Royal Decree 3/2010, of 8 January, regulating the National Security Framework in the area of e-Government

This document is a translation of:

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Publicado en: «BOE» núm. 25, de 29/01/2010.

Entrada en vigor: 30/01/2010

Departamento: Ministerio de la Presidencia

Referencia: BOE-A-2010-1330

Permalink ELI: https://www.boe.es/eli/es/rd/2010/01/08/3/con

published in the Spanish Official State Gazette (BOE). It is not an official translation and therefore has no legal validity.

It Includes corrections of errata awaiting publication in the Official State Gazette.

I

The necessary generalisation of the information society is, to a large extent, accessory to the trust of citizens in relations established through electronic media.

Within the Public Administrations scope, communication through electronic means involves the fulfilment of several obligations on the part of Administrations, such as promoting the conditions which ensure that freedom and equality may be real and effective and removing obstacles that hinder or prevent their full application. This requires the incorporation of the necessary peculiarities for guaranteeing the safe application of such technologies.

Article 42.2 of Law 11/2007 of 22 June 2007, on the electronic access of citizens to public services, provides a response to this problem by creating a National Security Framework, the purpose of which is to establish the principles and requirements of a security policy regarding the use of electronic means, to allow the adequate protection of information.

The aim of the National Security Framework is to create the conditions necessary to inspire trust in the use of electronic means, by implementing measures to guarantee the safety of systems, data, communications and electronic services, thereby allowing citizens and Public Administrations to exercise their rights and comply with their obligations through these methods.

The National Security Framework is intended to inspire trust in the provision of services and safeguard the information by information systems, in accordance with their functional specifications, preventing uncontrolled interruptions or changes and preventing non-authorised access to information. Simultaneously to the evolution of the services, and as they are gradually consolidated, the requirements of such services and the infrastructures that support them will be developed and improved on.

Currently, the information systems of public administrations are considerably interconnected with each other and with information systems from the private sector: business and citizens. In this way, security must face a new challenge that goes even further than the security of each individual system. For that reason, each system must have a clearly-defined perimeter and those responsible for each security domain must coordinate effectively with each other, to avoid the creation of "uncontrolled areas" and divisions that could damage the information or the services provided.

Within this context, security of networks and information is taken as the capacity of the information networks or systems to withstand accidents or illicit or wilful actions that could endanger the availability, authenticity, integrity and confidentiality of the data stored or transmitted and the services that such networks and systems provide or make accessible, based on a determined confidence level.

II

The National Security Framework takes into account the recommendations of the

European Union (Decision 2001/844/EC, ECSC, Euratom of the Commission, dated 29 November 2001, amending its internal Rules of Procedure and Council Decision 2001/264/EC of 19 March 2001, adopting the Council's security regulations), the technological situation of the different Public Administrations and the existing electronic services in such Administrations, the use of open standards and, in addition, standards that are generally used by the citizens.

The articulation thereof has been carried out based on national guidelines on e-government, personal information protection, electronic signatures and electronic identity documents, the National Cryptologic Centre (Centro Criptológico Nacional), the information society, the reuse of information in the public sector and collegiate bodies responsible for e-government, and the regulation of different Government instruments and services, directives and guidelines of the OECD and national and international standardisation legislation.

Law 11/2007 of 22 June 2007, inspires this provision and enables it to be applied, acting as a coadjutant to its implementation in aspects regarding the security of information technology systems in Public Administrations, thereby contributing to the development of an effective instrument that allows citizens' rights to be guaranteed within the e-government scope.

Organic Law 15/1999 of 13 December 1999, on the Protection of Personal Information and its implementation regulations, determines several measures aimed at protecting personal information Also provides criteria for establishing the proportionality between the security measures and the information that is to be protected.

Law 30/1992 of 26 November 1992, on the Legal System of Public Administrations and Common Administrative Procedure, the essential legal reference in all administrative regulation, determines the configuration of confidentiality, other than classified information and personal information that need to be physically protected. Likewise, it determines the legal basis for administrative communications and their legal requirements regarding validity and efficacy, upon which the necessary technological and security requirements will be based, in order to project their effects in communications sent by electronic means.

Law 37/2007 of 16 November 2007, on the reuse of information from the public sector which determines the basic regulations of the legal system applicable to the reuse of documents drawn up in the public sector, configuring a scope of exception regarding application, which includes the information mentioned in the National Security Framework.

Together with the above legislation, the content of this guideline has been inspired by Government documents on electronic security, such as the Security, standardization and preservation Criteria, CCN-STIC guidelines on the Security of Information and Communication Systems, the Methodology and tools for analysis and management of risks or the National Interoperability Framework, also implemented within the scope of Law 11/2007 of 22 June 2007.

III

This royal decree is limited to establishing the basic principles and minimum requirements which, in accordance with the general interest, nature and complexity of the regulated subject, allow the adequate protection of information and services. This requires including the scope and procedure to manage the electronic security of systems that process information from Public Administrations within the scope of Law 11/2007 of 22 June 2007. By this means, a common regulatory denominator is achieved, whose regulation does not exhaust all the options of standardisation and allows it to be completed by the regulation of the objectives (non-basic, in material terms) that can be decided on by territorial legislative policies.

To ensure that the above requirements are met, some security dimensions and levels are established, and the category of the systems, the adequate security measures and regular auditing of security; the implantation of a report to provide regular information on the security status of the information systems mentioned in this royal decree, the National Cryptologic Centre´s response capacity to confront security incidents and the inclusion of a glossary of terms, with a special mention to training.

This royal decree is structured in ten chapters, four additional provisions, one transitional provision, one repealing provision and three final provisions. The first four annexes are dedicated to the categories of systems, security measures, security auditing and the glossary of terms. The fifth annex establishes a specific administrative clause template to be included in the administrative clauses of the respective contracts.

This royal decree presents security as an integral activity that contains no occasional actions or temporary processes, due to the fact that the weakness of a system is determined by its most fragile part and this part is often the result of the coordination of measures that are adequate individually, but which are assembled defectively. The information processed in the electronic systems to which this royal decree refers will be protected, taking into consideration the terms set forth in Organic Law 15/1999 of 13 December, 1999.

The present royal decree is passed in application of the terms of final provision eight of Law 11/2007 of 22 June 2007, and in accordance with the terms of Article 42, section 3 and final provision one of that provision, it was prepared in collaboration with all the Public Administrations to which it applies, and received a favourable report from the Permanent Commission of the Higher Council of Electronic Government, the Public Administration Sector Conference and the National Local Authorities Commission, and has been submitted to the preliminary report of the Spanish Data Protection Agency. It has also been submitted to the opinion of citizens, in accordance with the forecasts established in Article 24 of Law 50/1997 of 27 November 1997.

By virtue thereof, and following the proposal of the Ministry of the Presidency, in accordance with the Spanish State Advisory Council and after deliberation by the Council of Ministers at its meeting on 8 January 2010,

I ORDER THE FOLLOWING:

CHAPTER I

General provisions

Article 1. *Object*

1. The purpose of this royal decree is to regulate the National Security Framework established in Article 42 of Law 11/2007 of 22 June 2007, and determine the security policy regarding the use of electronic means to which that act refers.

2. The National Security Framework is made up by the basic principles and minimum requirements necessary for the adequate protection of information. It will be applied by Public Administrations to ensure the access, integrity, availability, authenticity, confidentiality, traceability and preservation of data, information and services used in the electronic means they control in the performance of their powers.

Article 2. *Definitions and standards*

For the purposes provided for in this royal decree, the definitions, words, expressions and terms must be understood in the sense indicated in the Glossary of Terms included in Annex IV.

Article 3. *Scope of application*

The scope of application of this royal decree is the one set forth in Article 2 of Law 22/2007 of 22 June 2007.

The scope of application indicated above does not include systems processing information regulated by Law 9/1968 of 5 April 1968, on Official Secrets and developing rules.

CHAPTER II

Basic Provisions

Article 4. *Basic principles of the National Security Framework*

The ultimate objective of information security is to ensure that a government organisation can comply with its objectives in using information systems. The following basic principles must be considered in decisions regarding security:

a) Integral security
b) Risk management
c) Prevention, reaction and recovery

d) Lines of defence
e) Regular re-evaluation
f) Segregation of duties

Article 5. *Security as an integral process*

1. Security must be understood as an integral process, constituted by all the technical, human, material and organisational elements related to the system. The application of the National Security Framework will be governed by this principle, which excludes all occasional actions or conjunctural treatment.

2. Maximum attention will be paid to arousing awareness in the persons intervening in the process and their superiors in rank, so that neither ignorance nor a lack of organisation and coordination or inappropriate instructions are a source of risk for security.

Article 6. *Security management based on risks*

1. The analysis and management of risks will form an essential part of the security process and must be kept permanently updated.

2. Risk management will allow the maintenance of a controlled environment, reducing risks to acceptable levels. Reducing these levels will be achieved by deploying security measures to establish a balance between the nature of the information and the processes, the risks to which the information is exposed and security measures.

Article 7. *Prevention, reaction and recovery*

1. The security of the system will include aspects such as prevention, detection and mitigation, to ensure that threats do not materialise, and do not have a serious effect on the information being processed or the services being provided.

2. The prevention measures must eliminate or at least reduce the possibility of the threats materialising and harming the system. Such preventive measures will include, among others, dissuasion and reduction to exposure.

3. The detection measures will be accompanied by reactive measures, so that security incidents are prevented in time.

4. The recovery measures will allow the information and the services to be restored, so that situations in which a security incident disables the habitual methods can be corrected.

5. Without detriment to all other basic principles and minimum requirements that may be established, the system will guarantee the preservation of data and information in an electronic information device.

Likewise, the system will ensure that the services continue to be available during the whole life cycle of the digital information, through a design and procedures that form a basis for the preservation of digital heritage.

Article 8. *Lines of defence*

1. The system must have a protective strategy, formed by multiple security layers, and laid out so that if one of the layers fails, it allows:

a) Time to be saved in taking the appropriate reactive measures to prevent incidents that cannot be avoided.
b) A reduction in the likelihood of the system being harmed as a whole.
c) A reduction in the final impact on the system.

2. The lines of defence will be constituted by organisational, physical and logical measures.

Article 9. *Regular re-evaluation*

The security measures will be re-evaluated and updated regularly, to adapt their efficacy to the ongoing evolution of the risks and protective systems, to the point of re-considering security, if necessary.

Article 10. *Segregation of duties*

In the information systems, segregation of duties will be made between the party responsible for the information, the party responsible for the service and the party responsible for security.

The party responsible for the information will determine the requirements of the processed information; the party responsible for the service will determine the requirements of the services provided and the party responsible for security will determine the decisions to be taken to satisfy the information and service security requirements.

The party responsible for the security of the information systems will be different from the party responsible for providing the service.

The organisation's security policy will detail the attributes of each responsible party and the mechanisms for coordination and for solving conflicts.

CHAPTER III

Minimum Requirements

Article 11. *Minimum security requirements.*

1. All higher public administration bodies must have their own formal security policy to coordinate ongoing security management, which must be approved by the head of the higher body in question. That security policy must be established according to the basic principles indicated and must be implemented applying the following minimum requirements:

a) Organisation and implementation of security processes
b) Risk analysis and management
c) Personnel management
d) Professionalism
e) Authorisation and control of accesses
f) Protection of the premises
g) Product purchases
h) Security by default
i) Integrity and updating of the system
j) Protection of the information stored and in transit
k) Prevention in the presence of other interconnected information systems
l) Recording of activity
m) Security incidents
n) Continuity of the activity
o) Ongoing improvement of the security process

2. For the purposes indicated in the preceding section, higher bodies are considered to be those directly responsible for executing government, central, regional or local actions, in a specific sector of activity, in accordance with the provisions of Law 6/1997 of 14 April 1997, on the organisation and functioning of the General State Administration and Law 50/1997 of 27 November 1997, the respective regional by-laws and developing rules and Law 7/1985 of 2 April 1985, regulating the Local Regime rules, respectively.

Municipalities may have a common security policy, drafted by the Provincial Council, Insular Government or any other sole-proprietorship body from other representative corporations responsible for the regional government and provincial administration, or as applicable, the respective district entity to which they belong.

