INFORMATION SECURITY POLICY

Ineco, a leading engineering and consultancy company in sustainable mobility and digital transformation, reaffirms its strong commitment to ensuring information security throughout all its processes. This document serves as the reference framework for that **commitment**, which applies to all phases of the information life cycle (generation, distribution, storage, processing, transport, consultation and destruction), as well as to the information systems that support it. It encompasses all assets, processes, services and technologies involved in handling information, regardless of format or location, and covers both internal staff and third parties who access or manage information on Ineco's behalf.

MISSION

Ineco is responsible for powers and functions established in the organization's own articles of association, as well as those arising from its relationship with other companies, legal entities, public administrations or natural persons.

SCOPE

The scope of this information security policy is established in compliance with ENS and ISO 27001, defined as:

"*Information systems that support the services which make up Ineco's product catalogue*:

- *Smart Administration*
- *Smart Products*
- *ERTMS*
- *Consultancy*
- *Projects*
- *Works*
- *Operation*
- *Maintenance*
- *R+D+I*
- *ORAT*
- *Rolling Stock*
- *BIM*
- *Project Management*

according to the current Statement of Applicability "

REGULATORY FRAMEWORK

This policy has been developed in accordance with the current legal framework on information security, including the National Security Scheme (Royal Decree 311/2022 of 3 May), hereinafter referred to as NSS, the General Data Protection Regulation (GDPR) and other applicable regulations established in the document integrated into our management system.

INFORMATION SECURITY PRINCIPLES

The Information Security Policy applies the basic principles established in the ENS and ISO 27001 standard, in accordance with the general interest, nature and complexity of the regulated matter, allowing for adequate protection of information and services.

In accordance with the ENS and ISO 27001, Ineco implements several security measures proportional to the nature of the information and services to be protected, taking into account the category of the affected systems, under the following principles:

Security as an integrated process

Information security at Ineco must have the commitment and support of all management levels, so that it can be coordinated and integrated with the rest of the organisation's strategic initiatives to form a coherent and effective whole. Security is an integral process comprising all the technical, human, material and organisational elements related to the system, based on the continuous improvement of all these elements and the process itself.

Maximum attention must be paid to the training and awareness of the people involved in the process and those in positions of responsibility, in order to prevent ignorance, lack of organisation and coordination or inadequate instructions from becoming sources of security risk.

Prevention, detection, response and conservation

Ineco implements a comprehensive process for the prevention, detection, response and preservation of security incidents with procedures for detection, analysis, communication, resolution and recording of actions for the continuous improvement of system security, designating a point of contact for communications regarding detected incidents and establishing protocols for the exchange of information related to the incident, including communications with Computer Emergency Response Teams (CERT).

Defence lines

Ineco implements a protection strategy based on multiple layers, constituted by organizational, physical and logical measures in such a manner that, when one of the layers fails, the system automatically allows for the following:

- gain time for an appropriate response to incidents that could not be prevented;
- reduce the likelihood of the system as a whole being compromised; and
- minimise the final impact on the system

Continuous surveillance

Continuous surveillance requires the monitoring of activity logs. Only information strictly necessary for the investigation of improper or unauthorised activities that allows the person responsible for the activity to be identified will be recorded.

Periodic reassessment

Ineco implements regular and periodic security controls and assessments, either internally or with the help of third parties, in order to be aware of the security status of its systems at all times and to adapt their effectiveness to the constant evolution of risks and protection systems.

Separation of duties

Security is organized by involving all Ineco's members through the designation of different security roles with clearly differentiated duties.

At least the following positions shall be appointed: information manager, service manager, security manager, and system manager, with security responsibilities being distinct from system operation responsibilities.

ROLES AND COMMITTEES

In the context of information security, Ineco has defined the following roles and committees:

Information Security and Risk Committee

The Information Security and Risk Committee has been created for the Information Security Management and it consists of a multidisciplinary team that will coordinate the security activities and controls established at Ineco and ensure compliance with current internal and external regulations on personal data protection and security.

