Spain Country Report

enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports:

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: **Dan Cimpean, Johan Meire and Joris Lambrechts**.

Legal notice

Table of Contents

Spain

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level:*
    - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
    - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
    - *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
    - *Security incident management*
    - *Emerging NIS risks*
    - *Resilience aspects*
    - *Privacy and trust*
    - *NIS awareness at the country level*
    - *Country-specific activities for identifying and promoting economically efficient approaches to information security*
    - *Interdependencies, interconnection and improving critical information infrastructure protection*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year.

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

eGovernment strategy

The Spanish eGovernment strategy[1] aims to improve the quality of services provided by Central Government while bringing the Public Administration closer to citizens and businesses. Focus is set on the use of new technologies reducing bureaucracy, simplifying procedures and eliminating unjustified delays.

The **current Spanish eGovernment strategy** results from the following two policy documents:

- the **'**Avanza' Plan[2] for the development of the Information Society, launched in 2005. in January 2009, the plan entered its second phase, '**Avanza2**', which will run from 2009 to 2012;
- the **Action Plan for the Implementation of the so-called 'Law on eGovernment'**.

The 'Avanza' Plan for the development of the Information Society forms **part of the broader programme '**Ingenio 2010**'**[3], aimed at giving new impetus to R&D investment in Spain within the framework of the National Reforms Programme designed by the Government to **comply with the EU's** i2010 initiative[4]**.**

Avanza

'Avanza' is placed under the responsibility of the Ministry of Industry, Tourism and Trade, as the competent authority for Information Society Development. However, certain of its areas of action such as the '**Public eServices**' area imply a **close cooperation** with, on the one hand, the Ministry of the Territorial Policy and Public Administration (the Ministry of Public Administrations previously) responsible for the development of eGovernment, and, on the other hand, the Autonomous Communities (regions) and Local Governments that are responsible for eGovernment in their respective areas of competence.

The implementation of the Plan is indeed based on a cooperative model under which **each of the 17 Autonomous Communities has a separate action plan and budgetary contribution**. This is articulated around bilateral agreements signed between the Government and each autonomous region.

The 'Avanza' Plan opts for a user-centric eGovernment which furthermore overcomes the most serious challenges facing public eServices, namely, their uneven development and quality, as well as their lack of integration when these services are offered by distinct administrations or departments.

[1] *See: http://www.epractice.eu/en/document/288369*
[2] *See: http://www.planavanza.es/*
[3] *See: http://www.ingenio2010.es/*
[4] *See: http://www.epractice.eu/node/281014*

Some of the features are common to the first phase of the plan (initially established for the period 2006-2010) and to its new phase, 'Avanza2', launched in January 2009 and set to run until 2012. The 'Avanza' Plan remains **an initiative in constant evolution**.

First phase of the 'Avanza' Plan (2006-2008)

The first phase of the so-called Plan for the 'Development of the Information Society and for Convergence with Europe, and among Autonomous Communities and Cities - 2006-2010' ('Avanza') was approved by the Spanish Council of Ministers on 4 November 2005.

Reaching a **fully developed eGovernment** was among the main pillars of the 'Avanza' Plan. This objective also directly impacted on the other objectives of the Plan, and vice versa. The combination of objectives pursued by the 'Avanza' Plan could be synthesised in one: a joint effort from the private sector, the civil society and the various administrations is required.

As a result, the first version of the 'Avanza' Plan was oriented towards the adequate use of ICTs, so as to contribute to the rise of an economic growth model based on the increase of competitiveness and productivity, social and regional equality and the **increase of citizen welfare and quality of life**.

The first version of the 'Avanza' Plan consisted of **five main action fields**:

- **Households and Citizen Inclusion**: measures shall be developed to ensure a wider use of ICTs among households while increasing citizens' opportunities to participate in public life ('Avanza Citizenship');
- **Competitiveness and Innovation**: measures shall be taken to encourage the development of the ICT sector in Spain and to adopt technologically advanced solutions in favour of Spanish SMEs;
- **Education within the Digital Era**: incorporating ICTs in the education and training process in general, involving all agents taking part in this project;
- **Public eServices**: measures shall be taken to enable the delivery of new, user-friendly and better public services, as well as the improvement of citizens' quality of life and a greater efficiency for Spanish businesses;
- **The New Digital Context**: deploying a broadband infrastructure, so as to connect the entire country, generate citizens and businesses' confidence in the use of new technologies, provide advanced security mechanisms and promote the creation of new digital content.

The actions implemented during the first phase of the 'Avanza' Plan in the field of **Public eServices** targeted the following **objectives**:

- **Guarantee the right for citizens and businesses to be electronically connected with Public Administrations**: all public eServices should be available on the Internet by 2010. Among these services, at least 80 % should be fully transactional i.e. the entire case handling will occur online (payment included);
- Set up of mechanisms aimed at **adjusting the offer of eServices to the existing demand** by creating a clear catalogue of eServices explicitly indicating their respective development

schedule and functionalities, as well as the authorities responsible for their launch. Additionally, necessary actions will be taken in order to have multiplied by two the use of these services by the end of 2010;

- **Guarantee the existence of appropriate channels** in order to allow all citizens and businesses to access public services;
- **Modernise Spanish Public Administrations**, for them to adapt to the new paradigm of user-centric delivery of public services, in terms of better quality and performance, costs reduction, user satisfaction, interdepartmental integration and administrative simplification. To this end, several actions were promoted within the administration, including: the intensive use of ICTs, the necessary organisational and procedural changes, as well as the development of new abilities among public agents;
- **Create cooperation structures between the various levels of Government** i.e. the Central Government, the Autonomous Communities (regions) and the local entities. The aim is to ensure the development of joint solutions, as well as the integration of solutions developed by each one of them, in such a way that citizens may use new services independently of the administration providing them.

In order to implement the 'Avanza' Plan, **two specific plans of measures** covering respectively the year 2006 and the period 2007-2010 were adopted. The first phase of the Plan mobilised some € 9 billion over the 2005-2008 period.

Second phase of the 'Avanza' Plan – 'Avanza2' (2009-2012)

The so-called 'Avanza2 Plan' (2009-2012) aims to consolidate the milestones achieved during the first phase of the Plan while contributing **to foster the demand for ICT and to fortify the ICT industry**.

'Avanza2' is structured around **5 action lines**:

- **Development of the ICT sector:** to support companies, in particular SMEs, in developing new ICT products, processes, applications, contents and services, and participating in the establishment of the Future Internet and of digital content. Innovation programmes related to the Information Society and aimed at improving the competitiveness of the Spanish ICT sector will receive funding. Budget for 2009: €663 million;
- **ICT training:** to massively include citizens and companies in the Information Society, in particular SMEs and their employees, persons with disabilities and the elderly. Budget for 2009: €548 million;
- **Public eServices:** to improve the quality of public services delivered by the 'networked Public Administration', special emphasis being placed on the support to Local Government and on the development of the functionalities of the national eID card (DNIe). Likewise, this action line will be dedicated to stimulating the creation of new health and education platforms and content based on the achievements of the first phase of the Plan 'Avanza'. Budget for 2009: €186 million;

- **Infrastructure and Trust:** among other aims, this action line will further boost the development and establishment of the Information Society at local level in order to improve the delivery of Public eServices to both citizens and businesses. Budget for 2009: €89 million;
- **Security and Accessibility:** the objective of this action line is twofold: to foster citizens' and businesses' trust in ICT and to improve the accessibility of eServices. Budget for 2009: €11 million.

In July 2009, the Spanish Ministry of Industry, Tourism and Trade launched a public consultation on the first draft of a revised 'Avanza2' Plan for the period 2010-2012. The consultation closed on 11 September 2009.

The draft 'Avanza2' Plan 2010-2012 comprises new strategic lines. The consultation aimed to collect the stakeholders' opinion on the suitability of the proposed objectives and on the actions foreseen in order to reach them. The questionnaire was structured around the five action fields proposed for the new 'Avanza2', namely: Infrastructure; Trust and Security; Technological Empowerment; Digital Contents and Services; Competitiveness of the ICT Sector.

Those participating in the consultation were furthermore invited to suggest other domains (e.g. legal framework) where additional action could be taken with a view to achieve the objectives of the Plan 'Avanza2'.

On 21st November 2009, the Spanish Senate unanimously approved a report containing proposals, which have been all incorporated to the '**Avanza2 plan - 2011-2015 Strategy**'[5].

The strategy will focus on achieving the following 10 objectives:

- Promoting innovative ICT processes in the Public Administration;
- Spreading ICT in healthcare and for the welfare;
- Modernizing the education and training model through the use of ICT;
- Spreading telecommunication networks and increasing their capacity;
- Spreading trustworthy ICT among citizens and enterprises;
- Increasing the advanced use of ICT solutions among citizens;
- Spreading the use of ICT business solutions in enterprises;
- Developing technological skills in the ICT sector;
- Strengthening the digital content sector and intellectual property rights in the current technological context and within the Spanish and European legal framework;
- Developing green ICT.

'Avanza Local', the "municipal arm" of the 'Avanza' Plan, is intended to promote eGovernment at local level. Areas covered include the diffusion and implantation of the dedicated **'Avanza Local Solutions Platform'**[6], the development and implantation of technical solutions of particular use to

[5] *See: http://www.planavanza.es/InformacionGeneral/Estrategia2011/Paginas/Estrategia2011_2015.aspx*
[6] *See: http://www.planavanza.es/avanzalocal/Soluciones/Paginas/Plataforma.aspx*

Local Government, and the release of studies leading to a good practice catalogue for the content and use of municipal applications.

The **tools** included in the 'Avanza Local Solutions Platform' include:

- **'SIGEM'**[7], for managing the back office of the municipalities;
- **'LOCALWEB'**[8], for building and managing portals;
- **'LocalGIS'**[9] , a powerful Geo-information system;
- **'Avanza Local Padrón'**[10], an integrated system to manage census and enrolment list for polls;
- **'e-fácil'**[11] application and eInvoicing with the CIRCE[12] local module.

Action plan for the implementation of the 'Law on eGovernment'

The Law on Citizens' Electronic Access to Public Services13 (the so-called 'Law on eGovernment') entered into force in June 2007. It officially recognises the right of citizens to communicate electronically with Public Administrations, i.e. to conduct their administrative business by electronic means, 24 hours a day and 365 days a year.

Relevant State bodies are obliged to facilitate this via diverse channels such as the Internet, television or any related technology. This new right is to be respected by all Public Administrations from 31 December 2009 onwards. Among other detailed provisions, the law also generalises the use of eSignatures and allows for the extension of electronic processes within the State Administration.