3. All these minimum requirements will be required in proportion to the risks identified in each system, and some may not be required in systems with no significant risks and they will be complied with in accordance with what is set forth in Article 27.

Article 12. *Organisation and implantation of the security process*

Security will be a priority for all the members of the organisation. The security policy as set forth in Annex II, section 3.1 will identify a clear set of responsibilities in enforcing their compliance and be known to all the members of the administrative organisation.

Article 13. *Risk analysis and management*

1. Each organisation developing and establishing systems for processing information and communications will carry out its own risk management.

2. This management will be done by analysing and processing the risks to which the system is exposed. Without prejudice to the terms of Annex II, an internationally recognised method will be used.

3. The measures adopted to mitigate or eliminate the risks will be justified and there will always exist proportionality between them and the risks.

Article 14. *Personnel management*

1. All the personnel related to the information and systems will be trained and informed of their duties and obligations regarding security issues. Their actions will be supervised to verify that the established procedures are followed.

2. All personnel related to the information and systems will exercise and apply the security principles when performing their tasks.

3. The meaning and scope of the safe use of the system will be specified and expressed through a series of security rules.

4. To correct or demand responsibility, whichever applies, each user accessing the system information will be personally identified, so that it is known at all times who has the rights of access, what type of rights and who has carried out a particular activity.

Article 15. *Professionalism*

1. The security of the systems will be dealt with, reviewed and audited by qualified staff that is dedicated and instructed on all the phases of its life cycle: installation, maintenance, control of incidents and dismantling.

2. The personnel of the Public Administrations will receive the training that is necessary to guarantee the security of the information technologies applicable to the Government systems and services.

3. Public Administrations must, objectively and without discrimination, require the organisations providing security services to use qualified professionals, with the appropriate levels of management and maturity, in providing the services.

Article 16. *Authorisation and control of accesses*

Access to the information system will be controlled and restricted to duly authorised users, processes, devices and other information systems, and access will be restricted to the permitted functions.

Article 17. *Protection of the premises*

The systems will be installed in separate areas, equipped with an access control procedure. The rooms will be closed, at least, and the keys to such rooms will be subject to control.

Article 18. *Security product purchases and contracting of security services.*

1. When purchasing security products for information technologies and communications to be used by Public Administrations, any products whose relevant security functional features have been certified will be used in proportion to the system category and particular level of security, except in cases where the proportion of requirements against assumed risks does not justify it in the opinion of the Security Officer.

2. The certification referred to in the preceding paragraph must be in keeping with the most important internationally-recognised rules and standards within the functional security scope.

3. The Certification Body of the Spanish National Evaluation and Certification Scheme of the Security of Information Technologies, constituted in accordance with the terms of Article 2.2c) of Royal Decree 421/2004 of 12 March 2004, regulated by order PRE/2740/2007 of 19 September 2007, which determines the criterion to be met depending on the foreseen use of the product in question, in relation to the evaluation level, other additional security certificates that are required by the regulations and exceptionally, in cases in which no certified products exist. The indicated process will be carried out taking into account the evaluation criteria and methods, determined by the internal regulations included in that ministerial order.

4. To procure security services, please refer to the preceding paragraphs and Article 15.

Article 19. *Security by default*

The systems will be designed and configured so that they guarantee security by default:

a) The system must provide the minimum functionality required for the organisation to achieve its objectives.

b) The operating, administration and activity recording functions will be the minimum necessary and it will be ensured that they can only be accessed by authorised persons or from authorised sites or equipment, and if necessary, restrictions will be imposed regarding times and points of access provided.

c) In operating systems, functions that are of no interest will be eliminated or disabled by configuration control. This includes those that are in adequate for the purpose that is to be achieved.

d) Normal use of the system will be simple and safe, so that any unsafe use requires a conscious action on the part of the user.

Article 20. *Integrity and updating of the system*

1. All physical or logical elements will require formal authorisation before being installed in the system.

2. The security status of the systems will be known at all times, in relation to the manufacturers' specifications, vulnerable aspects and updates that affect them, and diligent action will be taken to control the risk in view of the security status thereof.

Article 21. *Protection of information stored and in transit*

1. In the system security structure and organisation, special attention will be paid to information stored or transiting through unsafe environments. Unsafe environments include laptops, personal assistants (PDAs), peripheral devices, information devices and communications on open networks or ones with weak ciphering.

2. Security includes procedures that ensure the retrieval and long-term preservation of electronic documents produced by Public Administrations within the scope of their authority.

3. All information not contained on electronic devices that has been generated by or is the direct consequence of the electronic information referred to in this royal decree will be protected with the same grade of security as that information. For this purpose the corresponding measures will be taken for the type of information device in which they are located, pursuant to the applicable regulations on the security thereof.

Article 22. *Prevention in the presence of other interconnected systems*

The system must protect the perimeter, specially, if connection is made to public networks. Public communication networks are taken as electronic communication networks used in full or in part for providing electronic communication services that are available to the public, in accordance with the definition established in Law 32/2003, Annex II, section 26, of 3 November 2003, on Telecommunications in General. In all cases the risks arising from the system interconnection through networks with other systems will be analysed, and their union points will be controlled.

Article 23. *Recording of activity*

For the exclusive purpose of achieving compliance with the object of this royal decree, with full guarantees of the right to honour, personal and family privacy and the image of those affected, and pursuant to the provisions on personal information protection, public or employment function, and other provisions that may apply, the activities of users will be recorded, retaining the necessary information for monitoring, analysing, investigating and documenting improper or unauthorised activities, allowing the person who is performing the activity to be identified at any time.

Article 24. *Security incidents*

1. A system will be established for detecting and taking action to confront malicious codes.

2. There must be procedures in place for managing security incidents and weaknesses detected in the components of the information system. Those procedures must cover detection mechanisms, classification criteria, analysis and resolution procedures and also

channels of communication with interested parties and recording actions. That record will be used for the ongoing improvement of the system security.

Article 25. *Continuity of the activity*

The systems will use backup copies and other mechanisms to guarantee the continuity of the operations, in the event of losing the usual operating methods.

Article 26. *Ongoing improvement of the security process*

The integral security process implanted will be updated and improved continuously. For this purpose, the criteria and methods established in national and international practice in relation to information technologies will be applied.

Article 27. *Compliance with the minimum requirements*

1. To ensure compliance with the minimum requirements set forth in this Royal Decree, Public Administrations will apply the security measures indicated in Annex II, taking into account:

a) The assets that comprise the system.
b) The system category, as provided for in Article 43.
c) The decisions taken to manage identified risks.

2. If a system affected by this royal decree processes personal information, the provisions of Organic Law 15/1999 of 13 December 1999, and the developing rules will be applied, without prejudice to the requirements set forth in the National Security Framework.

3. The measures referred to in paragraphs 1 and 2 will be considered minimum requirements and may be extended in cases of the indicated concurrence or the prudent arbitration of the party responsible for system security, taking account of the state of technology, the nature of the services provided and the information being processed, and the risks to which it is exposed.

4. The list of measures selected from Annex II shall be formalised in a document called the Statement of Applicability, signed by the Security Officer.

5. The security measures listed in Annex II may be replaced by other compensatory measures provided that documentary evidence shows that they provide equal or better protection against the risk to assets (Annex I) and that the basic principles and minimum requirements laid down in Chapters II and III of the Royal Decree are met. As an integral part of the Statement of Applicability, the correspondence between the compensatory measures being implemented and the measures in Annex II that they compensate shall be indicated in detail and the whole shall be formally approved by the Security Officer.

Article 28. *Common infrastructures and services*

The use of common infrastructures and services recognised by Public Administrations will enforce compliance with the basic principles and minimum requirements set forth in this royal decree, in conditions of greater efficiency. The specific cases of use of these common infrastructures and services will be determined by each Administration.

Article 29. *Technical security instructions and security guides.*

1. To guarantee full compliance with the provisions of the National Security Framework, in exercising its functions, the National Cryptologic Centre will prepare and distribute the respective information technology security guides and communications.

2. The Ministry of Finance and Public Administrations, as proposed by the Electronic Government Sector Committee given in Article 40 of Law 11/2007, of 22 June, and on the initiative of the National Cryptologic Centre, shall approve the technical instructions for compulsory security and shall publish them by means of a resolution from the Secretary of State for Public Administrations. In order to draft and maintain the technical safety instructions, the corresponding work groups will be set up in colleges with competence in e-government.

3. The technical safety instructions shall take into account the applicable harmonised European standards.

Article 30. *Information systems not affected*

The Public Administrations may determine the information systems that are not governed by the provisions of this royal decree, due to their being systems not related to the exercising of rights or compliance with duties by electronic means or access of citizens to government information and procedures by electronic means, pursuant to the provisions of Law 11/2007 of 22 June, 2007.

CHAPTER IV

Electronic communications

Article 31. *Technical security conditions of electronic communications*

1. The technical security conditions of electronic communications in relation to transmission and reception, their dates, the entire content of the communications and the true identification of the sender and addressee of those communications, as established in Law 11/2007 of 22 June 2007, will be implemented in accordance with the provisions of the National Security Framework.

2. Communications made under the terms indicated in the preceding paragraph will have the value and legal efficacy that correspond to their respective natures, pursuant to current legislation.

Article 32. *Technical requirements for electronic notifications and publications*

1. Electronic notifications and publications of decisions and administrative acts will be made so that they comply with the following technical requirements, pursuant to the provisions of this royal decree:

a) They will guarantee the authenticity of the organisation publishing them.

b) They will ensure the integrity of the information published.

c) They will record the time and date on which the decision or act published or notified was made available to the interested party and of the access to its content.

d) They will ensure the authenticity of the addressee of the publication or notification.

Article 33. *Electronic signature*

1. The electronic signature mechanisms will be applied based on the terms set forth in Annex II of this decree and in accordance with the provisions of the electronic signature and certificates policy, as it is established in the National Interoperability Framework.

2. The electronic signature and certificates policy will specify the processes for generating, validating and keeping record of electronic signatures and the characteristics and requirements governing the electronic signature, certificates, time stamping systems and other supporting elements for signatures, without prejudice to the provisions of Annex II, which will be adapted to each particular case.

CHAPTER V

Security audit

Article 34. *Security auditing*

1. The information systems referred to in this royal decree will be subject to ordinary regular audits at least every two years, to verify compliance with the requirements of this National Security Framework.

On an extraordinary basis, that audit will be performed whenever substantial changes are made to the information system that could affect the required security measures. The performing of the extraordinary audit will determine the date for calculating the two years established for performing the ordinary regular audit indicated in the preceding paragraph.

2. This audit will be performed depending on the system category, determined pursuant to Annex I and in accordance with the terms of Annex III.

3. Within the framework of the terms of Article 39 of Law 11/2207 of 22 June 2007, the audit will enter in depth into the system details, up to the level that is considered to provide sufficient evidence, within the scope established for the audit.

4. In performing this audit, generally accepted criteria, working methods and conducts will be used, and the national and international information that applies to this type of information systems audit.

5. The audit report will issue a decision on the degree of compliance with this royal decree, identify any faults and recommend potential corrective or complementary actions that may be necessary, and the recommendations that are considered appropriate. It will also include the methodology criteria used to perform the audit, the scope and objective of the audit and the information, facts and observations on which the conclusions are made.

6. The audit reports will be submitted to the respective persons responsible for the system and for security. These reports will be analysed by the latter who will present his/her conclusions to the system manager for the adequate corrective actions to be taken.

7. In the case of HIGH category system, in view of the audit decision, the system manager may agree to withdraw the operation of certain information, service or system in full during the time he considers fit, and to the full satisfaction of the prescribed modifications.

8. The audit reports may be requested by those responsible for each organisation with competence regarding the security of information technologies.

CHAPTER VI

Security status of the systems

Article 35. *Systems security status report*

The Electronic Government Sector Committee will collect information regarding the condition of the main security variables in the information systems covered by this Royal Decree in such a way that it builds up a general profile on security within Public Administrations.

The National Cryptologic Centre will articulate the necessary procedures for collection and consolidation of information, as well as methodological aspects to process and exploit it, through the corresponding work groups set up for this purpose in the Electronic Government Sector Committee and in the ICT Strategy Commission for the General State Administration.

