information Protection Standard
- Corporate Information Security in HR Management Standard
- Corporate Physical and Environmental Security Standard
- Corporate Operations and Infrastructure Security Standard
- Corporate Secure Application Development Standard
- Corporate Secure Configuration Standard
- Corporate Identity and Access Management Standard
- Corporate Threat and Vulnerability Management Standard
- Corporate IT Business Continuity Standard
- Corporate Supplier Relationship Security Standard
- Corporate Regulatory and Compliance Management Standard
- Corporate Information Security Event Management Standard
- Corporate Information Security Assurance Standard

B. Mapping of Information Security Policy Requirements

As part of the review of CCN-STIC-805 – Information Security Policy, a mapping exercise has been conducted between its content and the provisions of the Group's Corporate Information Security Policy. Below is the correspondence:

(References from CCN-STIC-805 appear in bold, and the corresponding sections of the Corporate Policy are shown in italics):

- **Mission or organisational objectives**
  - *Purpose*
  - *Scope of Application*
- **Policy principles**
  - *Principles of Action*
- **Regulatory Framework**
  - *Annex 2*
- **Security organization**
  - Organisational Structure

Note: Section C. ENS Roles and Responsibilities of this addendum establishes the relationship between the Group's Information Security Governance roles and the requirements of *Article 11* of the ENS. *Differentiation of responsibilities* in accordance with Royal Decree 311/2022. It also specifies the complementary responsibilities assigned to each role to ensure compliance.

- **Guidelines for structuring, managing and accessing security documentation**
  - *ISMS Components*

- **Awareness and training**
  - *Principles of Action (Principle 3 – Information Security Culture)*
- **Risk management**
  - *Scope of Application*
  - *Due Diligence*
  - *Reporting of Non-Compliance. Reporting of Information Security Incidents*
- **Security policy review process**
  - *Approval, Effective Date and Updating*
- **Staff obligations**
  - *Awareness and Statement of Compliance*
  - *Reporting of Non-Compliance*
- **Third parties / service providers**
  - *Due Diligence*

C. ENS Roles and Responsibilities

As established in section 5. *Organisational Structure of the Corporate Information Security Policy,* the Information Security Management System (ISMS) is structured around **three core pillars: Governance, Management and Operation.**

The Governance pillar is made up of the committees listed below, detailing the relationship of each committee's role with respect to the ENS. It also specifies the additional responsibilities that have been deemed necessary to incorporate to ensure compliance with the ENS in the Group.

- **Information Security Committee (CSI)**
  ENS Role: Information Owner

  For the purposes of compliance with the ENS, the following responsibilities are added to those of the CSI:

  - Ultimate responsibility for the use made of the information and, consequently, for its protection.
  - Authority to establish the information security requirements. Or, using ENS terminology, the authority to determine the security levels applicable to the information.

- **Sub-Committee on Information Security (SCSI)**
  ENS role: Service Owner

  For the purposes of compliance with the ENS, the following responsibilities are added to those of the SCSI:

  - In its capacity as Service Owner, the SCSI shall be the owner of the risks relating to the services.
  - Its main function shall be to establish the security requirements applicable to the services. Or, using ENS terminology, the authority to determine the security levels applicable to the services.

- **Delegated Information Security Committee (CODES)**
  ENS Role: System Owner

  For this role, no additional or supplementary responsibilities have been identified in relation to compliance with the ENS. The functions currently assigned already encompass the requirements established by the ENS for the role of System Owner.

- **Information Security and Cybersecurity Officer (RSIC)**
  ENS Role: Security Officer

  For the purposes of compliance with the ENS, the following responsibilities are added to those of the RSIC:

  - To determine the applicable security measures, based on the assessments carried out by the CSI, in its capacity as Information Owner, and by the SCSI, in its capacity as Service Owner.
  - To prepare and approve the Statement of Applicability, taking into account the requirements established by the CSI, as Information Owner, and by the SCSI, as Service Owner.
  - To analyse risks prior to the deployment of artificial intelligence systems within the entity, taking into account the assessments carried out by the CSI, as Information Owner, and the SCSI, as Service Owner, and, where applicable, by the Data Protection Officer, and to supervise such deployment.

Note: The detailed composition of the committees—*including ENS role mappings, responsibilities, members, appointment procedures and conflict-resolution mechanisms—is set out in the Corporate Information Security Governance Standard* and in the specific operating regulations of each committee.