The functions of the Information Security and Risk Committee are as follows:

- Develop and regularly review the Information Security Policy, which must be approved by Ineco's management.
- Define, within the Information Security Policy, the assignment of roles and criteria for achieving the relevant guarantees regarding separation of duties.
- Resolve any conflicts of responsibility that may arise between different managers and/or between different areas of the organisation, referring them to senior management in cases where it does not have sufficient authority to decide.
- Approve the regulatory framework and technical measures to be implemented in accordance with the Information Security Master Plan (ISMP).
- Coordinate all security functions within the organisation.
- Ensure compliance with applicable legal and sectoral regulations.
- Ensure that security activities are aligned with the organisation's objectives.
- Coordinate different areas' Continuity Plans in order to ensure seamless performance in the event that they need to be activated.
- Receive security concerns from management and forward them to the relevant department heads, obtaining the corresponding responses and solutions from them, which, once coordinated, must be communicated to management.
- Obtain, through the Security Manager, regular reports on the state of the organisation's security and any incidents, in order to be able to take the appropriate decisions.
- Promote continuous improvement of the information security management system (ISMS).
- Develop the organisation's strategy for the evolution of information security.
- Coordinate the efforts of the different areas in terms of information security, to ensure that efforts are consistent, aligned with the strategy decided upon in this area, and avoid duplication.
- Supervise and approve information security risk management, the Risk Treatment Plan (RTP) and the main residual risks assumed by the organisation, recommending possible actions to the Management.
- Through the Security Manager, monitor the performance of security incident management processes and recommend possible actions in relation to them.
- Promote the performance of periodic audits to verify compliance with the organisation's security obligations.
- Approve plans to improve the organisation's information security. In particular, ensure the coordination of different plans that may be carried out in different areas.
- Prioritise security actions when resources are limited.
- Ensure that information security is taken into account in all projects from their initial specification to their implementation.

This Committee identifies objectives and strategies related to information security and directs and controls security-related processes. Its composition shall consist of persons holding the following positions:

Secretary: Corresponds to the Secretary of the Information Security and Risk Committee.

- Convene meetings of the Information Security and Risk Committee
- Prepare the topics to be discussed at Committee meetings, providing timely information for decision-making.
- Prepare the minutes of the meetings.
- Responsibility for the direct or delegated execution of the Committee's decisions.
- Communicate the decisions taken by the Committee to the different persons responsible for their execution.
- Sign ISMS documents approved collectively by the Committee, on behalf of the Committee.

Members: Corresponds to the members of the Information Security and Risk Committee

- Participate in meetings.
- Contribute ideas and suggestions for the smooth running of meetings.

The Committee's decisions shall be agreed upon by all participants. All members of the Committee shall act independently and shall not be obliged to act or vote in accordance with other members of the Committee.

The Committee shall meet periodically, at least once a year, to validate and review all the above points.

ROLES AND DUTIES

Each year, management will appoint several security positions and present them at the meeting of the Information Security and Risk Committee. If no new appointments are made, the current positions will be understood to be renewed for a period of one year, with no maximum term, subject to the needs of the company.

The Information Security and Risk Committee shall formally appoint different responsible roles by means of minutes.

Their functions are as follows.

Service Manager

They have the authority to establish service requirements in terms of security or, in ENS terminology, the authority to determine service security levels. Although formal approval of the levels is the responsibility of the Service Manager, a proposal may be sought from the Security Manager, and it is advisable to listen to the opinion of the System Manager.

The Service Manager must consider that the provision of a service must always meet the security requirements of the information it handles, so that the security requirements of the information can be inherited, adding availability requirements, as well as others such as accessibility, interoperability, etc.

Accept the residual risk associated with the services for which they are responsible, obtained after carrying out the risk analysis.

Manage the processing of personal data and its treatment in accordance with the instructions of the DPO.

Delegation of duties

If, due to complexity, distribution, physical separation or number of users, additional staff are required to carry out the duties of Service Manager, as many Deputy Service Managers as deemed necessary may be appointed.