CHAPTER VII

Response to security incidents

Article 36. *Capacity to respond to incidents related to information security*

The National Cryptologic Centre (CCN) will articulate a response to security incidents related to the structure known as CCN-CERT (National Cryptologic Centre-Computer Emergency Reaction Team) which will act without prejudice to the response capacity for security incidents that could take place in each public administration, and the coordination function of the CCN at national and international level.

The Public Administrations shall notify the National Cryptologic Centre of any incidents with a significant impact on the security of the information handled and the services provided in relation to the system categorisation set out in Annex I to this Royal Decree.

Article 37. *Provision of services in response to security incidents to Public Administrations*

1. Pursuant to the terms of Article 36, the CCN-CERT will provide the Public Administrations with the following services:

a) Support and coordination for treating vulnerable aspects and solving of security incidents taking place in the General State Administration, regional Administrations, entities comprising Local Administrations and public Law Entities with their own legal status, that are linked to or depend on any of the preceding administrations.

Through its technical support and coordination service, the CCN-CERT will take prompt action to confront any aggression taking place in the Public Administration information systems.

To enforce compliance with the aforementioned objectives, audit reports from the affected systems will be used. In addition, audit logs, configurations and any other information considered relevant, as well as computer supports deemed necessary to investigate the incident in the affected systems, without prejudice to the provisions of Organic Law 15/1999, of 13 December, on the Protection of Personal Data, and implementing regulations, as well as possible institutional or organizational data confidentiality.

b) Investigation and disclosure of best information security practices among all the Public Administration members. For this purpose the CCN-STIC (National Cryptologic Centre-Security of Information and Communication Technologies) documents series prepared by the National Cryptologic Centre will provide rules, instructions, guidelines and recommendations for application by the National Security Framework to guarantee the security of Government information technologies systems.

c) Training for Government staff specialising in the security of information technologies, in order to update the knowledge of Government staff and arouse awareness and improve its capacities in detecting and controlling incidents.

d) Information about vulnerable aspects, alerts and warnings of new threats to information systems, gathered from different sources of renowned prestige, including own sources.

2. CCN will develop a framework which provides information, training, recommendations and the necessary tools so that the Public Administrations are able to respond to security incidents on their own. The CCN will be the coordinator of this framework at public state level.

CHAPTER VIII

Compliance regulations

Article 38. *Electronic sites and registries*

The security of electronic sites and registries and that of the electronic access of citizens to public services will be governed by the terms of the National Security Framework.

Article 39. *Life cycle of services and systems*

The security specifications will be included in the life cycle of services and systems, accompanied by the respective control procedures.

Article 40. *Control mechanisms*

Each Public Administration or Public Law Entity will establish its own control mechanisms to guarantee real and effective compliance with the National Security Framework.

Article 41. *Publication of compliance*

The bodies and Public Law Entities will publish the declarations of compliance and other distinctive signs of security, credited by them, obtained regarding the compliance with the National Security Framework in the respective electronic sites.

CHAPTER IX

Updating

Article 42. *Permanent update*

The National Security Framework will be permanently updated. It will be developed and completed over time, simultaneously to the progress of the e-government services, the evolution of technology and new international standards on the security and auditing of information systems and technologies, and at the same pace as the development of the infrastructures that support it.

CHAPTER X

Categorisation of the information systems

Article 43. *Categories*

1. In terms of security, the category of an information system will modulate the balance between the importance of the information it handles, the services it provides and the security effort required, depending on the risks to which it is exposed, based on the criterion of the principle of proportionality.

2. The determination of the category indicated above will be made based on the valuation of the impact that would have an incident affecting the security of the information or services with damage for the availability, authenticity, integrity, confidentiality or traceability, as security dimensions, following the procedure described in Annex I.

3. The evaluation of the consequences of a negative impact on the security of information and systems will be made based on their repercussion on the organisation's capacity to achieve its objectives, the protection of its assets, the compliance with its service obligations, respect for the law and the rights of citizens.

Article 44. *Authority*

1. The authority to conduct the evaluations referred to in Article 43 and subsequent amendments thereto, as applicable, will correspond to the person responsible for each piece of information or service, within the scope of their activity.

2. The authority to determine the category of the system will correspond to the person that is responsible for that system.

First additional provision. *Training*

Public Administration staff will receive, in accordance with the terms of additional provision two of Law 11/2007 of 22 June 2007, the necessary training to guarantee a sound knowledge of this National Security Framework; for this purpose the responsible organisations will provide the necessary elements to make this training an effective reality.

Second additional provision. *Public Administrations Information Security Committee*

The Public Administrations Security Information Committee, which reports to the e-government Sector Committee, will have one representative from each entity on that Sector Committee. It will have functions of cooperation in common matters related to the adaptation and implantation of the terms of the National Security Framework and of the rules, instructions, guidelines and recommendations issued for the application of that Plan.

Third additional provision. *Amendment of the Regulations implementing Organic Law 15/1999 (Protection of Personal Information), approved under Royal Decree 1720/2007 of 21 December, 2007*

Amendment of indent b), section 5 of Article 81 of the Regulations implementing Organic Law 15/1999 of 13 December 1999, on the Protection of Personal Information approved by Royal Decree 1720/2007 of 21 December 2007, which now reads as follows:

"b) whether they be files or treatments in which that information is contained, inadvertently or accessorily, without having any relation to their purpose."

Fourth additional provision. *Development of the National Security Framework*

1. Without prejudice to such proposals as may be agreed by the Electronic Government Sector Committee as may be established in Article 29, paragraph 2, the following technical safety instructions shall be developed and shall be binding on public administrations:

a) Security status report.
b) Notification of security incidents.

c) Security auditing.
d) Compliance with the National Security Framework.
e) Security product purchases.
f) Employment cryptology in the National Security Framework.
g) Interconnection in the National Security Framework.
h) Safety requirements in outsourced environments.

2. Such instructions shall be adopted in accordance with the procedure laid down in Article 29 (2) and (3).

Transitional provision. *Adaptation of systems*

1. The systems existing on the date of effect of this royal decree will be adapted to the National Security Framework so that they allow for compliance of what is set forth in final provision three of Law 11/2007 of 22 June 2007. The new systems will apply to what is established in this royal decree from the time they are conceived.

2. If, twelve months after the entry into effect of the National Security Framework, circumstances have arisen that make it impossible to apply what is set forth therein in full, an adaptation plan will be designed, defining the execution terms, which in no case will be more than 48 months after that plan has taken effect.

The plan referred to above will be prepared well in advance and approved by the competent higher institutions.

3. Until such time as a security policy has been approved by the competent higher institution, the security policies existing at executive management level will apply.

Single repealing provision.

All provisions of equal or lesser rank that oppose the terms of the present regulation are hereby derogated.

Final provision one. *Qualifying title*

This royal decree is issued by virtue of the terms of Article 149.1.18 of the Spanish Constitution, which attributes authority over the rules governing the legal regime of Public Administrations to the State.

Final provision two. *Regulatory development*

The Minister of the Presidency is authorised to issue the necessary provisions for the implementation and application of the terms of this royal decree, without prejudice to the authority of the regional authorities to implement and execute the basic State legislation.

Final provision three. *Entry into effect*

This royal decree will come into force the day after its publication in the “Official State Gazette”.

In Madrid, on 8 January 2010.

JUAN CARLOS R.

The First Deputy Prime Minister and Minister of the Presidency,
MARÍA TERESA FERNÁNDEZ DE LA VEGA SANZ

ANNEXES

ANNEX I System categories

1. Grounds for determining the category of a system.

The determination of a system category is based on evaluating the impact that an incident affecting the security of the information or systems would have on the organisation, with repercussions on the organisation's capacity to:

a) Fulfil its objectives.
b) Protect the assets under its charge.
c) Comply with its daily service obligations.
d) Respect current legislation.
e) Respect the rights of people.

Determining the category of a system will be done in accordance with the terms of this royal decree and will apply to all the systems used for providing e-government services and support in general administrative procedures.

2. Security dimensions.

To determine the impact that an incident affecting the security of the information or systems would have on the organisation and establish the system category, the following security dimensions will be considered, identified by their respective initials (in Spanish) in block capitals:

a) Availability [Av].
b) Authenticity [A].
c) Integrity [I].
d) Confidentiality [C].
e) Traceability [T].

3. Determination of the level required in a security dimension.

Information or services may be affected with respect to one or more of their security dimensions. Each security dimension affected will be included in one of the following levels: LOW, INTERMEDIATE or HIGH. If a security dimension is no affected, it will not be included in any level.

a) LOW level. This is used if the consequences of security incident affecting any of the security dimensions imply limited damage to the functions of the organisation, its assets or the people affected.

Limited damage is taken as the following:

1º. A considerable reduction in the capacity of the organisation to effectively deal with its usual obligations, even though these continue to be executed.
2º. Minor damage done to the assets of an organisation.
3º. Formal breach of a law or regulation that can be remedied.
4º. Damages caused to a person, which, albeit problematic, can easily be repaired.
5º. Others of a similar nature.

b) INTERMEDIATE level. This is used when the consequences of a security incident affecting any of the security dimensions entail serious damage to the functions of an organisation, its assets or the persons affected.

Serious damage is taken as:

1º. A significant reduction in the organisation's capacity to deal efficiently with its fundamental obligations, even though these continue to be executed.
2º. Significant damage done to the assets of the organisation.
3º. Material breach of a law or regulation or a formal breach that cannot be remedied.
4º. That which causes significant damage to a person and is difficult to repair.
5º. Others of a similar nature.

c) HIGH level. This is used when the consequences of a security incident affecting any of the security dimensions entails very serious damage to the functions of the organisation, its assets or the persons affected.

Very serious damage is taken as the following:

1º. The annulment of the organisation's capacity to deal with its fundamental obligations and if it is not possible to execute them.

2º. Very serious, irreparable damage caused to the organisation's assets.

3º. Serious breach of a law or regulation.

4º. Causing serious harm to a person that is difficult or impossible to repair.

5º. Others of a similar nature.

When a system handles different types of information and provides different services, the system level in each dimension will be the highest of those established for each type of information and each service.

4. Determination of the category of an information system.

1. Three categories are defined: BASIC, INTERMEDIATE and HIGH.

a) An information system is categorised as HIGH if any of its security dimensions is included in the HIGH level.

b) An information system is categorised as INTERMEDIATE if any of its security dimensions is included in the INTERMEDIATE level and none is included in a higher level.

c) An information system is categorised as BASIC if any of its security dimensions is included in the LOW level and none of them is included in a higher level.

2. The determination of the category of a system based on what is set forth above does not mean that the level of the security dimensions not affecting the determination of that category is altered as a result.

5. Sequence of actions to determine the category of a system:

1. Identification of the respective level of each type of information and service, depending on their security dimensions, and considering what is set forth in section 3.

2. Determination of the category of a system, depending on what is set forth in section 4.

ANNEX II Security measures

1. General provisions

1. To achieve compliance with the basic principles and minimum requirements established, the security measures indicated in this annex will be applied, which will be proportionate to:

a) The relevant security dimensions of the system to be protected.

b) The category of the information system to be protected.

2. The measures are divided into three groups:

a) Organisational framework [org]. This is constituted by the group of measures related to overall security organisation.

b) Operational framework [op]. This is constituted by the measures to be taken to protect the system operation as an integral series of components for achieving a purpose.

c) Protective measures [mp]. These are focused on protecting specific assets, depending on their nature and the quality required by the security level of the dimensions that are affected.

2. Selecting the security measures

1. In selecting the security measures, the following steps will be taken:

a) Identification of the types of assets present.

b) Establishment of the relevant security dimensions, taking into account the provisions of Annex I.

c) Establishment of the level that corresponds to each security dimension, in accordance with the provisions of Annex I.

d) Identification of the system category, pursuant to the terms of Annex I.

e) Selection of the appropriate security measures from those set forth in this annex, in accordance with the security dimensions and their levels, and for specific security measures, in accordance with the system category.