The Ministry of Public Administrations, in collaboration with the Ministry of Economy and Finance and the Ministry of Industry, Tourism and Trade, submitted a plan to the Spanish Council of Ministers in order to **determine the financial, technical and human resources** which are needed for the Central Government to meet the implementation deadline – 31 December 2009 **–** of the Law on eGovernment.

The resulting action plan was approved by the Council of Ministers in December 2007. Together with the strategic framework to which it belongs, the action plan is intended to enable the implementation of the provisions of the Law by all Central Government bodies, in a concerted and efficient manner.

To this end, the action plan considers the instruments described in the Law and puts them in an action and strategy framework to be developed in the next years. It thus defines the set of specific actions necessary to ensure the effective and efficient application of the Law, including the actions to be undertaken by each ministry, as well as those developed collectively for creating **common**

[7] *See: http://www.planavanza.es/avanzalocal/Soluciones/Paginas/Sigem.aspx*
[8] *See: http://www.planavanza.es/avanzalocal/Soluciones/Paginas/Localweb.aspx*
[9] *See: http://www.planavanza.es/AVANZALOCAL/SOLUCIONES/Paginas/LocalGis.aspx*
[10] *See: http://www.planavanza.es/avanzalocal/Soluciones/Paginas/Padron.aspx*
[11] *See: http://www.planavanza.es/avanzalocal/Soluciones/Paginas/e_facil.aspx*
[12] *See: http://www.epractice.eu/en/cases/circe (an eGovernment service to facilitate the creation of companies)*
[13] *See: http://www.060.es/te_ayudamos_a/legislacion/disposiciones/38437_LEG-ides-idweb.html*

infrastructures and services that will enable the development of new services and enhance interoperability in the existing ones.

The plan aimed to put in compliance with the Law 2,500 current administrative procedures by 31 December 2009, with a **timetable of gradual adjustment** that pays maximum attention to the procedures which are mostly used by citizens and companies. It breaks down into **four action lines** (and foresees 21 measures in total), as follows:

- **Orientating public services towards citizens** in order to improve their access to public services. Among other measures to be taken under this action line are: the consolidation of the public services' '060 Network'; the implementation of unique windows allowing for the full completion of administrative procedures within specific sectors of activity; the electronic access to public services for all citizens, thus paying special attention to the fight against the digital divide as well as to eAccessibility and citizens' freedom to choose which technological solution to use with the Administration; the increase of citizen participation in public life; the improvement of public services design, so as to better respond to the needs of service users;
- **Adjusting administrative procedures to the requirements of the new law**. In this light, all administrative procedures and public services shall be made electronically accessible from 2010 onwards. The plan thus calls for keeping up-to-date the list of eServices available at the eGovernment portal '060.es'[14] and for establishing a calendar of online availability onto the portal of the missing public services. In addition, the plan foresees the creation of a series of technical services aimed at supporting the efforts of public bodies in adapting the services they provide for citizens and businesses;
- **Creating, strengthening and sharing common infrastructure and services** that will facilitate the development of the necessary IT solutions while guaranteeing interoperability and reducing implementation time and costs. Among other measures approved under this action line are those related to: rendering operational the common communications infrastructure SARA; providing a validation platform for digital certificates and electronic signatures; ensuring the eIdentification and eAuthentication of public bodies and employees; creating an electronic archive or a system inter-connecting registers;
- **Launching horizontal actions, so as to ensure that the services implemented in the coming years do satisfy citizens' needs.** In order to attain this goal, the plan foresees the creation of a National Interoperability Scheme that will contain security, conservation and standardisation criteria, as well as recommendations for public information, formats and applications; the adoption of a plan for training public employees regarding the 'Law on eGovernment', the use of ICT and eGovernment in general; and the creation of a Centre of Technological Transfer.

[14] *See: http://www.060.es/*

The major result of the Action Plan has been a critical improvement in the availability of the public electronic services. Over 90% of procedures and administrative services provided by the national government (which is more than 98.5% of the cases handled) have an electronic version.

In *March* 2009, a **report on the progress of the action plan** for the implementation of the 'Law on eGovernment' revealed the following figures:

- The '060 Network' includes all Autonomous Communities and over 1,600 municipalities while offering 1 225 public eServices;
- The related phone number '060' receives an average of 180,000 calls per month;
- The SARA network interconnects the Central Government, all Autonomous Communities and over 1 650 municipalities;
- The multiPKI validation platform @firma15 validates 900,000 certificates on a monthly basis;
- 500,000 validations are carried out by the Identity and Residence Data Verification System.

According to the report 'Smarter, Faster, Better eGovernment - 8th Benchmark Measurement'16 (November 2009), prepared for the European Commission, the **top five strategic eGovernment priorities in Spain in 2009** were:

- To provide all national public administration services online by the end of 2009;
- To increase the use of eGovernment services and promote the adoption of the national eID card (DNIe) both in public and private eServices;
- To fulfil the deadline established by the Services Directive;
- To extend the functionalities of the national eProcurement platform and to promote its use among Local and Regional Government;
- To create new horizontal tools for eGovernment and to improve the existing ones.

The 060 Network, Sara Network and other shared services

The **060 Network (Red 060)** is a comprehensive and multi-channel platform to interact with each public administration in Spain. It consists of three different channels of contact.
The Network's local offices consist of 101 contact points for entrepreneurs – 31 **business information offices** and 80 **camera-less antennae** situated in city councils. In these offices, entrepreneurs can access eServices for businesses provided by all levels of government, as well as information, guidance and personalised advice. For instance, they can access services related to the creation, development or cessation of companies.

www.060.es is the first portal to give unified electronic access to Spain's public services, regardless of which administration runs them. The portal was renewed and updated in 2007, allowing personalized applications and formats for individual users. "060.es" now also offers interactive functions, including one that permits users to evaluate and comment on the services provided. Surveys and FAQs have also been added. To date, all Autonomous Communities (autonomous

[15] *See: http://www.epractice.eu/node/277227*
[16] *See: http://www.epractice.eu/en/library/299159*

government level of the different regions) and over 1,600 municipalities participate in the "060 Network", offering 1225 public eServices. Of these, 729 were provided by the various departments of the national administration, 340 by Autonomous Communities and 156 by local authorities. The user-focused design of the portal was scored with the maximum possible value in the 2009 assessment of e-Government services done by the European Commission. The related phone number "060" is intended to replace over 600 phone numbers available for citizens to access information of the national administration. It receives an average of 180,000 calls each month.

The **SARA network (Red SARA)**, interconnects the networks of the three levels of government in Spain in order to enhance collaboration and inter-operability among the respective information systems.

One of the services provided by the network is access to S-Testa, the pan-European network between the EU institutions and the Public Administrations of the EU Member States. The overall objective is to **save time, costs and facilitate the access and re-use of information**.

The network operates since 2006 and now allows access to diverse shared services as checking and notifying identity, residence and other personal data. It also provides access to '@firma' (the multiPKI Validation Platform for eID and eSignature services; payments; etc).

A common service for **Electronic notification and communication systems** was put in place in 2004. This system allows legally binding notifications to be received by citizens via the Internet. The number of citizens subscribed to the service has increased from 8,414 in 2004 to 74,629 in 2009, and the number of e-notifications issued annually has climbed from 36,051 in 2004 to 1,425,269 in 2010. It must be said that other government units and regional governments have put in place their own Electronic notification and communication systems where the demand of their services required.

Aiming to overcome a strictly bilateral model for the exchange of information between government units, a data-broker called **the Service Intermediation Platform** has been put in place in order to exchange the more common certificates in administrative procedures in a more efficient way.

Its first aim was to remove the paper photocopies of the national identity and residence documents, requested to the citizens in the majority of the administrative procedures.
This procedure has been replaced by a paperless electronic request to the Service Intermediation Platform, with the same legal value as the traditional identity documents. The system will include the verification of other data and citizens and enterprises' certificates (tax, labour, universities diplomas, real estate register - 'catastro', justice, etc).

Since the Service Intermediation Platform became operational on 1 January 2007, its has been increasing gradually. In 2009, more than 19 million consultations of citizens' identities and consultations of residence have been made (saving the same amount of paper certificates delivering).

Institutional setting of the eGovernment strategy

The Ministry of the Territorial Policy and Public Administration is responsible for e-Government policies and it operates the shared services. Through the Directorate General for the Promotion of e-Government in the State Secretariat of the Civil Service, the Ministry aims fostering the full integration of information technology and communications to the provision of public services and the promotion and development of e-Government.

There is a very wide range of institutions and bodies, which has been put into place over the past five years. The Royal Decree 589/2005 established the inter-ministerial Higher Council for e-Government (Consejo Superior de Administracion Electronica - CSAE), now with to the Ministry of the Territorial Policy and Public Administrations. Its mandate is to prepare, develop and implement the ICT and e-Government policies of the government.

The Council comprises senior officials from all ministries and is supported by a permanent commission, ministerial e-Government commissions, as well as technical committees and working groups. One of the functions of the CSAE is being an e-Government Observatory and follows-up the developments of e-Government in the National Government.

In addition, section 4 of Law 11/2007 is dedicated to co-operation between the national government and the other government tiers, and established for this purpose t**he Sectoral Committee for e-Government**. This close co-ordination over e-Government has already paved the way for administrative simplification and burden reduction in the implementation of the Services Directive.

In April 2006, a **mixed Advisory Council on e-Government** (Consejo Asesor de Administración Electrónica) was created to assist in the development of an integrated strategy for e-Government. Meeting at least twice a year, the Council includes representatives of business, academics and experts on the technological sector.

In parallel to the adoption of the Action Plan implementing Law 11/2007, two new bodies were created at the end of 2007:

In the framework of the e-Government and administrative burdens reduction strategies of the government, moreover, an **Inter-ministerial Commission for Administrative Simplification** operates within the Ministry of the Territorial Policy and Public Administrations with a view to analyse and table proposals for measures aimed at facilitating the relationship between citizens and the Central Government.

The **Ministry of Industry, Tourism and Trade** is responsible for conducting and implementing the Plan Avanza, notably through the **State Secretariat of Telecommunications and the Information Society** (SETSI).

The State Secretariat is in particular in charge of:

- Access to the Information Society;
- Business and the Information Society;
- Services in/for the Information Society;
- Multimedia.

"Red.es" is a state-owned company which is part of the SETSI. Its role is to **encourage, support and monitor** the **use of information and communication technologies in Spain**, notably in the public sector. Among other things, Red.es participates in the implementation of Plan Avanza by maintaining a **National Observatory of Telecommunications and the Information Society** and providing consulting and support services to central and local administrations.

On a technical ground, ASTIC is the **professional association of IT experts and managers of the General State Administration**. It provides support and information services to its members for the development and implementation of their e-Government projects.

The Spanish **Ministry of the Interior** is in charge of the implementation of the electronic ID card project.