The appointment is made by the Service Manager, who delegates functions by appointing delegates, with ultimate responsibility remaining with the Service Manager.

The delegates shall be responsible, within their scope, for all actions delegated by the Service Manager in relation to their role.

Information Manager

The Information Manager is responsible for establishing information security requirements. They are also responsible for determining the levels of information security in each dimension (confidentiality, integrity, authenticity, traceability and availability) within the framework established in Annex I of the ENS. Although formal approval of the levels is the responsibility of the Information Manager, they may seek a proposal from the Security Manager and should listen to the opinion of the System Manager.

They must adopt or request the adoption of the necessary technical and organisational measures to guarantee the security of personal data and prevent its alteration, loss, unauthorised processing or access, taking into account the state of technology, the nature of the data stored and the risks to which it is exposed, whether from human action or from the physical or natural environment, always following the instructions of the DPO.

They have ultimate responsibility for the use made of certain information and, therefore, for its protection.

Delegation of duties

If, due to complexity, distribution, physical separation or number of users, additional personnel are required to perform the duties of Information Manager, as many Information Managers as deemed necessary may be appointed.

The appointment is made by the Information Manager, who delegates functions by appointing deputies, but the final responsibility remains with the Information Manager.

The deputies shall be responsible, within their scope, for all actions delegated by the Information Manager in relation to their role.

Security Manager

They shall be responsible for making the appropriate decisions to meet information and service security requirements, maintaining the security of the information handled and the services provided by the information systems within their area of responsibility, compiling the security requirements of the Information and Service Managers, and determining the category of the System.

It is also their responsibility to carry out the Information Risk Analysis. To this end:

- They will provide Information and Service Managers with information on the expected residual risk level after implementing the treatment options selected in the risk analysis and the security measures required by the ENS.
- They shall prepare the Statement of Applicability based on the security measures required in accordance with Annex II of the ENS and the control requirements of ISO 27001, as well as the results of the Risk Analysis.
- Together with the System Manager, it will draw up Security Improvement Plans for approval by the Information Security and Risk Committee.
- It will monitor the main residual risks assumed by the Organisation and recommend possible actions to be taken in relation to them.

In addition, they will be responsible for:

- Validating the System Continuity Plans drawn up by the System Manager, which must be approved by the Information Security and Risk Committee and tested periodically to ensure their suitability.
- Promoting training and awareness in the area of Information Security within their area of responsibility.
- Approving the guidelines proposed by the System Manager to consider Information Security throughout the entire life cycle of assets and processes: specification, architecture, development, operation and changes.
- Prepare the annual report on the state of Information Security, with the progress of the improvement plan projects, a summary of security actions, incidents related to Information Security, the state of system security, and in particular the level of residual risk to which the system is exposed.

- Monitor the performance of security incident management processes and recommend possible actions in relation to them. In particular, ensure the coordination of the different security areas in the management of Information Security incidents.
- Advise area managers on the determination of the necessary security measures based on the security requirements established by Ineco's internal and external context.
- Periodically provide the Information Security and Risk Committee with a summary of security actions, incidents related to information security and the state of system security.

They will also act as secretary within the Information Security and Risk Committee.

Delegation of duties

If, due to complexity, distribution, physical separation of elements, or number of users, additional personnel are required to carry out the duties of the Security Manager, as many Deputy Security Managers as deemed necessary may be appointed.

The appointment is made by the Security Manager, who delegates duties to deputies, but ultimate responsibility remains with the Security Manager.

The deputies shall be responsible, within their scope, for all actions delegated by the Security Manager. They are usually responsible for the security of specific information systems or horizontal information systems.

Each deputy shall report directly to the Security Manager, to whom they are accountable.

System Manager

They are responsible for operating the information system.