2. For the purposes of facilitating compliance with the terms of this annex, when an information system contains systems that require the application of a different level of security measures from that of the main system, they may be separated from the latter, and the respective security measures level will be applied in each case, provided that the information and services affected can be defined.

3. The list of measures selected will be drawn up in a document called the Declaration of Applicability, which must be signed by the person responsible for system security.

4. The correspondence between the security levels required in each dimension and the security measures is indicated in the following table:

Dimensions				Security measures	
Affected	Basic/Low	Intermediate	High		
				org	**Organisational framework**
Category	applicable	=	=	org.1	Security policies
Category	applicable	=	=	org.2	Security standards
Category	applicable	=	=	org.3	Security procedures
Category	applicable	=	=	org.4	Authorisation process
				op	**Operational framework**
				op.pl	Planning
Category	applicable	+	++	op.pl.1	Risk analysis
Category	applicable	+	++	op.pl.2	Security architecture
Category	applicable	=	=	op.pl.3	Acquisition of new components
Av	n.a.	applicable	=	op.pl.4	Dimensioning / Capacity management
Category	n.a.	n.a.	applicable	op.pl.5	Certified components
				op.acc	Access control measures
AT	applicable	=	=	op.acc.1	Identification
ICAT	applicable	=	=	op.acc.2	Access requirements
ICAT	n.a.	applicable	=	op.acc.3	Separation of functions and tasks
ICAT	applicable	=	=	op.acc.4	Access rights management process
ICAT	applicable	+	++	op.acc.5	Authentication mechanism
ICAT	applicable	+	++	op.acc.6	Local access (local logon)
ICAT	applicable	+	=	op.acc.7	Remote access (remote login)
				Op.exp	Operations
Category	applicable	=	=	op.exp.1	Inventory of assets
Category	applicable	=	=	op.exp.2	Security configuration
Category	n.a.	applicable	=	op.exp.3	Configuration management
Category	applicable	=	=	op.exp.4	Maintenance
Category	n.a.	applicable	=	op.exp.5	Change management
Category	applicable	=	=	op.exp.6	Protection against malicious code
Category	n.a.	applicable	=	op.exp.7	Incident management
T	applicable	+	++	op.exp.8	Log of user activity
Category	n.a.	applicable	=	op.exp.9	Incident management log
T	n.a.	n.a.	applicable	op.exp.10	Activity log protection
Category	applicable	+	=	op.exp.11	Protection of cryptographic keys
				op.ext	External services
Category	n.a.	applicable	=	op.ext.1	Contracting and service-level agreements
Category	n.a.	applicable	=	op.ext.2	Daily management
Av	n.a.	n.a.	applicable	op.ext.9	Alternative means
				op.cont	Continuity of service
Av	n.a.	applicable	=	op.cont.1	Impact analysis
Av	n.a.	n.a.	applicable	op.cont.2	Continuity plan
Av	n.a.	n.a.	applicable	op.cont.3	Regular tests
				op.mon	System monitoring
Category	n.a.	applicable	=	op.mon.1	Detection of intruders
Category	applicable	+	++	op.mon.2	Metrics system

Dimensions				Security measures	
Affected	Basic/Low	Intermediate	High		
				mp	Protective measures
				mp.if	Protection of facilities and infrastructure
Category	applicable	=	=	mp.if.1	Separate areas with access control
Category	applicable	=	=	mp.if.2	Identification of individuals
Category	applicable	=	=	mp.if.3	Outfitting of sites
Av	applicable	+	=	mp.if.4	Electrical power
Av	applicable	=	=	mp.if.5	Fire protection
Av	n.a.	applicable	=	mp.if.6	Flood protection
Category	applicable	=	=	mp.if.7	Logs of equipment entry and exit
Av	n.a.	n.a.	applicable	mp.if.9	Alternative facilities
				mp.per	Personnel management
Category	n.a.	applicable	=	mp.per.1	Job description
Category	applicable	=	=	mp.per.2	Duties and obligations
Category	applicable	=	=	mp.per.3	Awareness
Category	applicable	=	=	mp.per.4	Training
Av	n.a.	n.a.	applicable	mp.per.9	Alternative personnel
				mp.eq	Equipment protection
Category	applicable	+	=	mp.eq.1	Tidy work stations
A	n.a.	applicable	+	mp.eq.2	Blocking of work stations
Category	applicable	=	+	mp.eq.3	Protection of laptops
Av	n.a.	applicable	=	mp.eq.9	Alternative means
				mp.com	Communications protection
Category	applicable	=	+	mp.com.1	Safe perimeter
C	n.a.	applicable	+	mp.com.2	Confidentiality protection
IA	applicable	+	++	mp.com.3	Protection of authenticity and integrity
Category	n.a.	n.a.	applicable	mp.com.4	Separation of networks
Av	n.a.	n.a.	applicable	mp.com.9	Alternative means
				mp.si	Protection of information carriers
C	applicable	=	=	mp.si.1	Labelling
IC	n.a.	applicable	+	mp.si.2	Cryptography
Category	applicable	=	=	mp.si.3	Custody
Category	applicable	=	=	mp.si.4	Transport
C	applicable	+	=	mp.si.5	Erasure and destruction
				mp.sw	Protection of software applications
Category	n.a.	applicable	=	mp.sw.1	Development
Category	applicable	+	++	mp.sw.2	Acceptance and commissioning
				mp.info	Information protection
Category	applicable	=	=	mp.info.1	Personal data
C	applicable	+	=	mp.info.2	Information assessment
C	n.a.	n.a.	applicable	mp.info.3	Ciphering
IA	applicable	+	++	mp.info.4	Electronic signature
T	n.a.	n.a.	applicable	mp.info.5	Time stamping
C	applicable	=	=	mp.info.6	Cleaning documents
Av	applicable	=	=	mp.info.9	Backup copies (backup)
				mp.s	Services protection
Category	applicable	=	=	mp.s.1	E-mail protection
Category	applicable	=	+	mp.s.2	Protection of web services and applications
Av	n.a.	applicable	+	mp.s.8	Protection against denial of services
Av	n.a.	n.a.	applicable	mp.s.9	Alternative means

The following conventions are used in the tables of this annex:

a) To indicate that a determined security measure must be applied to one or several security dimensions at a specific level, the term “applicable” is used.

b) “n.a.” means “not applicable”.

c) To indicate that the requirements of a level are equal to those of a lower level, the sign “=“ is used.

d) To indicate an increase in requirements, graded in accordance with the security dimension level, the signs “+” and “++” are used.

e) To indicate that a measure specifically protects a certain security dimension, this is explained by its initial.

f) In the tables of this Annex green, yellow and red colours have been used the following way: the green colour to indicate that a certain measure is applied in BASIC or superior category systems; the yellow to indicate the measures that begin to be applied in

INTERMEDIATE or superior category; the red one to indicate the measures that are only of implementation in HIGH category.

3. Organisational framework [org]

The organisational framework is constituted by a set of measures related to the overall organisation of security.

3.1 Security policy [org.1].

Dimensions	All		
Category	basic	intermediate	high
	applicable	=	=

The security policy will be approved by the respective higher competent authority, in accordance with the provisions of Article 11, and will be set out in a written document in which the following at least is clearly specified:

a) The objectives or mission of the organisation.
b) The legal and regulatory framework in which the activities are to be implemented.
c) The security roles or functions, defining for each, the duties and responsibilities of the position and the procedure for the designation and removal thereof.
d) The structure of the committee or committees responsible for the management and coordination of security, detailing their scopes of responsibility, the members and their relation with other elements of the organisation.
e) The guidelines for structuring the system security documents, and their management and access.

The security policy will make reference to and be coherent with the provisions of the Security Document required by Royal Decree 1720/2007, in all areas that apply.

3.2 Security regulations [org.2].

Dimensions	All		
Category	basic	intermediate	high
	applicable	=	=

A series of documents will be available, describing:

a) The correct use of equipment, services and facilities.

b) What is considered as improper use.

c) The responsibility of the staff with respect to compliance with or breach of these regulations: rights, duties and disciplinary measures in accordance with current legislation.

3.3 Security procedures [org.3].

Dimensions	All		
Category	basic	intermediate	high
	applicable	=	=

A series of documents will be available, indicating clearly and precisely:

a) How to perform the habitual tasks.
b) Who must perform each task.
c) How to identify and report irregular behaviours.

3.4 Authorisation process [org.4].

Dimensions	All		
Category	basic	intermediate	high
	applicable	=	=

A formal process will be established for authorisations, covering all the elements of the information system:

a) Habitual and alternative use of the facilities.
b) Incorporation of equipment in production, particularly equipment that involves cryptography.

c) Incorporation of applications in production.
d) Establishing of communications links with other systems.
e) Use of habitual and alternative communication methods.
f) Use of information devices.
g) Use of mobile equipment. Mobile equipment is taken as including laptop computers, PDAs or other similar equipment.
h) Use of third party services, under contract or agreement.

4. Operational framework [op]

The operational framework is comprised of the measures to be taken to protect the system as an integral part of components for a purpose.

4.1 Planning [op.pl].

4.1.1 Risk analysis [op.pl.1].

Dimensions	All		
Category	basic	intermediate	high
	applicable	+	++

BASIC category

An informal analysis will suffice, performed in a natural language. I.e., a textual expression describing the following aspects:

a) Identifying the most valuable assets in the system.
b) Identifying the most likely threats.
c) Identifying safeguards to protect against those threats.
d) Identifying the main residual risks.

INTERMEDIATE category

A semi-formal analysis will be made, using a specific language, with a basic catalogue of threats and defined semantics. In other words, a presentation with tables describing the following aspects:

a) Identification and qualitative evaluation of the most valuable assets in the system.
b) Identifying and quantifying the most likely threats.
c) Identifying and evaluating safeguards to protect against those threats.
d) Identifying and evaluating the main residual risks.

HIGH category

A formal analysis will be made, using a specific language, with internationally-recognised mathematical grounds. The analysis will include the following aspects:

a) Identification and qualitative evaluation of the most valuable assets in the system.
b) Identifying and quantifying the most likely threats.
c) Identifying vulnerable areas that could propitiate those threats.
d) Identifying and evaluating the adequate safeguards.
e) Identifying and evaluating residual risks.

4.1.2 Security architecture [op.pl.2].

Dimensions	All		
Category	basic	intermediate	high
	applicable	+	++

System security will be subjected to an integral approach, detailing at least the following aspects:

BASIC category

a) Documentation on facilities:

1. Areas.
2. Access points.

b) Documentation on the system:

1. Equipment.
2. Internal networks and connections to the exterior.
3. Access points to the system (work stations and administration consoles).

c) Lines of defence scheme:
1. Interconnection points to other systems or networks, particularly in relation to the Internet or public networks in general.
2. Firewalls, DMZ, etc.
3. Use of different technologies to prevent vulnerable areas that could lead to the simultaneous perforation of several defence lines.

d) System for identifying and authenticating users:

1. Use of shared keys, passwords, ID cards, biometrics or other similar elements.
2. Use of files or directories for authenticating users and determining their rights of access.

INTERMEDIATE category

e) Management system, relating to planning, organization and control of information security resources.

HIGH category

f) Information security management system with regular updating and approval.

g) Internal technical controls:

1. Validation of input, output and intermediate data.

4.1.3 Acquisition of new components [op.pl.3].

Dimensions	All		
Category	basic	intermediate	high
	applicable	=	=

A formal process is established for planning the acquisition of new system components. This process will:

a) Be based on the conclusions of the risk analysis: [op.pl.1].
b) Be in accordance with the chosen security architecture: [op.pl.2].
c) Include the technical, training and joint financing requirements.

4.1.4 Dimensioning / management of capacities [op.pl.4].

Dimensions	Av		
Level	low	intermediate	high
	n/a	applicable	=

INTERMEDIATE level

Prior to putting into operation, a study will be made of the following aspects:

a) Processing needs.
b) Information storage needs: during processing and during the retention period.
d) Communication needs.
e) Personnel needs: number and professional qualifications.
f) Needs in terms of facilities and auxiliary resources.