Co-operation between the Central Government and the Autonomous Communities (regions) is also covered. The **Sectoral Committee of e-Government** has been active since 2004. Since Law 11/2007 came into force, this Committee has served as the **technical body of co-operation** between the Central Government and the Autonomous Communities (regions) and local governments in the field of e-Government.

In addition, the Sectoral Committee monitors the **implementation of the principles and goals stated in Law 11/2007**. In particular, the Committee is responsible for ensuring the interoperability of the applications and systems in use within public administrations, and for preparing joint action plans in order to improve the e-Government development.

Finally, with a view to ensure that the e-Government rights of citizens are respected, Law 11/2007 provides for the appointment of a form of e-Government ombudsman, the **Defender of the e-Government users** (Defensor del usuario de la administración electrónica) in charge of monitoring its application.

The Defender will publish an annual report gathering the complaints and suggestions received, together with proposals for actions and measures to be taken in order to ensure an adequate protection of users' rights.

The Defender is to be chosen among recognised experts in the field of e-Government and reports to the Ministry of the Territorial Policy and Public Administrations, and is to execute his/her functions with impartiality and independently.

e-Government Strategy 2011-15

The recently approved "Plan Avanza2" has an advanced role in the future e-Government strategy of the national government. Reaping the benefits of the services already deployed through the promotion of its usage will be the major objective. The forthcoming strategy will be closely aligned with the priorities set in the Malmö Declaration.

Among the targets set in "Plan Avanza2" related with e-Government, three of them are linked with achieving a more sustainable Public Administration:

- Elimination of the usage of paper in Public Administrations by 2015;
- 3% savings by 2013 and 5% savings by 2015 in the ICT budget of the National Government by means of resources sharing;
- 20% savings by 2015 in the Government Energy Consumption through the usage of ICTs;
- The development of an "Open Government Action Plan" is one of the measures included in "Plan Avanza2". The establishment of an specific Open Government portal and the promotion of open data initiatives and advance in the re-use of public sector information are also mentioned in the new strategy.

Avanza2 is a first step in his eGovernment strategy which will be fully developed with the development at a national level of the lines of action of the European eGovernment Action Plan 2011-2015.

eIdentity

A cornerstone in the Spanish e-Government Strategy has been the deployment of the **e-DNI** (Electronic Identification National Document), the national eID, which must be accepted in all the e-services.

The new Electronic 'DNI' ('DNIe' or 'DNI electrónico') is a smart card that allows its holder to:

- Accredit electronically and unambiguously his/her identity;
- Digitally sign electronic documents, giving them a legal value equivalent to giving them a handwritten signature.

The e-DNI provides strong authentication based in digital certificates which are stored in a smart card. Over 20 million of Spaniards have obtained it since 2006. Beside this national eID, there are more than 2 million digital certificates legally binding provided by other public and private entities.

Any person can use his/her DNIe perform multiple steps securely online with the government, with public and private companies and with other citizens.

The digital certificates and e-signatures validation system called "**@firma**" is the core of the eID management system. According to the eDNI Certificate Practice Statement, @firma is the universal validation system for the digital certificates stored in this smart card for the public sector. **@firma** also provides the validation service for all the digital certificates issued by other providers according to the eSignature Act (Royal Decree 59/2003).

Managed by the Ministry of the Territorial Policy and Public Administrations, the service provided by **@firma** is free of charge to all national, regional and local government units. According to the internal data provided by **@firma**, its usage has been increased from 880,827 validations in 2006 to 14,458,488 validations in 2009. For more information we refer the reader to the sources: http://www.dnielectronico.es/ and http://www.usatudni.es/dnie/

Spain is also an active member of the European project STORK (Secure idenTity acrOss borders linKed) that is aimed at enabling businesses, citizens and government employees to use their national electronic identities in any Member State.

The consortium members include national authorities, non profit organisations, private companies and academic partners from: Austria, Belgium, Estonia, France, Germany, Italy, Luxembourg, Netherlands, Portugal, Slovenia, Spain, Sweden, United Kingdom and Iceland.

The regulatory framework

The following Spanish national regulations have relevance and applicability in the domain of network and information security:

e-Governance Legislation

Law on Citizens' Electronic Access to Public Services

The Law on Citizens' Electronic Access to Public Services[17] (the so-called 'Law on eAdministration') was adopted on 22nd of June 2007 and will become effective from 1st January 2010.

This law officially recognises the **right of citizens to communicate electronically with Public Administrations** i.e. to conduct their administrative business by electronic means 24 hours a day and 365 days a year. Relevant State bodies are obliged to facilitate this via diverse channels such as the Internet, television or other technology. This new right is to be respected by all Public Administrations from 31 December 2009 onwards. Furthermore, this law stipulates that any business conducted by electronic means will be just as valid as if it were conducted by traditional means.

The aim of the law is to enhance efficiency by **doing away with the need to present paper documents** to authorities, to promote "closeness to the citizen and administrative transparency" and, more generally, to contribute to the development of eGovernment. It introduces a principle of technological neutrality which gives both citizens and administrations the right to choose between technological alternatives. However, as regards communications between administrative authorities, the law stipulates that the electronic means of communication shall be preferred to traditional ones.

The law also establishes the basic principles for the use of Information technology between citizens and the Administration, but also among Public Administrations (central, regional and local). In this respect, a key clause requires public bodies to "use information technologies" while "ensuring the availability, accessibility, integrity, authenticity, confidentiality and conservation of the data, information and services that they manage in the exercise of their competences".

Royal Decree 1671/2009

The Council of Ministers approved on 6 November 2009 this Royal Decree whose purpose is to partially implement the Law on Citizens' Electronic Access to Public Services. In this light, the Decree establishes a flexible framework for the implementation of eGovernment. It regulates the following aspects in the Central Government:

- The **'electronic offices'** - electronic access points to the Central Government services - the Decree defines a common framework for their creation, features and application scope, thus reinforcing their reliability while easing their localisation by the citizens;

[17] *Source: http://www.epractice.eu/files/eGovernment%20in%20ES%20-%20December%202009%20-%2013.0%20-%20PDF.pdf*

- The **'General Access Point'**, that is, the single access gate - to the public services of the Central Government and other public bodies – through which citizens will find the information they need in order to take part in electronic proceedings;
- **Electronic registers**, with a major novelty, namely, the creation of a Common Electronic Register which will receive all the documents and communications that were mistakenly presented by citizens to the wrong eRegisters, so as to allow the Administration to know about these documents;
- The minimal and essential **requirements pertaining to eIdentification and eAuthentication**, so as to strengthen the flexibility criterion introduced by the eGovernment Law. To this end, the decree lays down specific provisions to facilitate the performing of proceedings in the name of a third party, by means of two mechanisms: the authorisation to present electronic documents on behalf of an interested party and the possibility for mandated civil servants to carry out the eIdentification and eAuthentication of citizens in the services and procedures for which they are needed;
- **Electronic communications and notifications** - the Decree establishes the necessary guarantees so that the facilities included in the Law on Citizens' Electronic Access to Public Services do not become a disadvantage for the interests of the citizens or for the general interest. The Decree regulates the conditions concerning the obligation of communicating through electronic means, the choice of the communication and notification channel by the citizens, the use of email for notification purposes and other conditions pertaining to electronic communications and notifications;
- The **proceedings for obtaining or submitting documents** which are in the hands of the Central Government and its public bodies. Thanks to this regulation, citizens are exempt from having to visit the Administrations' offices to obtain or to bring such documents;
- **Electronic documents**: features, validity, electronic copies, groups of senders, archiving, preservation and disposal.

Royal Decree 3/2010

The Royal Decree 3/2010, of January 8th (Official Diary of the State, January 29th) regulates the National Security Framework[18] (in Spanish 'Esquema Nacional de Seguridad' - ENS) foreseen in the article 42 of Spain's Law on Citizens' Electronic Access to Public Services (Law 11/2007, also referred to as the 'eGovernment Law').

The **ENS sets out the security policy to be applied by all public administrations is Spain for the use of electronic means in the frame of eGovernment** by formulating the basic principles and the minimal requirements for an adequate protection of information. The systems which manage classified information are out of this scope.

The main objective of the ENS is the creation of the necessary conditions of confidence in the use of eGovernment services, through the adoption of measures to ensure the security of information and

[18] *Source : http://www.epractice.eu/en/library/309251*

services that permits the exercise of rights and the fulfilment of duties through the electronic access to public services. The ENS also introduces the common elements that will guide the activity of Public Administrations in relation to security and the common language that will facilitate the interaction among public administrations as well as the communication of security requirements to the ICT Industry.

In order to create such conditions, the ENS introduces the **common elements** that must guide the action of the Public Administrations regarding security. Particularly it introduces the following main elements:

- The **basic principles to** be taken into account when adopting decisions about security;
- The **minimum requirements** for the adequate protection of information;
- The **procedure to fulfil the basic principles and minimum requirements** by means of the adoption of proportionate security measures, according to the information and services to be protected and to the risks to which they are exposed. This is made through the categorization of systems in three levels, Low, Medium, High, on the basis of the possible impact of security incidents in availability, confidentiality, integrity, authenticity and traceability;
- The **security audit**: The need to perform regular security audits is also enshrined in the ENS; it provides for the regular performance of an audit, every two years at least for systems categorized as medium or high;
- The **response to security incidents (CERT)**: The ENS defines the methodology to respond to incidents affecting security and outlines the important part played by the National Cryptology Centre, either as the editor of the Security Guides for the Administration or as the main actor of the coordination of response to security breaches (CCN-CERT);
- The ENS recognizes the role of **certified products in the fulfilment of the minimum security requirements**, the relationship with the Certification Body of the National Evaluation and Certification Scheme, how certified products contribute in a proportionate way to security in a number of security measures stated in the Framework and a model statement for calls for tenders;
- The **compliance with the National Security Framework**.

This Royal Decree was prepared following a process coordinated by the Ministry of Territorial Policy and Public Administration (formerly by the Ministry of the Presidency) with the support of the National Cryptologic Centre (CCN), Ministry of Defence. The Ministry of Industry, Tourism and Trade has an implicit role through its responsibilities in the regulation of eSignature and eGovernment and an explicit one by means of the National Institute of Communication Technologies (INTECO).

Freedom of Information Legislation

Law on Rules for Public Administration

The Law on Rules for Public Administration of November 1992[19] provides for **the access to Government records and documents**, as well as administrative proceedings by Spanish citizens. The document in question must be part of a file which has been completed.

Agencies must respond to an access request within three months' time. Documents can be withheld if the public interest or a third party's interest would be better served by non-disclosure, or if the request affects the effectiveness of operations of the public service. Access can be further denied if the documents refer to Government actions related to constitutional responsibilities, national defence or national security, investigations, business, industrial secrecy or monetary policy.