They will be responsible for managing Ineco's information system, including:

- Develop, operate, and maintain the Information System throughout the entire life cycle, including its specifications, installation, and verification of its correct operation.
- Ensure that specific security measures are properly integrated into the overall security framework.
- Agree to suspend the handling of certain information or the provision of a certain service if serious security deficiencies are reported that could affect the fulfilment of the established requirements. This decision must be agreed with those responsible for the affected information, the affected service and the Security Manager before being implemented.

They will establish guidelines and measures for action, taking responsibility for:

- Define the topology and management of the Information System, establishing the criteria for use and the services available therein.
- Define the policy for connecting or disconnecting new equipment and users to the System.
- Decide on the security measures to be applied by the System component suppliers during the development, installation and testing stages.
- Determine the authorised hardware and software configuration to be used in the System.
- Define the responsibilities of each entity involved in the maintenance, operation, implementation and supervision of the System.
- Develop security procedures.
- Establish contingency and emergency plans, conducting frequent exercises to familiarise staff with them.
- Approve changes that affect the security of the System's mode of operation.

- Approve any substantial modification to the configuration of any element of the System.
- Monitor the security status of the Information System and report it periodically or in the event of relevant security incidents to the Information Security Manager.

The System Manager shall act autonomously and shall not be obliged to act under the influence of the Security Manager beyond the latter's supervisory functions, derived from the role he or she performs. Similarly, he or she shall have independence in his or her decisions and voting in the Security Committee, being independent from the Security Manager.

Delegation of duties

If, due to its complexity, distribution, physical separation of its elements or number of users, additional personnel are needed to carry out the functions of System Manager, as many Deputy System Managers as deemed necessary may be appointed.

The appointment is made by the System Manager, who delegates functions by appointing delegates, but the final responsibility remains with the System Manager.

The delegates shall be responsible, within their scope, for all actions delegated by the System Manager relating to the operation, maintenance, installation and verification of the correct functioning of the information system.

Data Protection Officer

The Data Protection Officer shall have the following duties with regard to the responsibilities defined in the ENS:

- Inform and advise the controller or processor and the employees who carry out processing of their obligations pursuant to the applicable regulation and other Union or Member State data protection provisions.
- Monitor compliance with the provisions of the Regulation, other Union or Member State data protection provisions and the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the corresponding audits.
- Provide advice, when requested, on data protection impact assessments and monitor their implementation in accordance with the ENS.
- Cooperate with the supervisory authority.
- Act as the point of contact for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and consult, where appropriate, on any other matter.

The Data Protection Officer shall perform his or her duties with due regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of the processing.

Coordination and conflict resolution

The Information Security and Risk Committee shall issue instructions to the Security Manager, who shall be responsible for ensuring compliance by supervising that administrators and operators implement the established security measures.

System Manager:

They inform the Information Manager of any functional incidents relating to the information under their responsibility.

They inform the Service Manager of any functional incidents relating to the service under their responsibility.

They Report to the Security Manager on:

- Security measures, particularly those relating to system architecture decisions.
- Consolidated summary of security incidents.
- Evaluation of the effectiveness of the protection measures to be implemented.

Security Manager:

They inform the Information Manager of security decisions and incidents affecting the information under their responsibility, in particular the residual risk assessment and significant risk deviations from the approved margins.

They inform the Service Manager of security decisions and incidents affecting the service under their responsibility, in particular the residual risk assessment and significant risk deviations from the approved margins.

They report to the Information Security and Risk Committee:

- Consolidated summary of security actions.
- Consolidated summary of information security incidents.
- Status of system security, in particular the residual risk to which the system is exposed.

The Information Security and Risk Committee shall be responsible for resolving any conflicts of responsibility that may arise between the managers and/or between different areas of the organisation, referring them to senior management in cases where it does not have sufficient authority to decide.

All decisions made by the Security Manager that directly affect the System Manager shall be referred to the Security Committee for evaluation prior to any change or decision.

MINIMUM REQUIREMENTS

Ineco relies on Information and Communication Technology (ICT) systems to achieve its objectives. These systems must be managed diligently, taking appropriate measures to protect them from accidental or deliberate damage that could affect the **availability, integrity, confidentiality, traceability, and authenticity** of the information processed or the services provided.