4.1.5 Certified components [op.pl.5].

Dimensions	All		
Category	basic	intermediate	high
	n/a	n/a	applicable

HIGH category

The security functionalities and level of the systems, products and equipment used must have been assessed in accordance with European or international standards and their certificates must be recognised by the Spanish National Assessment and Certification Scheme for Information Technology Security.

European or international regulations are considered to be ISO/IEC 15408 or others of a similar nature and quality.

A technical safety instruction manual shall provide details of the necessary criteria.

4.2 Access control. [op.acc].

Access control covers all preparatory and executive activities to ensure that a determined entity, user or process can or cannot access a system resource in order to perform a specific action.

The access control implanted in a real system will be a point of equilibrium between ease of use and protection of the information. In Low level systems, priority will be attached to ease of use, whereas in High level systems, priority will be attached to protection.

In all access controls, the following will be required:

a) All access will be prohibited, unless expressly granted.

b) The entity must be specifically identified [op.acc.1].

c) The use of the resources will be protected [op.acc.2].

d) For each entity, the following parameters will be defined: what is to be accessed, with what rights and with what authorisation [op.acc.4].

e) The people authorising, using and controlling use will be different persons [op.acc.3].

f) The identity of the entity will be sufficiently authenticated [mp.acc.5].

g) Both local access ([op.acc.6]) and remote access ([op.acc.7]) will be controlled.

Through compliance with all the indicated measures, it is guaranteed that no-one can access resources without authorisation. Furthermore, the use of the system will be recorded ([op.exp.8]) in order to detect and take action in the face of any accidental or deliberate fault that occurs.

When systems are interconnected in which the identification, authentication and authorisation take place in different security domains, under different responsibilities, in cases in which required, local security measures will be accompanied by the respective collaborative agreements that define effective mechanisms and procedures for assigning responsibilities in the case of each system ([op.ext]).

4.2.1 Identification [op.acc.1].

Dimensions	AT		
Level	low	intermediate	high
	applicable	=	=

Identification of the users of a system will be done in accordance with what is set forth below:

1. The identification systems mentioned in the applicable legislation may be used as a unique identifier.

2. When the user has different roles in the system (e. g. a citizen, an internal employee of the organization and a system administrator), he or she will receive unique identifiers for each case so that privileges and activity records are always designated.

3. Each entity (user or process) that accesses the system will have a unique identifier in such a way that:

a) You can find out who receives access and what access rights they receive.

b) You can find out who has done something and what they have done.

4. User accounts will be managed as follows:

a) Each account shall be associated with a unique identifier.

b) Accounts must be disabled in the following cases: when the user leaves the organization; when the user ceases to be required to perform the function for which the user account was required; or, when the person who authorized it orders otherwise.

c) The accounts shall be retained for the period required to meet the traceability needs of the associated activity records. This period shall be referred to as the retention period.

5 In the cases referred to in Chapter IV on "Electronic Communications", the participating parties shall identify themselves in accordance with the mechanisms provided for in the relevant European and national legislation, with the following correspondence between the levels of the authenticity dimension of the information systems to which they have access and the levels of security (low, substantial, high) of the electronic identification systems provided for in Regulation (EU) No. 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC:

– If a LOW level of authenticity dimension is required (Annex I): Low, substantial or high level of security (Article 8 of Regulation No 910/2014).

– If a INTERMEDIATE level in the authenticity dimension (Annex I) is required: Substantial or high level of security (Article 8 of Regulation No 910/2014)

– If a HIGH level in the authenticity dimension (Annex I) is required: High security level (Article 8 of Regulation No 910/2014).

4.2.2 Access requirements [op.acc.2].

Dimensions	ICAT		
Level	low	intermediate	high
	applicable	=	=

The access requirements will be in keeping with what is specified below:

a) The system resources will be protected with a mechanism that prevents them from being used, except entities that have sufficient access rights.

b) Access rights for each resource will be established based on the decisions of the staff responsible for the resource, in keeping with the system security policy and regulations.

c) In particular, access to components and the files or configuration records of the former will be controlled.

4.2.3 Separation of functions and tasks [op.acc.3].

Dimensions	ICAT		
Level	low	intermediate	high
	n/a	applicable	=

INTERMEDIATE level

The access control system will be organised so that two or more persons must be present at once for performing critical tasks, without the option of just one person being authorised, who could make an improper use of his/her rights to commit an illicit action.

Specifically, at least the following functions will be separated:

a) Operation development.
b) Configuration and maintenance of the operating system.
c) Auditing or the supervision of any other function.

4.2.4 Access rights management process [op.acc.4].

Dimensions	ICAT		
Level	low	intermediate	high
	applicable	=	=

The access rights of each user will be restricted, based on the following principles:

a) Minimum privilege. The privileges of each user will be reduced to the minimum that is strictly necessary for the user to fulfil his/her obligations. In this way any accidental or deliberate damage that could be caused by an entity will be restricted.

b) Need to know. The privileges will be limited so that users are only allowed to access the information they need to know to comply with their obligations.

c) Authorisation capability. Only staff who are authorised to do so may know, alter or cancel authorisation to access the resources, in accordance with the criteria set forth by the responsible for those resources.

4.2.5 Authentication mechanism [op.acc.5].

dimensions	ICAT		
level	low	intermediate	high
	applicable	+	++

The authentication mechanisms for the system will be adapted to the system level, based on the considerations below, and the following authentication factors may be used.

– “something that you know": passwords or shared keys.

– “something you have": logical components (such as software certificates) or physical devices (tokens).

– “something that is”: biometric elements.

The aforementioned factors may be used alone or combined to generate strong authentication mechanisms.

The CCN-STIC guidelines will develop the appropriate concrete mechanisms for each level.

The instances of the authentication factor (s) used in the system will be called credentials.

Before providing authentication credentials to users, they must be identified and registered reliably with the system or with an electronic identity provider recognized by the Administration. Several possibilities for registering users are envisaged:

– By means of the user's physical presentation and verification of his/her identity in accordance with current legislation, before an official authorized to do so.

– Telematically, by means of an electronic ID card or a qualified electronic certificate.

– Telematically, using other legally accepted systems to identify citizens covered by the applicable legislation.

LOW level

a) As a general principle, the use of any single-factor authentication mechanism shall be permitted.

b) If used as a "known" factor, basic quality rules shall apply.

c) Credential security shall be ensured so that:

1. Credentials will be activated once they are under the effective control of the user.
2. The credentials will be under the sole control of the user.
3. The user shall acknowledge that he has received them and that he knows and accepts the obligations involved in their possession, in particular the duty of diligent custody, protection of their confidentiality and immediate information in the event of loss.
4. The credentials will be changed periodically according to the organization's policy, depending on the category of the system being accessed.
5. Credentials will be removed and disabled when the entity (person, team or process) they authenticate terminates its relationship with the system.

INTERMEDIATE level

a) The use of at least two authentication factors shall be required.

b) In the case of the use of "something known" as an authentication factor, stringent quality and renewal requirements shall be established.

c) The credentials used must have been obtained after prior registration:

1. Face-to-face.
2. Telematics using qualified electronic certificate.
3. Telematics by means of authentication with an electronic credential obtained after a face-to-face or telematic pre-registration using a qualified electronic certificate in a qualified signature creation device.

HIGH level

a) Credentials shall be suspended after a defined period of non-use.

b) In the case of using "something that is held", the use of hardware cryptographic elements using algorithms and parameters accredited by the National Cryptologic Centre will be required.

c) The credentials used must have been obtained after pre-registration in person or telematically using qualified electronic certificate as a qualified signature-creation device.

4.2.6 Local access [op.acc.6].

dimensions	ICAT		
level	low	intermediate	high
	applicable	+	++

Local access is considered access made from work stations on the organisation’s premises. Such access will take into account the security dimensions level:

LOW level

a) Attacks that could disclose information in the system without accessing it will be prevented. All information disclosed to the party attempting to gain access will be the minimum essential information (access dialogues will only provide information that is strictly necessary).

b) The number of attempts permitted will be limited, blocking opportunity of access once a certain number of consecutive failed attempts have been made.

c) Successful accesses and failed attempts will be recorded.

d) The system will inform users of their obligations immediately after gaining access.

INTERMEDIATE level

Users will be informed of the last access made using their identity.

HIGH level

a) Access will be restricted by time, date and place from which the access is made.

b) The points where the system requires a renewal of the user’s authentication will be defined by a single identifier, and an established session will not be sufficient.

4.2.7 Remote access [op.acc.7].

dimensions	ICAT		
level	low	intermediate	high
	applicable	+	=

Remote access is defined as access made from outside the organisation’s premises, through third-party networks.

LOW level

The system's security will be guaranteed when users or other entities gain remote access, which means protecting both the access itself (as in [op.acc.6]) and the remote access channel (as in [mp.com.2] and [mp.com.3]).

INTERMEDIATE level

A special policy will be established covering all elements that can be processed remotely, and positive authorisation will be required.

4.3 Operations [op.exp].

4.3.1 Inventory of assets [op.exp.1].

dimensions	All		
Category	basic	intermediate	high
	applicable	=	=

An updated inventory will be kept of all the system elements, describing their nature, and identifying their owners; i.e., the person responsible for all decisions in relation to them.

4.3.2 Security configuration [op.exp.2].

dimensions	All		
Category	basic	intermediate	high
	applicable	=	=

The equipment will be configured before being put into operation, so that:

a) All standard accounts and passwords are eliminated.
b) The “minimum functionality” rule is applied:

1º. The system will provide the required functionality for the organisation to achieve its objectives, and no other functionality.
2º. It will not provide free functionalities or operating, administrative or auditing functions, thereby reducing its perimeter to the minimum one necessary.
3º. All functions that are of no interest, unnecessary and those that are not appropriate for the purpose that is to be achieved will be eliminated or deactivated by controlling the configuration.

c) The “security by default” rule will be applied:

1º. The security measures will show respect for users and protect them, unless they consciously expose themselves to risks.
2º. To reduce the security, users will perform conscious actions.
3º. Natural use, in cases in which the user has not consulted the manual, will be safe use.

4.3.3. Configuration management [op.exp.3].

dimensions	All		
Category	basic	intermediate	high
	n/a	applicable	=

INTERMEDIATE category

The configuration of the system components will be constantly managed so that:

a) The ‘minimum functionality’ rule ([op.exp.2]) is maintained at all times.
b) The ‘security by default’ rule ([op.exp.2]) is maintained at all times.
c) The system is adapted to new needs that have been previously authorised ([op.acc.4]).
d) The system reacts to reported vulnerabilities ([op.exp.4]).
e) The system reacts to incidents (see [op.exp.7]).

4.3.4 Maintenance [op.exp.4].

dimensions	All		
Category	basic	intermediate	high
	applicable	=	=

The following is provided, for maintenance of the physical and logical equipment that comprises the system:

a) The manufacturers’ specifications will be applied for all matters relating to installation and maintenance of the systems.

b) Ongoing monitoring of faults reported will be carried out.

c) A procedure will be established for analysing, giving priority to and determining when to apply security actions, patches, improvements and new releases. Such assigning of priorities will take into account the variation of the risk depending on whether updating is applied or not.

4.3.5 Change management [op.exp.5].

dimensions	All		
Category	basic	intermediate	high
	n/a	applicable	=

INTERMEDIATE category

Constant control will be maintained of changes made to the system, so that:

a) All changes announced by the manufacturer or supplier will be analysed to determine their appropriateness in order to decide whether or not they will be incorporated.

b) Before producing a new release or patched release, a check will be made on equipment not used for production to ensure that the new installation functions properly and does not impair the effectiveness of the functions that are necessary for daily operations. The test equipment will be equivalent to the production equipment as regards the aspects tested.

c) Changes will be planned to reduce any impact on the provision of the services affected.

d) A risk analysis will be carried out to determine whether the changes are relevant for the security of the system. All changes involving a situation of risk at a high level will be expressly approved prior to being implanted.

4.3.6 Protection from malicious codes [op.exp.6].

dimensions	All		
Category	basic	intermediate	high
	applicable	=	=

Malicious codes include: viruses, worms, trojans, spyware and in general, all element known as “malware”.

Mechanisms will be implanted to prevent and take action in the presence of malicious codes, through maintenance based on the manufacturer’s recommendations.