Access to documents that contain personal information is limited to the persons named within the documents. There are also restrictions for information protected by other laws, including: classified information; health information; statistics; the civil and central registries; the law on the historical archives.

Access denials can be appealed administratively. The Ombudsman can also review cases of failure to follow the law.

Law on Citizens' Electronic Access to Public Services

Pursuant to this law, citizens have the right to access by electronic means the status of administrative proceedings they are interested in, except in cases where the applicable norm sets out explicit restrictions to such access. Furthermore, the administration shall put a restricted electronic access service at the disposal of the interested citizen who, once identified, may follow up the status of the relevant proceeding.

Data Protection/Privacy Legislation

Law on the Protection of Personal Data

The Organic Law 15/1999 of 13 December 1999 on the Protection of Personal Data[20] brought Spanish law in line with the EU Data Protection Directive (95/46/EC).

This law regulates the **processing of personal data in the public and private sectors**. It grants citizens with the right to access and correct their personal information in the records held by public and private bodies. Personal information may only be used or disclosed to a third party with the consent of the individual, and only for the purposes it was collected. Additional protections are provided for sensitive data. Furthermore security measures regarding personal data processing are regulated in Spain by the Royal Decree 1720/2007, which approves the regulation implementing

[19] Source: http://www.epractice.eu/files/eGovernment%20in%20ES%20-%20December%202009%20-%2013.0%20-%20PDF.pdf
[20] Source: http://www.epractice.eu/files/eGovernment%20in%20ES%20-%20December%202009%20-%2013.0%20-%20PDF.pdf

Organic Law 15/1999. This regulation establishes the measures to be implemented considering the different levels of security required accordingly with the sensitiveness of the personal data and the purpose of the processing.

Both regulations are enforced by the Spanish Data Protection Agency.

Law on Citizens' Electronic Access to Public Services

Even though this law does not bring any formal innovation to the Law on Protection of Personal Data, it states that **data security guarantees** in electronic administrative procedures must be "at least at the same level" as in traditional administrative procedures.

According to the principle of proportionality, the security level should be "appropriate to the nature and circumstances of the different transactions and proceedings" and data shall be required from citizens when "strictly necessary to the purpose for which they are requested".

In this light, public authorities in possession of data previously requested from citizens shall facilitate the electronic retrieval of those by other public bodies, provided that the interested individual consents to the access to his/her personal data pursuant to the law on the Protection of Personal Data.

eCommerce Legislation

Law on Information Society services and electronic commerce

The Law 34/2002 on Information Society Services and Electronic Commerce of 11 July 2002[21] implements the EU Directive on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market (Directive 2000/31/EC on 'electronic commerce').

It is to be noted that the Law 56/2007 on **measures to promote Information Society** modifies the Law on Information Society services and electronic commerce by establishing an eAccessibility obligation. It states the following: "As from 31 December 2008, the web pages of the Public Administrations will satisfy at least the average level of content accessibility criteria generally acknowledged. As an exception, this obligation will not apply when the technological solution supporting a functionality or service does not allow for such accessibility".

eSignatures Legislation

Law on electronic signature

The Law 59/2003 of 19 December 2003 on electronic signature[22] replaced a Royal Decree of 1999 on digital signatures. Aimed at **promoting a widespread use of digital signatures** for eGovernment and eCommerce, it transposed the EU Directive 1999/93/EC on a Community framework for electronic signatures into Spanish law.

---

[21] *Source: http://www.epractice.eu/files/eGovernment%20in%20ES%20-%20September%202009%20-%2012.0.pdf*
[22] *Source: http://www.epractice.eu/files/eGovernment%20in%20ES%20-%20September%202009%20-%2012.0.pdf*

Amongst other provisions, the law clarifies relevant concepts and terminology, introduces a digital signature for legal entities, promotes certification industry self-regulation, and establishes a legal framework for the development of a national electronic ID card.

In addition, the Royal decree of 23 December 2005 regulates the issuance of the national ID document and its eSignature certificates. This has been recently amended by Royal Decree 1586/2009, 16th October.

Law on Citizens' Electronic Access to Public Services

The so-called 'Law on eAdministration' of 2007 states that in their electronic relations with citizens, **Public Administrations shall accept any eSignature means that complies with the law on Electronic Signature of 2003**, provided that those means allow for the adequate identification of participants, as well as for the authenticity and integrity of electronic documents.

Moreover, the **law lists all eSignature means** - simple or advanced - which may be opted for by citizens and Public Administrations while specifying their conditions of use. The law furthermore states that, for any eGovernment transaction, citizens may use the eSignatures integrated in the national electronic ID card, whenever they are requested to sign a document electronically.

ICT Legislation

General Telecommunications Law

The General Telecommunications Law 32/2003 of 3 November 2003[23] **implements** in Spanish law the **EU regulatory framework for electronic communications**. It is worth noting that the transposition was completed with the adoption of a Regulation on electronic communication markets in December 2004. The regulation specifies conditions for electronic **communications services provision, the universal service and users' right protection.**

This Regulation completes the transposition of EU Directives on electronic communications, developing the Telecommunications Act with regard to five broad sections: conditions to be met by operators, regulation of Universal Service (benefits that includes designation of the provider, cost and funding), the protection of personal data in the provision of services, regulation of the lawful interception of communications, and, finally, a comprehensive and detailed regulation with regard to the rights of end users.

Ministerial Order ITC/2382/2008

The Ministerial Order ITC/2382/2008 of 5 August 2008 was published by the Ministry of Industry, Tourism and Trade. It established an in**tegrated framework for the promotion, financial support and management of the actions and projects within the 'Strategic Action for Telecommunications and the Information Society'** implemented under the National Plan of Scientific Research, Development and Technological Innovation (2008-2011).

For the Ministry's State Secretariat of Telecommunications and the Information Society, the support and the promotion of the activities led under this Strategic Action constitutes a basic strategy within the policies aimed at promoting the development of the Information Society. The Ministerial Order ITC/2382/2008 modified the Ministerial Order ITC/464/2008 of 20 February 2008.

Law on measures to promote Information Society

[23] *See:* http://www.epractice.eu/en/document/288370

The Government approved on December 2007 the **Law on Measures to Promote the Information Society**, which is part of the set of measures constituting the Plan 2006-2010 for the development of Information Society and Convergence with Europe and between Autonomous Communities and Cities (Plan Avanza).

The law introduces innovations in policy areas of the Services of Information Society and Electronic Commerce and Electronic Signature Law for the promotion of Information Society in Spain and aims to cover regulatory gaps, remove barriers and enhance the rights of citizens in the Information Society.

Self-regulations

Self-regulatory Code of Conduct for mobile operators designed to encourage responsible use by underage persons of electronic content serviced supplied via mobile telephone networks in Spain[24]

The Spanish mobile telecom operators have adopted a code of conduct that describes duties of the signatory members in ensuring minimum protective measures for safer use of the content provided on the mobile phone. The code has been tailored to the needs of the Spanish mobile electronic telecommunications market and complies with applicable European and national legislation.

Key policy measures

DNI electronico (DNIe), Spanish Electronic Identity Card.

In Spain, an operational eID smartcard ("DNI electronico") is implemented which is gradually substituting for the mandatory "paper" ID card. At this moment, more that 20 million have been distributed among Spanish citizens.

This eID smartcard contains 2 certificates for authentication and signing respectively, and gives any citizen a powerful tool to benefit from the Information Society in a secure way. In particular, it gives her/him a secure and easy way to accredit her/his identity on the Internet.

This project is lead by the Ministry of the Interior and the Ministry of Industry, Tourism and Trade is massively collaborating with it from the beginning. Many actions have been implemented under this collaboration (Among which are educational campaigns and the elaboration of protection profiles based on Common Criteria for the development of secure DNIe applications).

Esquema Nacional de Seguridad (ENS), National Security Framework within the e-government scope.

The Royal Decree 3/2010, of January 8th regulates the National Security Framework foreseen in the eGovernment Law 11/2007. For a description of the Royal Decree and Law, please refer to the section above.

[24] *See:* http://www.gsmeurope.org/safer_mobile/national.shtml

This Framework establishes the security policy in the use of electronic means in the scope of the eGovernment Law 11/2007; this security policy will be formed by the basic principles and minimum requirements for an adequate protection of information, among them, the implementation of risk analysis and the PDCA cycle.

The National Security Framework pursues the creation of the necessary conditions of confidence in the use of electronic means, through measures to ensure the security of systems, data, communications and electronic services that permits the exercise of rights and the fulfilment of duties through the electronic access to public services; to ensure that information systems will provide their services in accordance with their functional specifications and will protect information.

In order to create such conditions, the National Security Scheme introduces the common elements that have to guide the action of the Public Administrations regarding security. Particularly it introduces the following principal elements:

- The **basic principles** to be taken into account when adopting decisions about security;
- The **minimum requirements** for the adequate protection of information;
- The **procedure to fulfil** the basic principles and minimum requirements by means of the adoption of proportionate security measures.

Transposition of the amendments of the Telecommunications Package Directives regarding security and privacy.

In 2009, the regulatory framework for electronic communications networks and services was amended. Some of these amendments deals with security (article 13 a and b of the Framework Directive) and privacy (articles 4 and 5 of the Directive on privacy and electronic communications).

The State Secretariat for Telecommunications and the Information Society (SETSI) of the Ministry of Industry, Tourism and Trade, in collaboration with the Spanish Agency for Data Protection in privacy matters, is charge of this transposition that is already in its final stages (deadline: May 25th of 2011).

Critical Information Infrastructure Protection.

Critical Information Infrastructure Protection is included in the broader scope of Critical Infrastructure Protection. Two milestones may be emphasized here: first, the creation in 2007 of the National Centre for the Protection of Critical Infrastructures (Centro Nacional de Protección de Infraestructuras Críticas, CNPIC), under the Secretary of Security of the Ministry of Interior, and second, the Draft Law on Critical Infrastructure Protection, that is also in the final stages for its approval.

Children Protection

There are many actions to promote a safe Internet for children. Among them:

- **INTECO** (cfr. Country-specific activities for identifying and promoting economically efficient approaches section)**:** provides **information, advice, guides, reports, tools** and educational games for parents and children;
- **Ministry of Interior:** its two nationwide police forces (Cuerpo Nacional de Policía and Guardia Civil) have units specialized in fighting cybercrime and specially pornography. These units are the **Brigada de Investigación Tecnológica** (Cuerpo Nacional de Policía) and the **Grupo de Delitos Telemáticos** (Guardia Civil).

Protegeles.com is a non-profit web site for the **protection of childhood** that provides, among other services, a hotline to report harmful content.

Pantallasamigas.net is another non-profit web site for the **promotion of a safe use** of Internet among children and young people that also provides a hotline to report harmful content.

