INFORMATION SECURITY POLICY

CHANGE CONTROL

SECTIONS	COMMENTS
All	New wording.

Chief Executive Officer
Santiago García Salvador

CONTENTS

1. APPROVAL AND ENTRY INTO FORCE

The Chief Executive Officer of the Dragados Group approved this Policy on 10 June 2026.

This Information Security Policy shall remain in force until it is replaced. It shall be reviewed at least annually, together with any proposals for its update or continued maintenance.

2. INTRODUCTION

To help ensure information quality and the continuous delivery of the organization's services, the Dragados Group takes a preventive approach by implementing appropriate measures to protect systems from accidental or deliberate harm, monitoring day-to-day activities, and responding promptly to incidents.

Protecting systems and information from threats to confidentiality, integrity, availability, authenticity, and traceability requires a strategy that involves all personnel who handle the organization's information.

In line with ISO 27001, the Spanish National Security Framework (*Esquema Nacional de Seguridad*, hereinafter "*ENS*"), and other relevant security initiatives, the Dragados Group adopts a comprehensive approach to information security.

Accordingly, this Information Security Policy is issued and communicated to all employees to ensure awareness and compliance. This Policy, together with the standards and procedures derived from it, shall be reviewed, updated, and communicated periodically, and whenever necessary, to address emerging risks and threats and to continuously improve the effectiveness of the information security measures in place.

This document was prepared with reference to the guides *"CCN – STIC 805 Política de Seguridad de la Información"* and *"CCN – STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones"*, issued by the Spanish National Cryptologic Centre (*Centro Criptológico Nacional*, "CCN").

2.1. Prevention

The Dragados Group shall prevent, or where this is not possible, minimize any adverse impact on information or services resulting from security incidents. To achieve this, it shall implement the minimum security measures required by the *ENS*, together with any additional controls identified through threat and risk assessments. These controls, along with the security roles and responsibilities of all personnel, shall be clearly defined and documented.

To ensure compliance with this Policy, the Dragados Group shall:

i. Authorize systems before they become operational.

ii. Assess security regularly, including routine configuration changes.

iii. Require periodic third-party reviews to obtain an independent assessment.

2.2. Detection

As services may quickly degrade during an incident, from minor slowdowns to complete interruption, their operation shall be continuously monitored to detect anomalies in performance and enable an appropriate response, in accordance with Article 10 of the *ENS*.

Monitoring is especially important where defense-in-depth measures are implemented in accordance with Article 9 of the *ENS*. Detection, analysis, and reporting mechanisms shall be in place to keep relevant stakeholders informed on a regular basis and whenever a significant deviation from established normal parameters occurs.

2.3. Response

To ensure an appropriate response, the Dragados Group shall:

i. Establish effective mechanisms for responding to security incidents.

ii. Designate a point of contact for incident-related communications with relevant stakeholders, including clients, suppliers, and investor groups.

iii. Establish protocols for exchanging incident-related information, including two-way communications with Computer Emergency Response Teams (CERTs) and, where necessary, with Law Enforcement Agencies "*FF.CC. S.E.*" and the Spanish Data Protection Agency (*Agencia Española de Protección de Datos*, "*AEPD*").

2.4. Recovery

To ensure the availability of critical services, the Dragados Group shall implement appropriate measures and strategies, including the identification and assessment of risks, to enable timely preventive action and mitigation.

3. SCOPE

This Policy applies to the information systems of the Dragados Group that support services relating to the design, construction, and operation of civil engineering, building, and industrial projects, and to all personnel, whether internal or external, who are directly or indirectly involved in providing those services.

4. ORGANIZATION'S MISSION

The mission of the Dragados Group is to achieve global leadership in its sectors by maximizing client value through innovation and operational excellence, optimizing resource profitability, and promoting sustainable growth that supports economic and social development.

5. OBJECTIVES

To ensure the effective protection of information and the corporate resources needed for the proper delivery of the Dragados Group's services, against both internal and external threats, and to define that protection in terms of quality and security, the following objectives and basic principles are established:

i. Establish mechanisms to identify, control, and treat security risks.

ii. Implement preventive measures to reduce unforeseen incidents and ensure they are controlled and corrected, thereby strengthening the Dragados Group's digital operational resilience.

iii. Promote a security culture through employee awareness initiatives on compliance with the Organization's information security requirements.

iv. Ensure compliance with all applicable legal and regulatory requirements.

v. Maintain appropriate internal communication channels for security management matters.

vi. Invest in staff training and the resources needed to ensure the confidentiality, integrity, availability, authenticity, and traceability of information.

vii. Meet the needs of clients, the market, and society within the scope of the Dragados Group's activities.

viii. Establish and maintain an Information Security Management System, supported by the policies, standards, guidelines, requirements, and procedures needed to embed security requirements across the organization and protect the Dragados Group's information and assets.