ICT systems must be protected against rapidly evolving threats with the potential to impact any of the five dimensions of information security. To defend against these threats, a strategy is required that adapts to changes in environmental conditions to ensure the continuous provision of services. That is why ENS, in the Article 12, establishes that “All senior bodies of the Public Administrations must formally have their Security Policy, which shall be approved by the head of the corresponding senior body”.

This means that Ineco must apply the minimum security measures required by ENS, as well as continuously monitor service delivery levels, track and analyse reported vulnerabilities, and prepare an effective response to incidents to ensure the continuity of the services provided.

All areas must ensure that ICT security is an integral part of each stage of the system life cycle, from its conception to its withdrawal from service, including development or procurement decisions and operational activities. Security requirements and funding needs must be identified and included in planning, requests for proposals, and tender documents for ICT projects. Areas must be prepared to prevent, detect, react to, and recover from incidents, in accordance with Article 8 of ENS.

Ineco establishes the following **information security objectives**:

- Comply with security and privacy legislation.
- Guarantee the quality and protection of information.
- Guarantee the continued provision of services.
- Achieve full user awareness regarding information security.

Ineco's management, committed to the implementation and maintenance of the Information Security Management System, will set and approve acceptable risk level objectives annually in the Information Security and Risk Committee. The objectives must be current and aligned with the Organisation's purpose and strategy, be measurable or estimable, and consistent with these guidelines.

Personal data

Ineco will only collect personal data when it is appropriate, relevant, not excessive, and in accordance with the scope and purposes for which it was obtained, complying with the obligations and principles set forth in the applicable regulations in force at any given time regarding data protection.

Similarly, it shall adopt the necessary technical and organisational measures to comply with current data protection regulations, all in accordance with the internal regulations relating to the protection of personal data.

Risk Analysis and Management

Ineco is committed to controlling security risks and complying with current legislation and internal regulations through a process of continuous improvement in line with existing frameworks and methodologies for risk analysis and management.

In order to ascertain the level of exposure of information assets to security risks and threats, the Security Manager will arrange for a risk analysis to be carried out, the conclusions of which will be reflected in actions to address and mitigate the risk. These actions must be justified and proportionate to the risk to be mitigated and may even involve rethinking the security of the systems if necessary.

An additional risk analysis of information systems shall be considered when:

- Significant changes are made to the information system infrastructure.
- The provided services are modified.
- Serious security incidents occur.
- Serious vulnerabilities affecting the organisation's information systems are reported.

The conclusions of the risk analyses will be reviewed by the Security Manager, who will communicate them to the Information Security and Risk Committee.

Risk assessment criteria

In order to harmonise risk analyses, Ineco has established a benchmark assessment for the different types of information handled and the different services provided. The detailed risk assessment criteria will be specified in the internally developed risk assessment methodology.

At a minimum, all risks that could seriously impede the provision of services or the fulfilment of the organisation's mission must be addressed. Risks that involve a cessation of service provision will be given special priority.

Risk treatment guidelines

The Information Security and Risk Committee will streamline the availability of resources to meet the security needs of different systems, promoting horizontal investments.

Residual risk acceptance process

Residual risks shall be determined by the Security Manager.

The expected residual risk levels for each piece of information following the implementation of the planned treatment options must be accepted in advance by the person responsible for that information.

The expected residual risk levels for each service following the implementation of the planned treatment options must be accepted in advance by the person responsible for that service.

The residual risk levels will be presented by the Security Manager to the Information Security and Risk Committee, so that it may, where appropriate, evaluate, approve or rectify the proposed treatment options.

Security incident management

Incident monitoring and detection

Ineco has monitoring systems in place for the detection, analysis and reporting of incidents. These are included in the internal procedure for controlling systems in operation.

Incident response

To ensure the availability of services and guarantee the protection of information, Ineco has an incident management procedure in place as well as contingency plan.

The ICT system continuity plans are developed by the System Manager.