Chaval.es is al website for the **promotion of a safe and beneficial use of the Internet** targeted to parents and children, run by RED.es (that is Public business entity attached to the Ministry of Industry, Tourism and Trade in charge of driving the development of the Information Society in Spain).

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	• Ministry of Industry, Tourism and Trade (MITYC)— State Secretary of Telecommunications and Information Society (SETSI) • Ministry of Interior (Home Office) — Secretary of Security (SES) • National Cryptologic Centre - Centro Criptológico Nacional • Ministry of Territorial Policy and Public Administration- Ministerio de Política Territorial y Administración Pública (MPTAP) • National Centre of Protection of Critical Infrastructures (CNPIC) • Spanish Data Protection Agency - Agencia Española de Protección de Datos • Higher Council for Electronic Administration - Consejo Superior de Aministración Electrónica (CSAE) • Certification Body (CB) of the Spanish Evaluation and Certification Scheme • Council of Accreditation and Certification – Consejo de Acreditación y Certificación • National Institute of Communication Technologies (INTECO) • Sectoral Committee for e-Government • Advisory Council on e-Government (Consejo Asesor de Administración Electrónica)
CERTs	• CCN-CERT - Computer Security Incident Response Team of the Cryptology National Center (part of the Defence Ministry) • CSIRT-CV - Centro de Seguridad TIC de la Comunidad Valenciana • e-LC CSIRT - e-LaCaixa CSIRT • esCERT-UPC - CERT for the Technical University of Catalunya • INTECO-CERT- the INTECO IT Incident Response Center • IRIS-CERT - RedIRIS' security service • CESICAT – The Catalan Government agency in charge of executing the National Plan for IT security • S21sec CERT – Managed security services provider
Industry Organisations	• CONETIC (Spanish Electronics, Information Technology and Telecommunications Industry Association) • ISMS Forum Spain (Spanish forum for the promotion of Information Security) • Fundación Círculo de Tecnologías para la Defensa y la Seguridad: Initiative that encourages initiatives aimed at the creation and development of a national technology applicable to the Defence and Security, especially in the areas of electronics, computers and telecommunications. • AETIC (Spanish Electronics, Information Technology and Telecommunications Industry Association) • ASIMELEC (Spanish Electronic and Communications Multisectorial Industry Association) • AMETIC: Merge of AETIC and ASIMELEC • ASTEL (Competitive Telecommunications Association) • ANEI (National Association of Internet Enterprises) • AECEM – FECEMD (Spanish Association for Electronic Commerce and Relational Marketing) • CNCCS – Consejo Nacional Consultor sobre Cyber-Seguridad (National Advisory Council for Cyber-security) • Spanish platform for security and trust technologies (eSEC)
Others	• Council of Consumers and Users • Asociación de Usuarios de Internet (AUI) – Association of Internet Users • Asociación de Internautas – Association of "Internauts" • Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI) • Protegeles • Pantallasamigas.net • Chaval.es • Defender of the e-Government users (Defensor del usuario de la administración electrónica)

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"[25] – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory[26].

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Co-operation between public authority bodies

In Spain there is no single agency responsible for NIS.

The **Ministry of Industry, Tourism and Trade (MITYC)** is responsible for proposing and carrying out government policy in, among others, the area of electronic communications networks and services, and the Information Society. In particular, this responsibility is carried out by the Secretary of Telecommunications and Information Society (SETSI).

The **Ministry of Interior** has overall responsibility for critical infrastructure protection (CIP/CIIP). Within the Ministry of Interior, the Secretary of Security (SES) is responsible for development of the National Critical Infrastructure Protection Plan.

The **National Cryptologic Centre (CCN)** is the organization responsible for coordinating the different organizations' activities in the Public administration area using resources or encryption procedures and ensuring the security of the information technologies in all areas, keeping informed concerning the coordinated acquisition of cryptologic material and it is also responsible for providing training for Public Administration resources who specialise in this field.

CCN also acts as a certification body and runs the CCN-CERT, the Governmental CERT. It is established by law that the National Cryptologic Centre must establish the necessary relationships and the signature of the corresponding agreements with similar organizations of other countries, in order to carry out its functions. For the development of these functions, the CCN can establish the appropriate coordination with the national commissions to which the law assigns responsibilities in the field of the systems of information and communication technologies.

The **National Security Framework (ENS)** states that the CCN-CERT will provide the Public Administrations with the following services:

---

[25] *The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010*

[26] *http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/*

- **Support and coordination for treating vulnerable aspects and solving 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 objectives indicated above, the audit reports of the affected systems will be used.
- **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.
- **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.
- **Information about vulnerable aspects, alerts and warnings** of new threats to information systems, gathered from different sources of renowned prestige, including own sources.

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

The ENS also states that to guarantee full compliance with the provisions of the **National Security Framework**, in exercising its functions, the CCN will prepare and distribute the respective information technology security guides and communications.

Along this line, the CCN has developed its institutional and communication activity in different ways: adhesion and participation in organizations and international programs (especially in NATO and EU), collaboration agreements to impulse the security aspects, exchange of information, adjustment of regulations and international procedures or training campaigns or campaigns to raise awareness and which are meant for the staff of the Administration.

CCN is also a member of the **Superior Council of Electronic Administration**, the member body ascribed to the **Ministry of Territorial Policy and Public Administrations**, in charge of the preparation, creation, development and application of the Government's policy and strategy on information technology matters, as well as the promotion and implementation of the electronic Administration in the State's General Administration. It acts over plenary and in permanent commission and one of its members is the general Deputy General Director of the National Cryptologic Centre.

The CCN participates in the working groups coordinated by the National Centre of Protection of Critical Infrastructures, CNPIC, (depending on the Ministry of Interior) which guards and updates the Security Plan and the National Catalogue of Critical Infrastructures. It participates actively in national working groups on encryption of the Ministry of Defence.

Among the different agreements reached by the National Cryptologic Centre, the one signed with the National Institute of Communication Technologies (INTECO) stands out. This agreement's purpose is to promote security aspects within the development of the Information Society in Spain, by the exchange of information, specialized training and the development of technological projects. In addition, the CCN-CERT is a special member of the ABUSES forum, aimed at ISP technicians and professionals who manage or are interested in solving network security incidents and complaints.

In the same way, CCN maintains an agreement with the Federación Española de Municipios y Provincias (FEMP) whose aim is to boost information security among local entities.

The CCN-CERT, as the Spanish Government CERT, provides the necessary information and tools for the different administrations to develop their own CERTs, allowing this team to act as a catalyst and as coordinator of these ones. So, the first agreement with a regional government CERT was signed in 2008 with CSIRT-CV of Comunidad Valenciana to boost security aspects through information exchange, specialized training and the development of technological projects within this autonomous region.

Co-operation and initiatives on Security incident

The CCN attends the INFOSEC committees and accreditation panels in representation of the Delegated Authority of the ANS (National Authority of Security). It also attends other forums related to Information Technologies Security.

The CCN-CERT has also intervened in the meetings and working groups of the ENISA, NCIRC (NATO Computer Incident Response Capability) and CSIRTs with national responsibility (CERT CC). It is a member of the European Government CERTs (EGC) group, of the Forum of Incident Response and Security Teams (FIRST), of the Trusted Introducer of TERENA (Trans-European Research and Education Network Association) and of the APWG (Anti-Phishing Working Group).

In Spain, CCN-CERT is a distinguished member of CSIRT.es, a collaboration group between incident response teams whose sphere of action is established into user communities within the Spanish territory.

INTECO through INTECO-CERT is also integrated as a member in these forums such as FIRST, CERT/CC, APWG, TERENA, Trusted-Introducer, PSG of ENISA, DIGITAL PHISNET, CSIRT.es, ABUSES, ISMS Forum Spain, AENOR, etc.

There are many organizations that collaborate on a regular basis with CCN-CERT and INTECO-CERT spreading their **information** or providing them with **data on security incidents**:

- Central government, regional government, local government, councils;

- Universities and academic institutions;
- Media (Internet, press, radio);
- Antimalware manufacturers and distributors, vulnerability databases;
- Public sector companies, ISP's;
- Law enforcement agencies;
- International CERTS's and bodies (e.g. NIST (Department of Commerce, USA), INTECO has reached an agreement with NIST to promote and feed the international standard for ICT vulnerabilities, named CVE, on other languages such as Spanish).

The www.ccn-cert.cni.es portal is the main tool developed by the CCN-CERT to **coordinate and give support** to those responsible for the administrations' ICT. The Web offers, among other things, daily updated information concerning threats, vulnerabilities, configuration guidelines for different technologies, security tools, training courses or instructions for best security practices.

CCN-CERT has also developed **early warning services** to reduce the response time to solve incident affecting the Government networks.

Citizens and companies can also report incidents to INTECO-CERT via their portals http://www.inteco.es, http://cert.inteco.es, or the National Security Helpdesk for Citizens, http://www.osi.es, via email or via phone.

Co-operation between public network providers and public authorities

The National Centre for Critical Infrastructure (CNPIC) requests information about electronic communication networks from SETSI (Secretary of Telecommunications and Information Society), which collects the information from electronic communications networks operators and services providers, as well as citizens. As a result, SETSI asks infrastructure owners and service providers to share a summary of recovery plans, of which infrastructure is considered critical, of business continuity plans and so forth.
More information and indicators of security at households or SMEs is provided by INTECO.

Major electronic communications providers are obliged to carry out a quarterly publication of QoS parameters (services concerned: fixed publicly available telephone service (fixed PATS), mobile PATS, Internet access and directory service).

Additionally, electronic communications providers are obliged to report to the SETSI any disruptions of PATS or Internet access service which affect more than 100,000 subscribers. Moreover the SETSI may demand correcting actions. The Regulation on the provision of electronic communications services, universal service, and user protection forces electronic communications network providers and public telephone service providers to guarantee their networks´ integrity.

There is no mechanism in operation where telecom providers and infrastructure owners meet on a regular basis to address resilience and/or security issues. Nevertheless, telecom network owners and service operators have got their own coordination bilateral mechanisms, such as a committee addressing technical issues.

In events of **large service disruption affecting critical services** (health care, security, defence, etc.), Incident Management Committees are formed by the Regional Delegations of the Central Government (Delegaciones del Gobierno), The SETSI, critical services managers and involved electronic communication providers take part in these committees and exchange information with each other, set priorities and collaborate within their competence scope. Topics addressed deal with these regarding disruption events, such as:

- Elements involved;
- Expected recovery time and actions;
- Contingency measures;
- Priority setting;
- Possible causes;
- Damages;
- Measures to be taken to avoid similar future incidents.