4.3.7 Incident management [op.exp.7].

dimensions	All		
Category	basic	intermediate	high
	n/a	applicable	=

INTERMEDIATE category

An integral process will be implemented to deal with incidents that could affect system security, including:

a) Procedure for reporting security events and weaknesses, detailing the classification criteria and notification escalation.

b) A procedure for taking urgent measures, such as stopping services, isolating the affected system, collecting evidence and protecting records, whichever applies, depending on the case.

c) A procedure for assigning staff to investigate the causes, analyse the consequences and resolve the problem.

d) Procedures for informing all interested parties (internal and external).

e) Procedures for:

1. Preventing a repetition of the incident.
2. Including the identification of and method for dealing with the incident in the user procedures.
3. Updating, extending, improving or optimising procedures for resolving incidents.

The management of incidents affecting personal information will take into consideration the provisions of Organic Law 15/1999 of 13 December 1999, and the regulations that implement this act, without prejudice to also complying with the measures set forth in this royal decree.

4.3.8 Recording of user activity [op.exp.8].

dimensions	T		
level	low	intermediate	high
	applicable	+	++

The activities of system users will be recorded, such that:

a) The record indicates who carried out the activity, when and in respect of what information.

b) User activity will be included and, in particular, that of operators and administrators insofar as they are able to access the configuration and act on the maintenance of the system.

c) A record must be kept of all activities carried out successfully and of failed attempts.

d) Determining which activities should be recorded and in what detail will be decided in the light of the risk analyses performed on the system ([op.pl.1]).

LOW level

The activity logs on the servers will be activated.

INTERMEDIATE level

Activity records will be reviewed informally for abnormal patterns.

HIGH level

There will be an automatic system for recording and correlation of events, i. e. a centralized security console.

4.3.9 Incident management log [op.exp.9].

dimensions	All		
Category	basic	intermediate	high
	n/a	applicable	=

INTERMEDIATE category

All actions related to incident management will be recorded such that:

a) The initial report is recorded, as well as emergency actions and changes made to the system as a result of the incident.

b) Evidence that could subsequently be used in a lawsuit or to oppose that lawsuit will be recorded if the incident could lead to disciplinary actions being taken against staff, external suppliers or the prosecution of offences. Special legal advisory services will be used to determine the composition and detail of such evidence.

c) As a result of analysing the incidents, the determination of events as auditable will be reviewed.

4.3.10 Protection of activity records [op.exp.10].

dimensions	T		
level	low	intermediate	high
	n/a	n/a	applicable

HIGH level

The system records will be protected in order to:

a) Determine the record retention period.

b) Ensure the date and time. See [mp.info.5].

c) The records may not be modified or deleted by unauthorised personnel.

d) Security copies, where applicable, must comply with the same requirements.

4.3.11 Protection of cryptographic keys [op.exp.11].

dimensions	All		
Category	basic	intermediate	high
	applicable	+	=

Cryptographic keys will be protected during their whole life cycle: (1) generation, (2) transportation to the operating point, (3) custody during operations, (4) subsequent filing upon their removal from active operation and (5) eventual destruction.

BASIC category

a) The generation resources will be separated from the operating resources.

b) The operating codes that have been removed and must be filed will be filed in resources that are separate from the operating resources.

INTERMEDIATE category

a) Evaluated programmes or certified cryptographic devices will be used, in accordance with [op. pl. 5].

b) Algorithms accredited by the National Cryptologic Centre will be used.

4.4 External services [op.ext].

When using resources outside the organisation, comprising services, equipment, installations or staff, it must be considered that delegation is limited to their functions.

The organisation will at all times continue to be responsible for risks that are incurred as they affect the information being processed and the final services provided by the organisation.

The organisation will have the necessary resources to exercise its responsibilities and maintain control at all times.

4.4.1 Contracts and service level agreements [op.ext.1].

dimensions	All		
Category	basic	intermediate	high
	n/a	applicable	=

INTERMEDIATE category

Before using external resources, the characteristics of the services provided and the responsibilities of each party will be established through a contract. A description of what the minimum quality of the service provided entails and the consequences of breach will be given.

4.4.2 Daily management [op.ext.2].

dimensions	All		
Category	basic	intermediate	high
	n/a	applicable	=

INTERMEDIATE category

For the daily management of the system, the following points are established:

a) A routine system for measuring compliance with service obligations and a procedure for neutralising any deviations outside the agreed tolerance margin ([op.ext.1]).
b) A mechanism and coordination procedures for carrying out maintenance work on the systems covered by the contract.
c) The coordination procedures and mechanism in the event of incidents and disasters (see [op.exp.7]).

4.4.3 Alternative means [op.ext.9].

dimensions	A		
level	low	intermediate	high
	n/a	n/a	applicable

HIGH level

Service provision will be assured using alternative means in the event of the unavailability of the contracted service. The alternative service will have the maximum guarantees of security as the habitual service.

4.5 Continuity of the service [op.cont].

4.5.1 Impact analysis [op.cont.1].

dimensions	Av		
level	low	intermediate	high
	n/a	applicable	=

INTERMEDIATE level

An impact analysis will be made to allow the following to be determined:

a) The availability requirements for each service, measured as the impact of an interruption during a certain period of time.
b) The elements that are critical in providing each service.

4.5.2 Continuity plan [op.cont.2].

dimensions	A		
level	low	intermediate	high
	n/a	n/a	applicable

HIGH level

A continuity plan will be developed, establishing the actions to be executed in the event that the services provided using the habitual resources are interrupted. This plan will include the following aspects:

a) The functions, responsibilities and activities to be carried out will be identified.
b) A forecast will be drawn up of alternative means that can be used, in order to continue to provide the services.

c) All the alternative means will be planned and materialised through agreements or contracts with the respective suppliers.

d) All persons affected by the plan will receive special training on their role in that plan.

e) The continuity plan will form an inseparable and harmonious part of the organisation’s continuity plans regarding other aspects apart from security.

4.5.3 Regular tests [op.cont.3].

dimensions	A		
level	low	intermediate	high
	n/a	n/a	applicable

HIGH level

Regular tests will be performed to locate and correct any errors or faults that might exist in the continuity plan

4.6 System monitoring [op.mon].

The system will be subject to monitoring measures on its activity.

4.6.1 Detection of intruders [op.mon.1].

dimensions	All		
Category	basic	intermediate	high
	n/a	applicable	=

INTERMEDIATE category

Tools will be put in place to detect or prevent intruders.

4.6.2 Metrics system [op.mon.2].

dimensions	All		
Category	basic	intermediate	high
	applicable	+	++

BASIC category:

The necessary data shall be collected taking into account the system category in order to ascertain the degree of implementation of the security measures they apply from details given in Annex II and, where appropriate, to provide the annual report required by Article 35.

INTERMEDIATE category:

In addition, data will be collected to assess the incident management system, providing

– Number of security incidents handled.
– Time taken to close 50% of incidents.
– Time taken to close 90% of incidents.

HIGH category

Data will be collected to determine the efficiency of the ICT security system:

– Resources consumed: hours and budget.

5. Protective measures [mp]

The protective measures will be focused on protecting specific assets, depending on their nature, with the required level for each security dimension.

5.1 Protection of premises and infrastructures [mp.if].

5.1.1 Separate areas, with access control [mp.if.1].

dimensions	All		
Category	basic	intermediate	high
	applicable	=	=

The equipment will be installed in separate areas for their function.

Accesses to the areas will be controlled so that persons can only enter through the foreseen entrances, which will be controlled.

5.1.2 Personal identification [mp.if.2].

dimensions	All		
category	basic	intermediate	high
	applicable	=	=

The access control mechanism will be in keeping with the following provisions:

a) All persons entering the premises where there is equipment forming part of the information system will be identified.

b) The access and exit of all persons will be controlled.

5.1.3 Conditioning of the premises [mp.if.3].

dimensions	all		
category	basic	intermediate	high
	applicable	=	=

The premises where the information systems and their components are located will have the appropriate elements to guarantee the effective operation of the equipment installed there. In particular:

a) Conditions of temperature and humidity.

b) Protection against threats identified in the risk analysis.

c) Protection of the wiring against chance or deliberate incidents.

5.1.4 Electricity [mp.if.4].

dimensions	Av		
level	low	intermediate	high
	applicable	+	=

LOW level

The premises where the information systems and their components are located will have electricity and the respective connections that are needed for them to function, in such a way that:

a) The supply of electricity is guaranteed.

b) The correct functioning of the emergency lights is guaranteed.

INTERMEDIATE level

An electricity supply will be guaranteed for the systems in the event of a failure in the mains supply, guaranteeing sufficient time for an orderly completion of the processes and safeguarding the information.

5.1.5 Protection against fire [mp.if.5].

dimensions	Av		
level	low	intermediate	high
	applicable	=	=

The premises in which the information systems and their components are located will be protected against accidental or deliberate fires, applying at minimum the respective industrial regulations.

5.1.6 Protection against floods [mp.if.6].

dimensions	A		
level	low	intermediate	high
	n/a	applicable	=

INTERMEDIATE level

The premises in which the information systems and their components are located will be protected against accidental or deliberate incidents caused by water.

5.1.7 Recording of entries and exits of equipment [mp.if.7].

dimensions	all		
category	basic	intermediate	high
	applicable	=	=

A detailed record will be kept of all entries and exits of equipment, including the name of the person who has authorised the transfers.

5.1.8 Alternative facilities [mp.if.9].

dimensions	A		
level	low	intermediate	high
	n/a	n/a	applicable

HIGH level

The existence and availability of alternative facilities for working in the event of the usual ones not being available will be guaranteed. These alternative facilities will have the same security guarantees as the habitual ones.

5.2 Personnel management [mp.per].

5.2.1 Job characterisation [mp.per.1].

dimensions	all		
category	basic	intermediate	high
	n/a	applicable	=

INTERMEDIATE category

Each job will be characterised as follows:

a) A definition will be established of the responsibilities related to each job as regards security. That definition will be based on the risk analysis.

b) The requirements to be met by the people employed in the jobs will be defined, and in particular, in terms of confidentiality.

c) Such requirements will be considered in selecting the staff that is to carry out those jobs, including a check of their employment records, training and other references.

5.2.2 Duties and obligations [mp.per.2].

dimensions	all		
category	basic	intermediate	high
	applicable	=	=

1. Each person working in the system will be informed of the duties and responsibilities of their jobs as regard security.

a) The respective disciplinary measures will be specified.

b) Both the period during which the job is performed and the obligations on terminating the assignment or a transfer to another job will be covered.

c) The confidentiality obligation will be considered with respect to all information to which access is allowed, during the period the staff is assigned to the job and after its completion.

2. In the case of staff hired through third parties:

a) The duties and obligations of staff must be established.

b) The duties and obligations of each party must be established.

c) A procedure will be established for settling conflicts related to breach of obligations.

5.2.3 Awareness [mp.per.3].

dimensions	all		
category	basic	intermediate	high
	applicable	=	=

The necessary actions will be taken to regularly arouse awareness among the staff about its role and responsibility in ensuring that the system security is of the required standard.

In particular, regular reminders will be given about:

a) The security regulations in relation to the proper use of the systems.

b) The identification of suspicious incidents, activities or behaviours that must be reported for treatment by specialised staff.

c) The procedure for reporting security incidents, whether real or false alarms.

5.2.4 Training [mp.per.4].

dimensions	all		
category	basic	intermediate	high
	applicable	=	=

The staff will be regularly trained in all matters required for them to carry out their functions, in particular with regard to:

a) Systems configuration.

b) Detection of incidents and actions to be taken.

c) The control of information in any format. At least the following activities will be covered: storage, transfer, copies, distribution and destruction.

5.2.5 Alternative staff [mp.per.9].

dimensions	A		
level	low	intermediate	high
	n/a	n/a	applicable

HIGH level

The existence and availability of other people who can perform the functions in the event of unavailability of the habitual staff will be guaranteed. Such alternative staff will be subject to the same security guarantees as the habitual staff.