6. REGULATORY AND LEGAL FRAMEWORK

This Policy sets out the principal regulations applicable to the Dragados Group, including the following:

i. General Data Protection Regulation (Regulation (EU) 2016/679).

ii. Organic Law 3/2018, of 5 December, on Personal Data Protection and the guarantee of digital rights "*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*".

iii. Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce "*Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico*".

iv. Law 1/2019, of 20 February, on Trade Secrets "*Ley 1/2019, de 20 de febrero, de Secretos Empresariales*".

v. Royal Decree-Law 28/2020, of 22 September, on remote work "*Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia*".

vi. Law 10/2021, of 9 July, on remote work "*Ley 10/2021, de 9 de julio, de trabajo a distancia*".

vii. Royal Decree 311/2022, of 3 May, regulating the Esquema Nacional de Seguridad "*Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*".

viii. ISO 27001:2022 standard.

In addition, the Dragados Group maintains an internal register that documents the full applicable legal and regulatory framework.

7. INFORMATION SECURITY ORGANIZATION

7.1. Information Security Committee

To support the management of security within the Dragados Group, Management hereby establishes, through this Policy, an Information Security Committee responsible for managing and coordinating all activities related to the security of the organization's information systems.

The Information Security Committee shall consist of the heads of:

i. Information Security "*Seguridad de la Información*"

ii. Administration and Finance Management "*Dirección de Administración y Finanzas*"

iii. Compliance Management "*Dirección de Cumplimiento*"

iv. Human Resources Management "*Dirección de Recursos*"

v. Legal Management "*Dirección de Asesoría Jurídica*"

vi. Subdirección de Sistemas "*IT Systems Subdivision*"

The Committee may, on an ad hoc basis, include individuals or roles whose knowledge, experience, or area of responsibility is relevant to the matters on the agenda.

The Information Security Committee shall meet at least quarterly to review information security matters, and additionally whenever the Chair considers it necessary.

The Information Security Manager shall serve as both Chair and Secretary of the Information Security Committee and, in the latter role, shall be responsible for the following functions:

i. Call meetings of the Information Security Committee.

ii. Prepare meeting agendas and provide the information needed to support decision-making.

iii. Prepare meeting minutes.

iv. Coordinate and monitor actions arising from the Committee's decisions.

The functions of the Information Security Committee shall be as follows:

i. Assume the responsibilities of the Information Responsible *"Responsable de la Información - ENS"* (see section 7.2.3) and the Service Responsible *"Responsable del Servicio - ENS"* (see section 7.2.4).

ii. Address information security concerns raised by Management and the various departments.

iii. Report regularly to Management on the status of information security.

iv. Promote the continual improvement of the Information Security Management System.

v. Develop the organization's information security strategy.

vi. Lead the corporate information security strategy.

vii. Coordinate information security efforts across the different areas to ensure consistency, alignment with the defined strategy, and the avoidance of duplication.

viii. Develop, review, and regularly update the Information Security Policy for Management approval.

ix. Approve the information security standards and procedures arising from this Policy.

x. Define and approve information security training and qualification requirements for administrators, operators, and users.

xi. Promote periodic audits to verify compliance with the organization's information security obligations.

xii. Review the most significant audit results.

xiii. Approve and review information security objectives and indicators.

xiv. Review the results of risk analyses and monitor the actions arising from the Risk Treatment Plan.

xv. Monitor the organization's principal residual risks and recommend appropriate actions.

xvi. Monitor the effectiveness of security incident management processes, recommend appropriate actions, and ensure coordination among the different security areas involved in incident management.

xvii. Approve information security improvement plans across the organization and ensure coordination among plans implemented in different areas.

xviii. Prioritize security actions when resources are limited.

xix. Ensure that information security is considered in all ICT projects from initial specification to operational deployment.

xx. Resolve conflicts of responsibility between roles or organizational areas, escalating cases where the authority to decide is insufficient.

xxi. Ensure compliance with the Dragados Group Information Security Policy and alignment with the ACS policy and the Dragados Group Cybersecurity Framework ("*CNS*").