Fostering a proactive NIS community

International co-operation via the European Government CERTs (EGC) group

CCN-CERT is amongst the active members[27] of the **European Government CERTs (EGC) group**. ECG is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe. To achieve this goal, the EGC group members:

- Jointly develop measures to deal with large-scale or regional network security incidents;
- Facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities;
- Identify areas of specialist knowledge and expertise that could be shared within the group;
- Identify areas of collaborative research and development on subjects of mutual interest;
- Encourage formation of government CSIRTs in European countries;
- Communicate common views with other initiatives and organizations.

Data protection international co-operation

The Spanish DPA maintains a close collaboration with other European DPA's in order to investigate violations of Data Protection Act's, mainly with CNIL in France and ICO in Britain. It was done by means of investigation of complaints submitted to foreigner DPA's but with Spanish legal entities involved.

In other cases, there was a close interchange of information in case of international affairs, those who affect to companies that go through several countries.

The Spanish DPA collaborates with the European Union, by mean of twinning projects, to enhance the data protection enforcement in other countries that belong to the EU like Croatia or outside the EU like Israel, creating position in those countries for resident experts that develop training and awareness activities. In 2010 Spanish DPA started the development of the Twinning Project for Capacity Building of the Croatian Agency for Protection of Personal Data (CAPPD).

This Twinning Project includes a technical component based on the Croatian regulation which establishes as legal framework on security measures regarding personal data the ISO 27001 Standard. The role of the Spanish DPA is to coordinate the activities for the CAPPD to implement an Information Security Management System.

In addition, the Spanish DPA is an active member in the discussions of the article 29 working party that deals with the protection of personal data across Europe, in particular security measures, data interchange over communication networks, and so on.

---

[27] *The members of the European Government CERTs group include: Austria - GovCERT.AT, Finland - CERT-FI, France – CERTA, Germany - CERT-Bund, Hungary - CERT-Hungary, Netherlands - GOVCERT.NL, Norway – NorCERT, Spain - CCN-CERT, Sweden - CERT-SE, Swiss - GovCERT.ch, United Kingdom – CSIRTUK, United Kingdom – GovCertUK; See more details at: http://www.egc-group.org/*

Private sector NIS communities

CNCCS (Consejo Nacional Consultor sobre Cyber-Seguridad) is a private initiative born in May 2009 resulting from the concern of the Spanish security industry.

The Council brings together all the Spanish industry leaders in Computer Security: Aedel, Amper, Bdigital, Colegio Oficial de Ingenieros de Telecomunicaciones, Colegio Oficial de Ingenieros en Informática del País Vasco, Universidad Deusto, Hispasec Sistemas, Indra, Informática 64, Internet Security Auditors, Kinamik, Optenet, Panda Security, Secuware, S2grupo, S21sec and Tb security.

The **CNCCS** has the following objectives:

- Protecting consumer identity ;
- Critical Infrastructure Protection;
- The creation of national legislation to combat cyber-crime;
- The protection of corporate information;
- The evolution of the government structure from the focus of the physical realm to cyberspace ;
- The improvement and support, from the standpoint of the Council, of economic prosperity and national security.

Created by AETIC, the **Spanish platform for security and trust technologies** (**eSEC**) is a network for scientific and technologic cooperation that brings together companies and research institutes focused on technologies for the improvement of security and trust in the Information Society.

Its mission is:

- Definition of a **Strategic Research Agenda** in this sector;
- Mobilization of a **critical mass of R&D** to gain momentum to the Spanish sector.

Currently it has five working groups:

- **Development of applications** using the Spanish e-ID (DNIe);
- **Trustworthy** in the Future Internet;
- Property **security**;
- **Health** Privacy and Security;
- **Managed** Information Security.

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

Since beginning of 2010, there were no major changes to the security incident management stakeholders in Spain.

The main CERTs in charge of the coordination and response to security incidents at a national level remain:

- The **Spanish Governmental CERT**: CCN-CERT (Ministry of Defence). Run by the National Cryptologic Centre (CCN), the CCN-CERT offers support and coordination for the prevention and resolution of incidents suffered by the General, Autonomic or Local Administration. It has also a relevant role in the National Security Framework within the e-government scope (see above).
- **INTECO-CERT** (Ministry of Industry, Tourism and Trade) is the Spanish Computer Emergency Response Team for SMEs and Citizens. Its purpose is serving as a preventive and reactive support related to ICT security for SMEs and citizens. It has a vocation of public service as a non-profit organization and offers help that, in all cases, is free and rapidly managed. Additionally, INTECO has developed the protection profiles (ISO15408 - Common Criteria[28]) for the Spanish Digital Identity Card, DNIe, a catalog of SICT (Security Information and Communication Technologies) solutions and companies as well as security awareness programs such as security week, European data privacy day, safer internet day, etc .
- **IRIS-CERT** (Ministry of Industry, Tourism and Trade) is aimed to the early detection of security incidents affecting RedIRIS centres (that supports University and research institutions), as well as the coordination of incident handling with them. Furthermore proactive measures are in constant development. IRIS-CERT also acts as a last point of contact for incident handling coordination for emergency or high priority security matters affecting the .es domain (Spanish national ccTLD).

The Spanish competent national data protection authority disclosed the fact that it has imposed 39 fines in 2008 of for sending unsolicited email and SMS, two of them for 30.000 EUR (one of which for unsolicited SMS) with a total of 85.500 EUR.

Additional information about this kind of incidents is provided by INTECO through a National eFraud Repository, with more than 3.500 incidents in relation to electronic fraud (such as phishing, scam, trojans and malware, etc.). This repository provides support to different entities, such as Law Enforcement, eBusiness and eBank companies, ISPs, CERTs and CSIRTs, and also citizens and SMEs, in order to establish reactive and preventive strategies against eFraud.

[28] *See: http://www.commoncriteriaportal.org/*

Emerging NIS risks

In 2010, a new 'Information Society' report was released by the authorities on the implementation state of the different NIS risk safeguards.

The reports carried out within Plan Avanza2[29] (2008-2009) show that the implantation of usual safety precautions on the Net by users recorded an increase compared to previous years. However, there is a widespread spike in the total number of security issues experienced by users. An exception to this trend are the intrusions found in services such as email, which have been reduced, and scams using online accounts, which have remained unchanged at minimum and residual levels.

Resilience aspects

Compared with 2009, the authorities in charge of network resiliency in Spain in 2010 remain:

1. The Spanish National Centre for Critical Infrastructure Protection (CNPIC). The Secretary of Security (SES) of the Ministry of the Interior is responsible for working out the National Critical Infrastructure Protection Plan. Within the structure of the SES, the CNPIC leads and co-ordinates most initiatives and activities related with Critical Infrastructure Protection, and therefore CIIP, which are assigned to the State Secretariat. CNPIC was created in 2007.
2. The Secretary of Telecommunications and Information Society (SETSI) and the Ministry of Industry, Tourism and Trade (MITYC). The SETSI reports to the MYTIC. SETSI is one of the contact points for infrastructure operators and service providers in the telecom industry.
3. The Regional Delegations of the Central Government.

As specified in the Telecom's Act, it is part of MYTIC's and SETSI's mandate to ensure that the public service obligation is being met, consumer interests are addressed and spectrum regulation is done according to the Law. When it comes to user rights, MITYC promotes Quality of Service, particularly by making QoS transparent, publishing performance data on the Internet for consumers to see. In cases of large disruption events, the CNPIC requests information from SETSI, which collects the information from the different providers. The involved telecommunications operators shall provide SETSI, on a mandatory basis, with the following information:

- **During the first 2 hours of disruption:** preliminary report identifying the event (including physical location, starting time, end-users involved, possible causes, on-going correcting measures and scheduled recovery time).
- If the event **lasts more than 6 hours**: any necessary reports to update the initial information, a report including the adopted measures and any additional information requested by the SETSI.

[29] *Source: La sociedad en Red: "Informe anual de la sociedad de la información en Espana 2009" (Ed. 2010).* http://www.ontsi.red.es/informes-anuales/articles/1449

- By the **end of the event**, during the following 2 hours: closing event report, including exact time of recovery of each element involved.
- During the **following 10 days** after the recovery: a thorough report including, among other aspects, the disruption scope, affected users and damages, compensating actions, cause assessment, correcting measures and recurrence likelihood assessment.

Information about such large disruption events (such as disasters caused by nature such as avalanches or flooding, expected recovery time, contingency measures, possible causes, damages, etc …) is exchanged within the Incident Management Committees established by the Regional Delegations of the Central Government.

The Regulation on the provision of electronic communications services, universal service, and user protection forces electronic communications network providers and public telephone service providers to guarantee their networks´ integrity. Major electronic communications providers are obliged to carry out a quarterly publication of QoS parameters (services concerned: fixed PATS, mobile PATS, Internet access and directory service). Additionally, electronic communications providers are obliged to report to the SETSI any disruptions of PATS or Internet access service which affect more than 100,000 subscribers. Additionally, SETSI may demand correcting actions.

There is no specific regulation pertaining to resilience and dependability of networks in the Telecommunication Act itself. Neither has the CNPIC so far come up with a recommendation regarding regulation and resilience of e-communications networks.

Privacy and trust

Spanish Data Protection Agency (AEPD)

AEPD is the public law entity overseeing compliance with the legal provisions on the **protection of personal data** and, as such, is called to enforce and promote information security aspects related to data protection. In this respect, the Agency has the power to inspect, ex officio or in response to citizens' complaints, all equipments issued in the processing of personal data and to impose sanctions in case of non compliance with provisions referred to security measures. Apart from that, the Agency undertakes a variety of activities aimed at raising awareness of both citizens and companies with regard to data security.

The AEPD has dealt with more than 6.600 complaints in the last year, related with all kinds of Data Protection Act infractions. All have been processed, and, specifically on security measures and e-commerce, it has opened 73 files, 92 files on internet services, 447 to telecommunication companies and 697 in other new technology threads like video surveillance. It has issued fines around 20 million €. As it is describe in this document, the Spanish DPA has done many control, advice, and awareness activities. Their scope have been national and international.

Trust in the Information Society

Trust in the Information Society was a conference focused on e-trust and on how the Information Communication Technology (ICT) can be a generator of trust or can be adapted and used to generate e-trust. The Advisory Board of Research and Innovation for Security, Privacy and Trustworthiness in the Information Society – RISEPTIS – published in its latest report a set of conclusions that form the core of the event concerning trust in the Information Society. Derived from this report a set of fundamental topics emerge:

- Digital Life and Trust;
- Trustworthy networking and computing services;
- Management of Digital Identities in the Common European Framework;
- Development of the Legal Framework of the EU on Protection of Data and Privacy.

These and other topics of the highest importance for the future of the Information Society in Europe were discussed on the 10th and 11th of February in 2010 in the Auditorio of León, Spain. Conference report, conclusion, presentations and video of the whole conference are accessible via: http://trustworthyict.inteco.es/web/en.html & http://www.trustworthyict-inteco.webcastlive.es/.