Specific procedures for reporting and resolving incidents are in place and are updated periodically.

Personnel management

Personnel obligations

All Ineco members are required to be familiar with and comply with this Information Security Policy. The Information Security and Risk Committee is responsible for providing the necessary means to ensure that the information reaches those affected. To this end, this policy is available on the Intranet. An ongoing awareness programme will also be established for all Ineco members, particularly new recruits.

Third parties

When services are provided or information is managed for an external user, they will be made aware of the Information Security Policy, and channels will be established for reporting and coordination with the respective Information Security and Risk Committees.

When information is presented to external users, they will be made aware of this Policy as it relates to such services or information. Such third parties will be subject to the obligations set forth in this policy and may develop their own operating procedures to comply with it.

It will be ensured that third-party personnel are adequately aware of security matters, at least to the same level as that established in this document.

When any aspect covered in this document cannot be satisfied by a third party as required in the preceding paragraphs, a report from the Security Manager will be required, specifying the risks involved and how to deal with them. This report will require the approval of the Information and Services Managers concerned before proceeding.

A point of contact (POC) will be required for direct communication with third parties.

Awareness and training

Members of the organisation will attend an ICT security awareness session at least once a year, and a continuous awareness programme will be established for members of the organisation, particularly new recruits.

Individuals with responsibility for the use, operation or administration of ICT systems will receive training in the secure handling of systems to the extent that they need it to perform their work. Training will be mandatory before assuming responsibility, whether it is their first assignment or a change of job or responsibilities within the same job.

Professionalism

System security will be monitored, reviewed and audited by qualified personnel who are dedicated and trained in all phases of the system life cycle: installation, maintenance, incident management and decommissioning.

It is necessary that, in an objective and non-discriminatory manner, organisations providing security services to Ineco have appropriate levels of management and maturity in the services provided.

Access authorisation and control

Access to information systems must be controlled and limited to duly authorised users, processes, devices and other information systems, restricting access to permitted functions. This responsibility shall fall to the Security Manager.

Internal managers shall ensure, within the scope of their services and competences, compliance with the coordination instructions, measures and strategies determined by the Security Manager.

In order to correct or demand accountability, each user who accesses the information in the system must be uniquely identified, so that it is known at all times who has been granted access rights, what type of rights they are and who has performed a particular activity.

Protection of facilities

The systems will be installed in separate areas equipped with an access control procedure. Therefore, first of all, a physical security perimeter must be established to protect the organization's information in order to prevent incidents and ensure the functioning of the other measures.

Access to the premises, through authorized and controlled access routes, architectural barriers such as walls or windows, and additional elements such as controlled unloading areas, must be managed to protect areas that contain computer facilities or allow access to them.

Within the security perimeter, locations that store media that may contain confidential or specially protected data must be identified. These locations will have personal identification for users that allows validation of whether they have authorization for access.

Physical security measures for access to the security perimeter, consisting of doors, locks, alarms, and surveillance, must be validated and formalized in instructions for access to the premises, which must be communicated to all personnel.

Internal managers must ensure, within the scope of their services and competencies, compliance with the coordination instructions, measures, and strategies determined by the Physical Security Manager.

Purchase of security products

When purchasing ICT security products, as well as physical security products, to be used by Ineco, those that have certified security functionality related to the purpose of their purchase will be positively evaluated, and care will be taken to ensure that this is included in the contract specifications.

The indicated certification must comply with the most internationally recognized regulations and standards in the field of functional security.

It is established that all software and hardware products intended for security must comply with the minimum requirements defined by ENS. These products must be certified in accordance with standards recognized by the National Cryptological Centre through the CCN-STIC 105 guide or other internationally accepted security regulations.

Critical components must be certified, and compliance with organizational and technical measures such as encryption, access control, and protection against malicious code will be verified prior to implementation.

Default security

Systems must be designed and configured in such a way as to ensure default security:

- The system will provide the minimum functionality required for the organisation to achieve its objectives and will not provide any additional functionality.