5.3 Protection of the equipment [mp.eq].

5.3.1 Tidy work stations [mp.eq.1].

dimensions	all		
category	basic	intermediate	high
	applicable	+	=

BASIC category

Works stations will be left tidy, with no material on the desk other than that required for the activity being carried out at each particular time

INTERMEDIATE category

This material will be kept under lock and key when not in use.

5.3.2 Blocking of work stations [mp.eq.2].

dimensions	A		
level	low	intermediate	high
	n/a	applicable	+

INTERMEDIATE level

The work stations will be blocked after a certain time of inactivity, and a new user authentication will be necessary to resume the activity in progress.

HIGH level

After a certain time that is longer that the above, all sessions initiated from that station will be cancelled.

5.3.3. Protection of laptops [mp.eq.3].

dimensions	All		
category	basic	intermediate	high
	applicable	=	+

BASIC category

Any equipment that may leave the organisation's premises and that cannot be protected by the relevant physical means, where there is a clear risk of loss or theft, must be adequately protected.

Without prejudice to any general measures that may affect them, the following will be adopted:

a) An inventory of laptops will be kept together with the name of the person responsible for them and a regular control will be implanted to ensure they are actually under their control.

b) A communication channel will be set up to inform the incident management service of losses or thefts.

c) When a laptop connects remotely through networks that are not under the strict control of the organization, the server operation scope will limit the information and services accessible to a bare minimum, requiring prior authorization from whoever is responsible for the affected information and services. This point is applicable to connections over the Internet and other unreliable networks.

d) All attempts will be made to ensure that the equipment contains no remote codes for access to the organisation. Remote access codes are taken as those that could enable access to other equipment in the organisation, or others of a similar nature.

HIGH category

a) They will be fitted with violation detector devices to allow it to be known whether the equipment has been manipulated and activate the preliminary incident management procedures.

b) All top level information stored in disks will be protected by ciphering.

5.3.4 Alternative means [mp.eq.9].

dimensions	A		
level	low	intermediate	high
	n/a	applicable	=

The existence and availability of alternative means for processing information will be guaranteed, in the event of a failure in the usual means. Such alternative means will be subject to the same guarantees of protection.

Likewise, a maximum time will be established for the alternative equipment to be put into operation.

5.4 Protection of communications [mp.com].

5.4.1 Safe perimeter [mp.com.1].

dimensions	all		
category	basic	intermediate	high
	applicable	=	+

BASIC category

A firewall system will be installed to separate the internal and external networks. All traffic will cross that firewall which will only allow previously authorised flows to cross it.

HIGH category

a) The firewalls system will consist of two or more pieces of equipment made by different manufacturers, following a waterfall model layout.
b) Redundant systems will be installed.

5.4.2. Confidentiality protection [mp.com.2].

dimensions	C		
level	low	intermediate	high
	n/a	applicable	+

INTERMEDIATE level

a) Virtual private networks will be used if the communication runs through networks outside the security domain.
b) Algorithms accredited by the National Cryptologic Centre will be used.

HIGH level

a) Preferably, hardware devices will be used in establishing and using the virtual private network.
b) Products certified in accordance with the provisions of [op.pl.5] must be used.

5.4.3 Protection of authenticity and integrity [mp.com.3].

dimensions	I-A		
level	low	intermediate	high
	applicable	+	++

LOW level

a) The authenticity of the other end of a communication channel will be ascertained before exchanging information (see [op.acc.5]).
b) Active attacks will be prevented, guaranteeing that they are at least detected, and the foreseen procedures will be activated for treating the incident. Active attacks are considered to be the following:

1. The alteration of the information in transit
2. The injection of spam
3. Kidnapping of the session by a third party

c) Any authentication mechanism from among those provided for in the applicable regulations will be accepted.

INTERMEDIATE level

a) Virtual private networks will be used if the communication runs through networks outside the security domain.

b) Algorithms accredited by the National Cryptologic Centre will be used.

c) Any authentication mechanism from among those provided for in the applicable regulations will be accepted. Where shared keys are used, intermediate quality requirements will be applied against divination attacks, dictionary or brute force.

HIGH level

a) Preferably hardware devices will be used in establishing and using the virtual private network.

b) Products certified in accordance with the provisions of [op.pl.5] must be used.

c) Any authentication mechanism from among those provided for in the applicable regulations will be accepted. Where shared keys are used, high quality requirements will be applied against divination attacks, dictionary or brute force.

5.4.4 Separation of networks [mp.com.4].

dimensions	all		
category	basic	intermediate	high
	n/a	n/a	applicable

Separation of networks restricts access to information and thus, the spread of security problems, which are restricted to the environment where they occur.

HIGH category

The network will be segmented so that:

a) The users accessing each segment are controlled.

b) The available information leaving each segment is controlled.

c) The networks can be segmented by physical or logical devices. The interconnection point will, in particular, be maintained and monitored (as in [mp.com.1]).

5.4.5 Alternative means [mp.com.9].

dimensions	A		
level	low	intermediate	high
	n/a	n/a	applicable

HIGH level

The existence and availability of alternative communication resources will be guaranteed, in the case that the habitual resources fail. These alternative communication resources:

a) Will be subject to and provide the same guarantees of protection as the habitual ones.

b) Guarantee a maximum time for putting them into operation.

5.5 Protection of information devices [mp.si].

5.5.1 Labelling [mp.si.1].

dimensions	C		
level	low	intermediate	high
	applicable	=	=

The information devices will be labelled so that the security level of top level information they may contain is indicated, without revealing their contents.

Users will be trained to understand the meaning of the labels, either through a simple inspection or using a repository that explains it.

5.5.2 Cryptography [mp.si.2].

dimensions	I-C		
level	low	intermediate	high
	n/a	applicable	+

This measure is applied in particular to all removable devices. Removable devices are considered to be CDs, DVDs, USB disks or any other similar ones.

INTERMEDIATE level

Cryptographic mechanisms will be applied to guarantee the confidentiality and integrity of the information they contain.

HIGH level

a) Algorithms accredited by the National Cryptologic Centre will be used.
b) Products certified in accordance with the provisions of [op.pl.5] must be used.

5.5.3. Custody [mp.si.3].

dimensions	all		
category	basic	intermediate	high
	applicable	=	=

Due diligence and control will be applied to information devices remaining under the control of the organisation, through the following actions:

a) Guaranteeing access control with physical means ([mp.if.1] and [mp.if.7]) or logical ([mp.si.2]) means, or both.
b) Guaranteeing that the manufacturer's maintenance requirements are met, particularly as regards temperature, humidity and other environmental aggressions.

5.5.4 Transport [mp.si.4].

dimensions	all		
category	basic	intermediate	high
	applicable	=	=

The systems manager will guarantee that the devices remain under control and that they satisfy the security requirements while they are moved from one place to another.
For this purpose:
a) An outgoing register will be established, identifying the transportation firm receiving the information device to be transported.
b) An access register will be established, identifying the transportation firm delivering the information device.
c) A routine procedure will be created for comparing exits with arrivals and raising the alarm if an incident is detected.
d) Cryptographic protection methods will be used ([mp.si.2]) in keeping with the information contained that is of the highest level.
e) Keys will be controlled in accordance with [op.exp.11].

5.5.5 Deleting and destroying [mp.si.5].

dimensions	C		
level	low	intermediate	high
	applicable	+	=

The measure for deleting and destroying information devices will be applied to all equipment that could store information, including electronic and non-electronic means.

LOW level

a) Storage media to be reused for other information or released to another organisation must have their content deleted in a secure manner.

INTERMEDIATE level

b) The information devices will be destroyed using safe procedures in the following cases:

1. If the nature of the information device makes safe deletion impossible.
2. When the procedure associated with the type of information contained requires so.

c) Products certified in accordance with the provisions of ([op. Pl.5]) must be used.

5.6 Protection of data-processing applications [mp.sw].

5.6.1 Development of applications [mp.sw.1].

dimensions	All		
category	basic	intermediate	high
	n/a	applicable	=

INTERMEDIATE category

a) The development of applications will be carried out using a different system and separate from production, with no tools or development data in the production area.

b) A recognised development method will be used that:

1. Takes into account the security aspects during the whole life cycle.
2. Applies a specific treatment to the data used for tests.
3. Allows for the inspection of the source code.
4. Includes secure programming standards.

c) The following elements will be an inseparable part of the system design:

1. The identification and authentication mechanisms.
2. The mechanisms for protecting the information processed.
3. The generation and processing of auditing tracks.

d) Tests performed prior to the implantation or modification of the information systems will not be done using real data, unless the respective security level can be assured.

5.6.2 Acceptance and putting into operation [mp.sw.2].

dimensions	all		
category	basic	intermediate	high
	applicable	+	++

BASIC category

Before being transferred to production, the correct functioning of the application will be checked.

a) A check will be made to verify that:

1. The acceptance criteria are met as regards security.
2. The security of other service components is not impaired.

b) The tests will be performed in an isolated environment (pre-production).

c) The acceptance tests will not be made using real data, unless the respective security level can be assured.

INTERMEDIATE category

The following inspections will be made before being put into operation:

a) Analysis of vulnerable aspects.
b) Penetration tests.

HIGH category

The following inspections will be made before being put into operation:

a) Analysis of coherence in the integration of processes.
b) The opportunity of performing a source code audit will be considered.

5.7 Protection of the information [mp.info].

5.7.1 Personal information [mp.info.1].

dimensions	all		
category	basic	intermediate	high
	applicable	=	=

If the system processes personal information, the provisions of Organic Law 15/1999 of 13 December 1999, and the regulations that implement this act will apply, without prejudice to also complying with the measures set forth in this royal decree.

The provisions of the preceding paragraph also apply if the provision of legal rank refers to personal information in the protection of information.

5.7.2 Classification of the information [mp.info.2].

dimensions	C		
level	low	intermediate	high
	applicable	+	=

LOW level

1. For the classification of information, the provisions regarding the nature of the information will apply.

2. The security policy will establish the person responsible for each type of information managed by the system.

3. The security policy will directly or indirectly include the criteria that determine the required security level in each organisation, within the framework established in Article 43 and the general criteria established in Annex I.

4. The person responsible for each type of information will adopt the criteria determined in the preceding section, to assign to each type of information the security level required, and will be responsible for documenting and formally approving them.

5. The person responsible for each type of information at any given time will have the exclusive authority to change the required security level, in accordance with the previous sections.

INTERMEDIATE level

The necessary procedures for describing in detail the way in which the information is to be labelled and processed, considering the security level it requires, describing how the following will be done:

a) Access control.
b) Storage.
c) Making of backup copies.
d) Labelling of information devices.
e) Digital transmission.
f) And any other activity related to that information.

5.7.3. Ciphering of information [mp.info.3].

dimensions	C		
level	low	intermediate	high
	n/a	n/a	applicable

HIGH level

The following provisions apply for ciphering of information:

a) Information with a high confidentiality level will be ciphered both during storage and during transmission. It will only be clear as long as use is being made of it.

b) The provisions set out in [mp.com.2] will apply for the use of cryptography in communications.

c) For the use of cryptography in information devices, the provisions set out in [mp.si.2] will apply.

5.7.4 Electronic signature [mp.info.4].

dimensions	IA		
level	low	intermediate	high
	applicable	+	++

The electronic signature shall be used as an instrument capable of allowing verification of the authenticity of the provenance and integrity of the information, providing the basis for avoiding repudiation.

The integrity and authenticity of the documents shall be guaranteed by electronic signatures with the following conditions, proportionate to the security levels required by the system.

Where other electronic signature mechanisms subject to law are used, the system should incorporate sufficient countervailing measures offering equivalent or superior guarantees as regards the prevention of repudiation, using the procedure mentioned in Article 27 (5).

LOW level

Any kind of electronic signature from among those provided for in current legislation may be used.

INTERMEDIATE level

a) Whenever advanced electronic signature systems based on certificates are used, they shall be qualified.

b) Algorithms and parameters accredited by the National Cryptologic Centre shall be used.

c) Verification and validation of the electronic signature shall be guaranteed for the time required by the administrative activity that it supports, without prejudice to the possibility of extending this period in accordance with the provisions of the applicable Electronic Signature and Certificate Policy. For that purpose:

d) All relevant verification and validation information shall be attached or referenced to the signature:

1. Certificates.
2. Verification and validation data.

e) The organisation collecting documents signed by the applicant shall verify and validate the signature received at the time of receipt, attaching or unambiguously referencing the information described in items 1 and 2 of paragraph (d).

f) Electronic signature of documents by the Administration shall unambiguously annex or refer to the information described in sections 1 and 2.