NIS awareness at the country level

The reports carried out within Plan Avanza have proved the need to provide security support to the Spanish business network (94% are SMEs) and to the citizens, whose training and awareness in computer security matters must be increased.

In this context, the first version of Avanza Plan (2005-2009) included a specific line of action on "**Education within the Digital Era**" to incorporate ICTs in the education and training process in general, involving all agents taking part in this project. The second phase of the Plan, Avanza2 (2009-2012), includes a line of action on "Security and Accessibility" with the objective of fostering citizens' and businesses' trust in ICT and to improve the accessibility of eServices.[30]

In addition, **INTECO**, through INTECO-CERT, the National Security Helpdesk for Citizens, and the Information Security Observatory, arises as a public initiative with the following aims:

- To provide clear and concise information about technology and its use and security, in order to increase the understanding among citizens of these matters. During 2009 and 2010 INTECO developed two awareness campaigns, one focused on citizens and the other on SMEs;
- Make SMEs and citizens aware of the significance of considering and properly tackling the aspects related to computer security and communication networks. This included developing different kinds of awareness-raising programs which reached nearly 2.000 SME's and online training courses which reached nearly 16.000 citizens in 2010;
- To provide best practices, recommendations, security bulletins and alerts, vulnerabilities management service, precautions guides and security tools in order to improve security;

[30] *See: http://cert.inteco.es/About/Mission_and_Aims/*

- To provide popularization, training, prevention and reaction tools & services against incidents in information security matters: INTECO developed a Catalogue of ICT Security Companies and Solutions which organises the different companies working in Spain in the area according to a self-developed taxonomy;
- To act as a link between the needs of SMEs and citizens and the solutions offered by the companies of the Information Technologies security sector;
- To provide information and indicators about vulnerabilities, alerts and advice on new threats targeted at Information Systems, compiled from different renowned and prestigious (including their own);
- To provide different security studies and indicators of spam, eFraud, security levels at households and SMEs, etc.

All the CERTs described in the Incident Management section above are strongly committed to creating awareness among their respective audiences.

As an example targeted to the broad public Spain has the **Oficina de Seguridad del Internauta** (**OSI**)[31], Office for the safety of web users, run by the National Institute of Communication Technologies (INTECO), under the Ministry of Industry, Tourism and Trade.
OSI is a security helpdesk for internet users and provides information and support to prevent and solve security**.**

OSI's aim is building trust among citizens, especially those with very basic knowledge in ICT. OSI provides services of value for this target group, assuring that they are equipped with adequate ICT Security safeguards. Security services are offered free of charge to all users through a multi-channel communications platform that meets different needs and skills: web site, email and call centre (+34 901 111 121).

Its mission is to raise security culture, prevention, awareness and training providing clear and precise information and security tools, as well as fostering early detection and denunciation of any kind of threats, frauds and attacks in the Internet. It is supported by a web portal (www.osi.es), but it can be reached also by phone and e-mail.

The **CNCCS** (National Advisory Council for Cyber-security), with the participation of INTECO, has launched an awareness campaign on information security for citizens and SMEs in 2010 called Haztepre[32].

For Public administrations, CCN-CERT offers its services to all those responsible for Information Technologies by means of several important courses of action, including:

- **Research and diffusion** of the best practices on information security among all the members of Public Administrations. On this matter, the aforementioned Series CCN-STIC, developed

[31] *See: http://www.osi.es/*
[32] *See : http://www.haztepre.es/*

by the CCN, offer standards, instructions, guidelines and recommendations to ensure security of ICT systems in the Public Administration;

- **Training** through SICT courses, is aimed at training specialised Public administration staff in the area of ICT security. These courses are available throughout the year. The main objectives, besides keeping the CCN-CERT staff up to date, is to raise awareness and improve the staff's ability to detect and manage incidents;
- **Information** about vulnerabilities, alerts and advice on new threats targeted at Information Systems, compiled from different renowned and prestigious (including their own).

The CCN-CERT has an intense plan of **communication and awareness** in order to reach the acknowledgment and confidence of the people in charge of information and communication security in the Administration. Presentations of services for those in charge of security for the General Administration of the State and for those of regional governments of Aragón, Asturias, Cantabria, Castilla-La Mancha, Castilla y León, Comunidad Valenciana, Galicia and Madrid, and their corresponding city councils.

Likewise, the Spanish Governmental CERT conducts **seminars and workshops** on raising awareness, aimed at training and upgrading administration staff knowledge in the field of information security. All general, regional and local administration staff can attend these workshops should they wish to do so (the last conference, III Jornada STIC CCN-CERT was provided with the attendance of 300 participants from all parts of Spain). Additionally INTECO organizes an annual ICT conference named International Meeting of Information Security (ENISE[33]) about Technology challenges in Security and ICT.

One of the cornerstones of the Spanish regulation on security measures with regard to personal data is the obligation for the controllers to adopt a security document as a personal data policy. To this end, a guideline for the implementation of the security measures as well as a template of the security document has been delivered by the Spanish DPA.

Additionally an electronic tool (EVALUA) has been made available for controllers and processors to self-assess their compliance regarding data protection and security measures legal requirements.

The Spanish DPA has carried out **sector audits** related with the security measures taken in companies, public bodies, health centres and so on. The purpose of those sector audits was the awareness of the people in charge of the security measures required by the provisions of the Data Protection Act. Another important result is that the Spanish DPA draws up recommendations reports that release to the entities of each economical sector with the aim to regulate those sectors.

In addition, the Spanish DPA prepare conferences, seminars, reports, proceedings and other material, oriented to professionals and citizens, to aware about the risk and best practice in the use of network and information technologies.

[33] *See : http://enise.inteco.es/en*

In the private sector, the Law on Measures to Promote the Information Society requires Internet service providers to inform their users about technical means of protection from Internet security issues (viruses, spyware and spam) and on the tools to filter out unwanted content. The Spanish Government is developing a new action plan will include measures against malicious code, unsolicited emails (spam) messages and deceptive or fraudulent (phishing).

The service provider TELEFONICA plays an active role in the NIS awareness process and informs its clients extensively on how to combat spam and how to avoid other fraudulent practices on Internet. Likewise, TELEFONICA offers its clients different tools to combat spam, spyware and malicious software like spam filters, antivirus, etc… In Spain, VODAFONE, in its privacy policies, also informs its clients on how to avoid frauds on the Internet.

The internet users' association tried to create a platform with information on the fight against spam. The Spanish Data Protection Agency published recommendations to prevent spam. In 2008, INTECO published a very comprehensive report named "Study on the situation, nature and economic and social impact of spam". It also provides prevention information and more studies on its website (http://www.inteco.es and https://ersi.inteco.es/).[34]

[34] *Source:* *http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf*

Country-specific activities for identifying and promoting economically efficient approaches to information security

National Institute of Communication Technologies

Promoted by the Ministry of Industry, Tourism and Trade, INTECO (National Institute of Communication Technologies) is a **platform for the development of the Knowledge Society** through projects in the area of innovation and technology.

It has three **lines of action**:

- Security;
- Accessibility;
- ICT quality.

INTECO develops many activities for the identification and promotion of economically efficient approaches to information security. They include:

- Elaboration of protection profiles based on Common Criteria for the development of secure DNIe applications;
- National Laboratory of Software Quality;
- The Information Security Observatory;
- INTECO-CERT (cfr. Incident Management section);
- OSI (cfr. NIS awareness section);
- Sensors Networks[35] ;
- Major involvement in the DNIe project (cfr. eIdentity section).

To improve the security levels when the citizens contract services and products through Internet or by phone call, the Spanish DPA has carried out **specific sector audits** to analyze how is guaranteed the authentication, confidentiality and integrity of the data related with the contracting procedure. The results were draw up in recommendations reports released to the companies to improve the quality of the services and the rights of the citizens. Those recommendations are intended to improve the security and confidence of the citizens in the e-commerce activities and to give no fault liability to the companies.

Spanish Evaluation and Certification Scheme

The **Certification Body (CB)** of the Spanish Evaluation and Certification Scheme operates under the scope of the National Cryptologic Center, as laid out in the Act 11/2002[36], regulating the National Intelligence Centre, and the Royal Decree 421/2004[37], regulating the National Cryptologic Centre.

[35] *See : https://ersi.inteco.es/index.php?lang=en*
[36] *See : http://www.oc.ccn.cni.es/pdf/LeyesdelCNI.pdf*
[37] *See : http://www.oc.ccn.cni.es/pdf/RD421-2004CentroCriptologicoNacional.pdf*

The Certification Body operates under request of any private or public party that may wish to perform as a **security evaluation accredited laboratory**, as well as under request of any private or public product or system developer that may wish to certify the security properties by the Scheme and when such products or systems are subject to be included under the scope of the National Cryptologic Centre.

The Certification Body licenses laboratories based on the compliance of the requirements laid out in the Third Title[38], and in accordance with the procedure established in the Fourth Title[39] of the IT security evaluation and certification regulations, approved by ORDEN PRE/2740/2007[40].

The **Certification Body** certifies the security of information technology products in accordance with the procedure established in the Fifth Title[41], and following the evaluation standards, criteria and methodology listed in the Sixth Title[42] of the cited IT security evaluation and certification regulations.

The "Common Criteria"[43] certificates issued by this Certification Body are recognized by more than twenty countries.

In addition, the Certification Body is accredited by the Entidad Nacional de Acreditación[44], in accordance with the requirements laid out in the standard UNE-EN 45011:1998 for product certification[45].

The Council of Accreditation and Certification whose legal basis is the ORDEN PRE/2740/2007[46] is an advisory instrument of the Certification Body integrated by representatives of the Administration (Certification Body, Ministry of Defense, Ministry of Industry, Tourism and Commerce, Council for Electronic Administration), the Evaluation Laboratories and the ICT Industry as stated in its legal basis.

[38] *See : http://www.oc.ccn.cni.es/pdf/ORDENPRE27402007.pdf*
[39] *See : http://www.oc.ccn.cni.es/pdf/ORDENPRE27402007.pdf*
[40] *See : http://www.oc.ccn.cni.es/pdf/ORDENPRE27402007.pdf*
[41] *See : http://www.oc.ccn.cni.es/pdf/ORDENPRE27402007.pdf*
[42] *See : http://www.oc.ccn.cni.es/pdf/ORDENPRE27402007.pdf*
[43] *See : http://www.commoncriteriaportal.org/*
[44] *See : http://www.enac.es/*
[45] *See : http://www.oc.ccn.cni.es/pdf/45_CPR110.pdf*
[46] *ORDEN PRE/2740/2007 de 19 de septiembre, por la que se publica el Reglamento de Evaluación y Certificación deSeguridad de las Tecnologías de la Información especifica la creación de un órgano asesor del OC denominado Consejo deAcreditación y Certificación*

Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection

CNPIC (under the Secretary of Security of the Ministry of the Interior) guards and updates the **National Plan of Critical Infrastructures Protection** and the National Catalogue of Critical Infrastructures. For its management, an information system called "Hermes" is being developed.