The Information Security Committee shall periodically obtain the information it needs from internal and external technical and legal personnel to support informed decision-making in matters requiring assessment or reporting.

In its meetings, the Committee shall review the development of information security based on defined indicators, the results of threat and risk analyses, internal and external audits, and the status of corrective and preventive actions.

All of the above is intended to support Management's ongoing assessment of the effectiveness, efficiency, and continual improvement of the Information Security Management System.

7.2. Roles and responsibilities in information security

In addition to the Information Security Committee, described above, the roles and responsibilities of the other positions involved are as follows:

i. Information Security Responsible "*Responsable de Seguridad - ENS*", represented by the Information Security Manager.

ii. IT System Responsible "*Responsable del Sistema - ENS*", represented by the Head of IT Systems Subdivision.

iii. Information Responsible "*Responsable de la Información - ENS*", represented by the Information Security Committee.

iv. Service Responsible "*Responsible del Servicio - ENS*", represented by the Information Security Committee.

7.2.1. Information Security Responsible "***Responsable de Seguridad - ENS***"

The functions of the Information Security Responsible "*Responsable de Seguridad - ENS*" are as follows:

i. Maintain the security of the information handled and the services delivered by the information systems within their scope of responsibility, in accordance with the organization's Information Security Policy.

ii. Promote information security training and awareness within their scope of responsibility.

iii. Participate in the management of significant security alerts, incidents, and issues that may affect the Dragados Group and its information assets or pose a serious risk to them.

iv. Support and oversee the investigation of security incidents from notification to resolution.

v. Implement and monitor the technical and organizational measures needed to ensure data security and prevent unauthorized alteration, loss, processing, or access.

vi. Ensure that system security documentation is kept up to date, including the Information Security Policy, security standards, and related procedures.

vii. Perform risk analyses annually.

viii. Analyse incidents and propose safeguards to prevent recurrence.

ix. Review and update security improvement plans.

7.2.2. IT System Responsible "*Responsable del Sistema - ENS*"

The functions of the IT System Responsible "*Responsable del Sistema - ENS*" are as follows:

i. Develop, operate, and maintain ICT systems throughout their lifecycle, including specification, installation, verification, and proper operation.

ii. Define the information system's topology and management, including the criteria for its use and the services available within it.

iii. Ensure that implemented security measures align with the Information Security Regulatory Framework.

iv. The IT System Responsible "*Responsable del Sistema - ENS*" may decide to suspend the processing of certain information or the delivery of a specific service if serious security deficiencies are identified that could compromise compliance with established requirements. Before doing so, the decision shall be agreed with the Information Responsible "*Responsable de la Información - ENS*", the Service Responsible "*Responsable del Servicio - ENS*", and the Information Security Responsible "*Responsable de Seguridad - ENS*".

v. Work with the Information Security Manager to maintain system security documentation, particularly security procedures.

vi. Review and update security improvement plans in coordination with the Information Security Manager.

vii. Implement approved security plans following a security incident.

7.2.3. Information Responsible "*Responsable de la Información - ENS*"

The functions of the Information Responsible "*Responsable de la Información - ENS*" are as follows:

i. Hold ultimate responsibility for the use and protection of specific information. The Information Responsible "*Responsable de la Información - ENS*" is therefore ultimately accountable for any error or negligence that leads to a security incident.

ii. Define information security requirements or, in ENS terminology, determine the security levels applicable to the information.

iii. The Information Security Committee has been assigned the role of Information Responsible "*Responsable de la Información - ENS*".

iv. Although formal approval of the security levels rests with the Information Responsible, input may be sought from the Information Security Manager, and the views of the IT System Responsible "*Responsable del Sistema - ENS*" shall be taken into account.

7.2.4. Service Responsible "*Responsable del Servicio – ENS*"

The functions of the Service Responsible "*Responsable del Servicio – ENS*" are as follows:

i. Define the security requirements for services or, in ENS terminology, determine their security levels.

ii. Define service security requirements, including interoperability, accessibility, and availability.

iii. Determine the security levels applicable to the services.

iv. The Information Security Committee has been assigned the role of Service Responsible "*Responsable del Servicio - ENS*".

v. Although formal approval of security levels rests with the Service Responsible "*Responsable del Servicio - ENS*", input may be sought from the Information Security Responsible "*Responsable de Seguridad - ENS*", and the views of the IT System Responsible "*Responsable del Sistema - ENS*" shall be taken into account.