HIGH level

1. Qualified electronic signature must be used, including qualified certificates and qualified signature creation devices.
2. Products certified in accordance with the provisions of [op.pl.5] must be used.

5.7.5 Time stamping [mp.info.5].

dimensions	T		
level	low	intermediate	high
	n/a	n/a	applicable

HIGH level

The time stamps will prevent the possibility of subsequent denial:

1. Time stamps will be affixed to all information that could be used as electronic evidence in the future.
2. The pertinent data for the subsequent checking of the date will be treated with the same

security level as the information dated for the effects of availability, integrity and confidentiality.

3. The time stamps will be renewed regularly until the protected information is no longer required for the administrative process it supports.

4. Certified products (according to [op.pl.5]) or admitted external services (see [op.exp.10]) must be used.

5. ‘"Qualified electronic time stamps" according to European standards will be used.

5.7.6 Cleaning of documents [mp.info.6].

dimensions	C		
level	low	intermediate	high
	applicable	=	=

In the document cleaning process, all additional information included in hidden fields will be removed from the documents, in addition to meta-data, comments or previous reviews, unless that information is relevant for the person receiving the document.

This measure is particularly important if the document is widely distributed, as occurs when the public is offered information in a web server or other type of repository.

It will be borne in mind that breach of this measure may cause harm to:

a) Maintaining the confidentiality of information that should not have been revealed to the person receiving the document.

b) Maintaining the confidentiality of the sources or origins of the information that must not be known by the person receiving the document.

c) The good image of the organisation disseminating the document, by showing negligence in its operations.

5.7.7 Backup copies [mp.info.9].

dimensions	Av		
level	low	intermediate	high
	applicable	=	=

Backup copies must be made that make it possible to recover data that has been lost, whether accidentally or intentionally, up to a specified time in the past.

Those backup copies will have the same security level as the original data as regards integrity, confidentiality, authenticity and traceability. In particular, consideration must be given to the advisability of encrypting the backup copies, or the need for doing so, as applicable, in order to guarantee confidentiality.

The backup copies must include:

a) Information about the operations of the organisation.
b) Applications being used, including the operating systems.
c) Data on configuration, services, applications, equipment or other similar information.
d) Codes used to preserve the confidentiality of the information.

5.8 Protection of services [mp.s].

5.8.1 E-mail protection (e-mail) [mp.s.1].

dimensions	all		
category	basic	intermediate	high
	applicable	=	=

E-mails will be protected against threats to which they may be exposed, by acting as follows:

a) Information distributed by e-mail will be protected, including the text of the message and any attachments.

b) The information for routing messages and establishing connections will be protected.

c) The organisation will be protected against problems arising through the e-mail, specifically:

1. Unsolicited mail or “spam”.

2. Dangerous programs comprised of viruses, worms, trojans, spyware or others of a similar nature.

3. “Applet” type mobile codes.

d) Rules for the correct use of the e-mail by certain staff will be established. Such rules will include:

1. Limits on the use of private communications as supports.

2. Activities to arouse awareness and training on using the e-mail.

5.8.2 Protection of web services and applications [mp.s.2].

dimensions	All		
category	basic	intermediate	high
	applicable	=	+

Sub-systems used for publishing information will be protected against threats to which they may be exposed.

a) If the information has any kind of access control, it will be guaranteed that the information cannot be accessed by removing the authentication, in particular by taking measures regarding the following aspects:

1. Every attempt will be made to prevent the server from providing access to document using alternative routes other than the determined protocol.

2. URL manipulation attacks will be prevented.

3. Attacks intended to manipulate fragments of information stored on a website visitor’s hard disk through the visitor's browser (cookies), at the request of the website server, will be prevented.

4. Attacks launched to inject the code will be prevented.

b) Privilege escalation attempts will be prevented.

c) Cross-site scripting attacks will be prevented.

d) Attacks attempting to manipulate programs or devices that perform an action on behalf of others (known as “proxies”) will be prevented, and special high-speed storage systems (“caches”) will also be prevented.

LOW level

"Web site authentication certificates" shall be used in accordance with the relevant European standards.

HIGH level

"Qualified authentication certificates for the website" shall be used in accordance with European standards in this field.

5.8.3 Protection against denial of service [mp.s.8].

dimensions	A		
level	low	intermediate	high
	n.a.	applicable	+

INTERMEDIATE level

Preventive and reactive measures will be established against denial of service (DOS) attacks. For this purpose:

a) The system will be fitted with sufficient capacity to amply deal with the foreseen load.

b) Technologies will be deployed to prevent all known attacks.

HIGH level

a) A system will be established for detecting service denial attacks.

b) Procedures will be established for taking actions in the face of attacks, including communication with the communications supplier.

c) The launch of attacks from the organisation’s premises that could harm others will be prevented.

5.8.4 Alternative means [mp.s.9].

dimensions	A		
level	low	intermediate	high
	n/a	n/a	applicable

HIGH level

The existence and availability of alternative means will be guaranteed, in order to provide services in the event of the usual means failing. These alternative means will be subject to the same level of protection as the usual ones.

6. Implementation and completion of the security measures

The security measures will be implemented and completed in accordance with final provision two.

7. Interpretation

This annex must be interpreted giving its words their literal meaning, in relation to the context and the historical and legislative background, which include the provisions of the CCN-STIC technical instructions on implementation and different application scenarios, such as websites, electronic certificate validation services, electronic date stamping services and validation of dated documents, taking account of the spirit and purpose of such elements.

ANNEX III Security Audit

1. Purpose of the audit.

1.1 The security of an organisation's information systems will be audited as follows:

a) The security policy will define the roles and functions of those responsible for the information, services, assets and security of the information system.

b) Procedures will be in place for solving conflicts between those persons.

c) Persons will be designated for those roles in the light of the “separation of functions” principle.

d) A risk analysis will have been performed, with an annual review and approval procedure.

e) The protection recommendations described in Annex II on Security Measures will have been complied with, depending on the conditions of application in each particular case.

f) An information security management system will exist, which will be documented and have a regular management approval process in place.

1.2. The audit will be based on the existence of evidence that allows compliance with the above points to be objectively supported:

a) Documentation of procedures.
b) Recording of incidents.
c) Examination of affected staff: knowledge and praxis regarding the measures affecting them.
d) Certified products. Use of products that satisfy the requirements of article 18 "Purchase of products and contracting security services" shall be considered sufficient evidence.

2. Auditing levels

The auditing levels used for the information systems will be the following:

2.1. Auditing of BASIC category systems.

a) Information systems belonging to the BASIC category or a lower one do not require an audit. A self-evaluation procedure performed by the staff in charge of the information system, or any person delegated by that staff will be appropriate.

The result of the self-evaluation will be documented, indicating whether each security measure has been implanted, subject to regular review and evidence to support the previous evaluation.

b) The self-evaluation reports will be analysed by the competent security head, who will submit his/her conclusions to the system head for the opportune corrective measures to be taken.

2.2. Auditing systems belonging to the INTERMEDIATE or HIGH category.

a) The audit report will provide a decision regarding the degree of compliance with this royal decree, identifying faults and suggesting any potential corrective measures or complementary measures deemed necessary, and any recommendations that are considered appropriate. It will also include the methodology criteria used to perform the audit, the scope and objective of the audit and the information, facts and observations on which the conclusions are made.

b) The audit reports will be analysed by the competent security head who will submit his/her conclusions to the system head for the opportune corrective measures to be taken.

3. Interpretation.

This annex must be interpreted giving its words their literal meaning, in relation to the context and the historical and legislative background, which include the provisions of the relevant CCN-STIC technical instruction, taking account of the spirit and purpose of those words.

ANNEX IV

Glossary

Asset. A component or functionality of an information system that could be deliberately or accidentally attacked, with specific consequences for the organisation. It includes: information, data, services, applications (software), equipment (hardware), communications, administrative resources, physical resources and human resources.

Risk analysis. The systematic use of the available information for identifying hazards and estimating risks.

Security auditing. An independent review and examination of the system records and activities to check the suitability of the system controls, ensure that the security policy is enforced and the operating procedures established, detect security breaches and recommend the appropriate modifications in the controls, policy and procedures.

Authenticity: A property or characteristic that consists of an entity being what it says it is or guaranteeing a source from which data come.

System category. A level, within the Basic-Intermediate-High scale, used to describe a system for the purpose of selecting the best security measures for that system. The system category includes a holistic vision of the set of activities as a harmonious whole, aimed at providing a series of services.

Confidentiality. A property or characteristic that consists of information not being made available or disclosed to non-authorised third parties, entities or processes.

Availability: a property or characteristic of assets, consisting of authorised entities or processing having access to them if so required.

Electronic signature A series of data in electronic format, affixed next to others or associated with them, that can be used as a means for identifying the signer.

Incident management. An action plan for dealing with incidents that arise. In addition to solving them, it must include measures that allow the quality of the protection system to be known and detect trends before they are converted into important problems.

Risk management: activities coordinated to direct and control an organisation with respect for risks.

Security incident: an unexpected or undesirable event with consequences that are to the detriment of the information system security.

Integrity: a property or characteristic consisting of the information asset not having been altered in a non-authorised way.

Security measures: a series of provisions aimed at protecting potential risks to the information system, for the purpose of ensuring its security objectives. It may be in the form of prevention measures, dissuasion, protection and reaction, or recovery.

Electronic signature policy: a set of regulations on security, organisation, technical and legal affairs to determine how electronic signatures are generated, verified and controlled, including the characteristics required of the signature certificates.

Security policy: a set of directives set down in a written document, that govern the way in which an organisation controls and protects the information and services it considers are critical.

Basic security principles: Fundamentals that must govern all actions taken to guarantee information and services.

Process: an organised set of activities that are carried out to produce a product or services; it has a delimited beginning and end, involves resources and gives rise to a result.

Security process: a method used to achieve the organisation's security objectives. The process is designed to identify, measure, manage and keep under control all risks that could affect the system regarding security.

Minimum security requirements. A series of requirements necessary to guarantee information and services.

Risk. An estimation of the degree to which a threat may materialise to one or more assets, causing damage or harm to the organisation.

Security of networks and information: the capacity of the networks or information systems to resist accidents, wilful or illicit actions that compromise the availability, authenticity, integrity and confidentiality of the data stored or transmitted and the services that those networks and systems provide or make accessible, with a certain level of confidence.

Accredited services: services provided by a system with authorisation granted by a responsible authority, to deal with a certain type of information, under precise conditions regarding the security dimensions, based on its operating concept.

Information security management system (ISMS) Management system that, based on a risk analysis, is established to create, implement, run, supervise, review, maintain and improve information security. The management system includes the organisational structure, policies, planning, responsibilities, practices, procedures, processes and resources.

Information system. An organised set of resources created to ensure that information can be collected, stored, processed or treated, maintained, used, shared, distributed, made available, presented or transmitted.

Traceability: a property or characteristic consisting of the actions of an entity being the exclusive responsibility of that entity.

Vulnerability: a weakness that can be taken advantage of by a threat.

Acronyms

CCN: National Cryptologic Centre (Centro Criptológico Nacional).

CERT: Computer Emergency Response Team.

STIC: Security of Information and Communication Technologies.

ANNEX V

Specific administrative clause model

Specific administrative clause.– In compliance with the provisions of Article 115.4 of Legislative Royal Decree 3/2011, of 14 November, approving the consolidated text of the Public Sector Contracts Act, and article 18 of Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the field of Electronic Administration, the tenderer shall include precise, documented and accredited references. Its components comply with what is indicated in measure op. pl. 5 on certified components, set out in section 4.1.5 of Annex II to the aforementioned Royal Decree 3/2010, of 8 January.

When these are used to process personal data, the bidder shall also include the provisions of the single additional provision of Royal Decree 1720/2007, of 21 December, which approves the regulations implementing Organic Law 15/1999, of 13 December, on personal data protection.