- The operation, administration and activity logging functions shall be the minimum necessary, and it shall be ensured that they are only accessible by authorised persons, or from authorised locations or equipment, with restrictions on hours and authorised access points being required where appropriate.
- In an operating system, functions that are unnecessary and even those that are inappropriate for the intended purpose shall be removed or deactivated through configuration control.
- Ordinary use of the system must be simple and secure, so that unsafe use requires a conscious act on the part of the user.

System integrity and updates

All physical or logical elements will require formal authorisation prior to their installation in the system.

The security status of the systems must be known at all times, in relation to the manufacturers' specifications, vulnerabilities and updates that affect them, reacting diligently to manage the risk in view of their security status.

Protection of stored and in-transit information

In the structure and organisation of system security, special attention shall be paid to information stored or in transit through insecure environments. The following devices shall be considered insecure environments: portable equipment, peripheral devices, information media (USB sticks, hard drives) and communications over open networks or with weak encryption.

Security procedures shall include those that ensure the long-term recovery and preservation of electronic documents produced by Ineco within the scope of its competences.

All information in non-electronic format that has been the cause or direct consequence of electronic information must be protected with the same degree of security as the latter. To this end, the measures corresponding to the nature of the medium in which they are stored shall be applied, in accordance with the rules applicable to the security of such media.

Prevention against other interconnected information systems

The system must protect the perimeter, particularly if it is connected to public networks. A public communications network shall be understood as an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public. In any case, the risks arising from the interconnection of the system, or through networks, with other systems shall be analysed, and their point of connection shall be monitored.

Activity log

For the sole purpose of complying with the applicable regulations, and in accordance with the regulations on personal data protection, civil service or labour regulations, and other applicable provisions, user activities will be recorded, retaining the information necessary to monitor, analyse, investigate and document improper or unauthorised activities, allowing the person acting to be identified at all times.

Business continuity

The systems shall have backups and shall establish the necessary mechanisms to ensure continuity of operations in the event of loss of the usual means of work.

Continuous improvement of the security process

The comprehensive implemented security process must be continuously updated and improved. To this end, the criteria and methods recognised in national and international practice relating to information technology management shall be applied.

DOCUMENTATION STRUCTURE

Ineco's safety regulations are structured into six levels:

1. Policies: Document that sets out the organisation's intentions and direction, as formally expressed by senior management.
2. Manuals: Document that sets out the specifications for all or part of the organisation’s management system.
3. Processes: Document that schematically lists a set of activities that use inputs to provide an expected result.
4. Procedures: Document specifying who, what, where, when and why a process or activity is carried out. The how, depending on each case, may be specified in the procedure itself or in a work instruction. A procedure may describe all or part of a process within the organisation.
5. Work instructions: Document specifying how a specific process or activity is carried out.
6. Forms, records, others: Documents containing the form and means established by the organisation to record certain activities or processes, presenting results obtained or providing evidence of activities carried out, offering supporting information, etc.

A full description of the documentation structure can be found in the internal document established for this purpose.

Information rating

The provisions of the internal information classification document will be followed, which covers the following cases:

- TLP in messaging (such as email and chat)
- TLP in documents

This is a scheme created to promote better exchange of sensitive information in the field of information security.

CLIMATE CHANGE

Ineco has analysed the services provided by the organisation, as well as its usual operations for providing them, and has not found any aspects that could influence global climate change. The analysis establishes compliance with the established legal requirements.

The requirements of the interested parties have been analysed and none specifically related to climate change have been found.

Ineco has established actions to reduce its carbon footprint, the main ones being the verification of its carbon footprint calculation in accordance with ISO 14064, certification to ISO 14001 and providing employees with the option of carpooling to the office via an app.

Based on both analyses, it has been concluded that there is no need to apply measures beyond the standard legal requirements established.

Ineco undertakes to disseminate this policy by making it available to all stakeholders, promoting and ensuring compliance with it.

26 February 2026

Ineco’s Board of Directors