7.2.5. Appointment and Renewal Procedure

Management of the Dragados Group shall assign information security roles and responsibilities on the proposal of the Information Security Committee. Management shall also appoint the members of the Information Security Committee.

Management also reserves the right to review and update these assignments and responsibilities at any time.

8. RISK MANAGEMENT

All systems subject to this Policy shall undergo risk analysis to identify threats and assess the risks to which they are exposed. This analysis shall be repeated:

i. Regularly, and at least annually.

ii. Whenever the information handled changes.

iii. Whenever the services provided change.

iv. Whenever a serious security incident occurs.

To harmonize risk analyses, the Information Security Committee shall establish a reference classification for the types of information handled and the services provided. It shall also promote the availability of resources to meet the security needs of the different systems, including cross-functional investment where appropriate.

9. PERSONNEL OBLIGATIONS

All Dragados Group personnel, whether internal or external, who use or have access to corporate information or technological systems shall have the following obligations:

i. Know, comply with, and uphold this Information Security Policy, together with the security standards and procedures that support it and apply to them.

ii. Participate in information security awareness activities.

iii. Use information systems, services, and accessible information only for professional purposes, in line with the duties of their role and the purpose for which access was granted.

iv. Protect the confidentiality of the information to which they have access, in accordance with its classification and characteristics.

v. Report any event that may constitute a security breach or expose a weakness that could lead to further breaches.

vi. Cooperate in resolving security breaches and implementing preventive actions when required.

vii. Participate in the information security governance structure when required, in line with the responsibilities of their role.

viii. Refrain from intentional or negligent actions that may compromise the security of technological systems or the information they contain.

Furthermore, all Dragados Group personnel shall use the resources made available to them for the performance of their duties appropriately, proportionately, and only where justified.

10. THIRD-PARTY RELATIONSHIPS

When the Dragados Group provides services to other organizations or handles their information, those organizations shall be informed of this Information Security Policy. Communication channels shall also be established for reporting and coordination between the respective security committees, together with procedures for responding to security incidents.

Similarly, when the Dragados Group uses third-party services or discloses information to third parties, those parties shall be informed of this Information Security Policy and the security standards applicable to the relevant services or information. They shall comply with the applicable regulatory obligations and may develop their own operational procedures to do so. Specific procedures for incident reporting and resolution shall also be established.

11. PERSONAL DATA

The processing of personal data within the Dragados Group's information systems shall at all times comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, GDPR), as well as Organic Law 3/2018, of 5 December, on Personal Data Protection and the guarantee of digital rights ("*Ley Orgánica 3/2018, de 5 de Decembre, de Protección de Datos Personales y garantía de los derechos digitales*", LOPDGDD).

The Dragados Group maintains an up-to-date Record of Processing Activities documenting all personal data processing operations, including, among other matters, their purposes, legal basis, categories of data and data subjects, retention periods, and any recipients or disclosures of personal data.

All Dragados Group information systems shall implement appropriate technical and organizational measures to ensure a level of security proportionate to the risk, taking into account the nature, scope, context, and purposes of processing, as well as the risks to the rights and freedoms of natural persons. These measures shall be determined through the relevant risk analysis and aligned with the guidelines of the *Esquema Nacional de Seguridad (ENS)* and the obligations and principles set out in the GDPR.

12. SYSTEM SECURITY DOCUMENTATION

The Dragados Group documentation system comprises this Information Security Policy and the supporting Information Security Regulatory Framework, which includes guidelines, requirements, technical protocols, and internal manuals governing the security requirements established in the *Esquema Nacional de Seguridad (ENS)* and the ISO/IEC 27001 standard.

The Information Security Committee of the Dragados Group shall ensure that this documentation set is reviewed at least annually and whenever significant changes occur in the information systems, identified risks, services provided, or applicable regulatory framework, and updated as necessary.

Furthermore, the Dragados Group has established categories and criteria for classifying information and information assets in accordance with Annex I of Royal Decree 311/2022 of 3 May, which regulates the *Esquema Nacional de Seguridad (ENS)*. These criteria are set out in the document *"DSI-02 Information Classification Guidelines"*.

All security documentation shall be stored in the Dragados Group's corporate document repository, with access restricted to authorized personnel. The current approved version of the Information

Security Policy shall be available to all personnel in read-only mode for awareness and compliance purposes.