Another important milestone is the **Draft Law on Critical Infrastructure Protection**, which is in the final stages for its approval. Among other issues, this Law transposes the Council Directive 2008/114/EC on the identification and designation of European critical infrastructures. This Law also establishes the whole organization in charge of Critical Infrastructure Protection as well as the role of the private sector in this organization.

Three cornerstones of CIP are **inter-service coordination, public-private partnership and international cooperation**.

Regarding international cooperation, CNPIC is a member of the EU Council working group on civil protection (PROCIV) and point of contact of the European Commission on CIP matters.

During the Spanish Presidency of the EU, CNPIC organized two international events:

- International Critical Infrastructure Protection Meeting (Madrid, 18-19 February 2010)
- EU-US Expert Meeting ON Critical Infrastructures Protection (Madrid, 4-5 March 2010)

CNPIC has also attended European Commission meetings organized by ENISA as the Article 13 Working Group, EFMS (European Forum for Member States) and EP3R (European Public Private Partnership for Resilience) and is responsible for CIWIN (Critical Infrastructure Warning Information Network) in Spain.

CNPIC also participates in the MERIDIAN[47] process, which aims to provide Governments worldwide with a means by which they can discuss how to work together at the policy level on critical information infrastructure protection (CIIP)

[47] *See: http://www.meridianprocess.org*

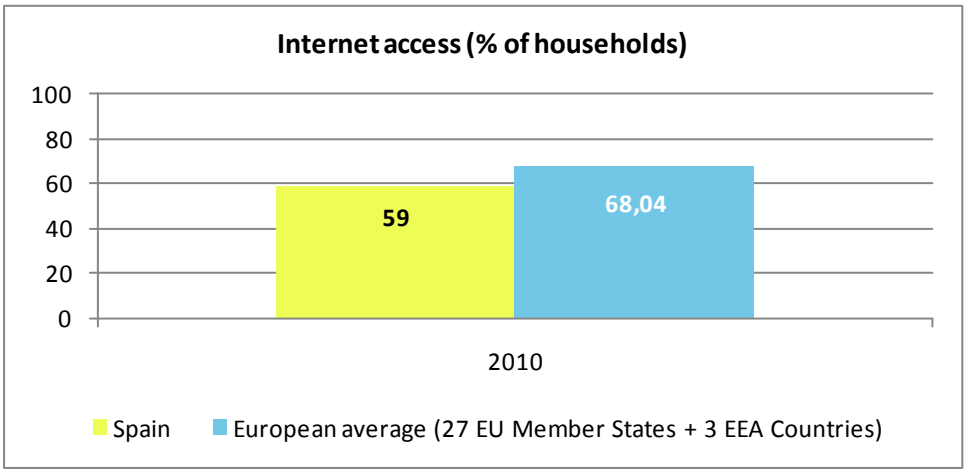
Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Spain, a series of relevant statistics are included in this section. The graphs indicate that the information society in Spain is relatively mature.

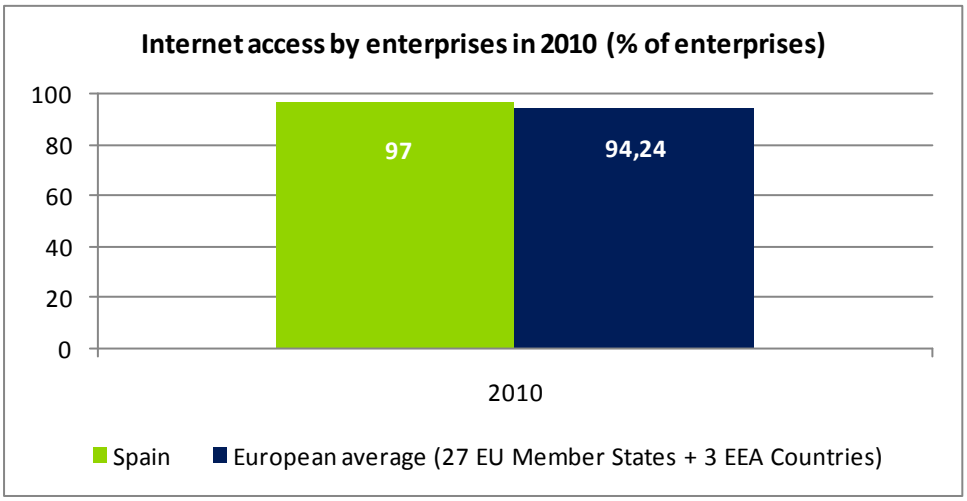
Internet access of population and enterprises

The following graphs provide an overview of the situation[48] of Internet access in Spain for enterprises and respectively households, relative to the European average.

The percentage of households with Internet access is below the European average:



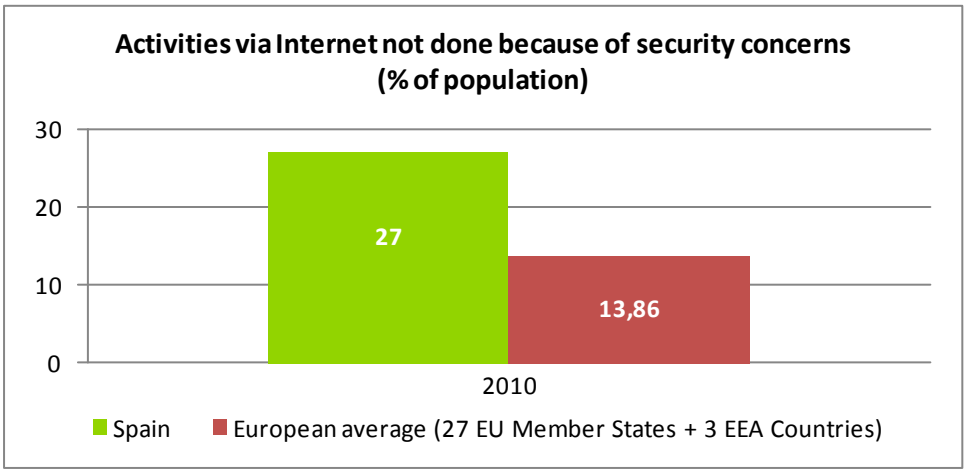
While Internet access by enterprises is above the average:



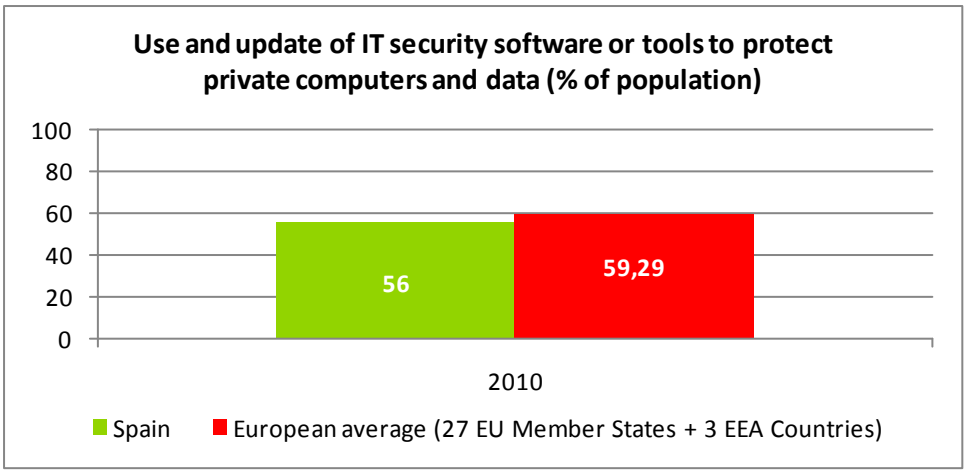
[48] *Source: Eurostat*

Statistics on use of Internet by individuals and related security aspects

The percentage of population in Spain that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is above the European average:



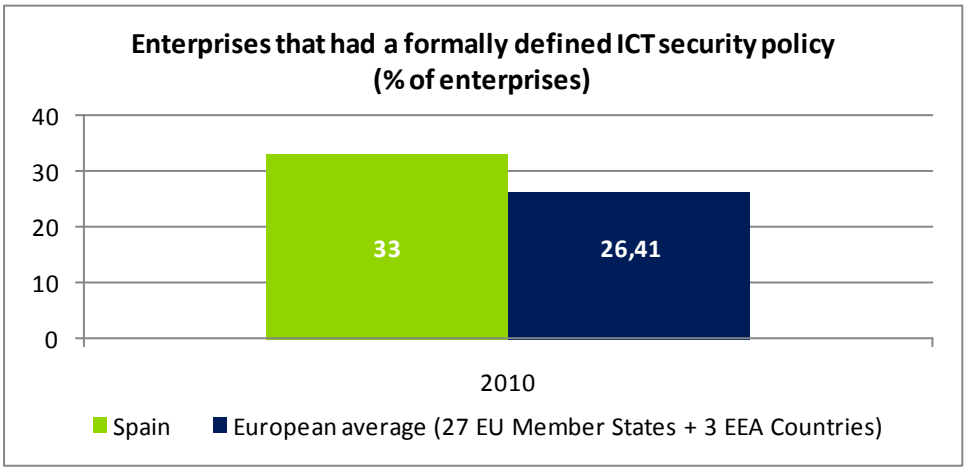
This can be an indication of either less confidence in web-based transactions or of more awareness of the general public regarding IT threats.



Meanwhile, it appears that the use of security tools to protect private computers and data is below the European average.

Statistics on use of Internet by enterprises and related security aspects

More enterprises in Spain have a formally defined ICT security policy[49], compared with their European peers. See below:



Other statistics

INTECO provides a site where local studies are published on a frequent basis: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1 .

NTECO provides statistics related with spam and malware in email in real time throough the website https://ersi.inteco.es/

[49] *Source: Eurostat*

APPENDIX

National authorities in network and information security

National authorities	Role and responsibilities	Website
1. Ministry of Industry, Tourism and Trade (MITYC)— Secretary of Telecommunications and Information Society (SETSI)	NRA for Telecommunications and Information Society (electronic communications, information society services, e-commerce, electronic signature, safer Internet). The state secretariat also provides NIS services for citizens and small & medium enterprises (SME's) run by INTECO (see 'Other bodies' section). SETSI includes "Red.es", a state-owned company. Its role is to encourage, support and monitor the use of information and communication technologies in Spain	www.mityc.es/Telecomunicaciones www.mityc.es/dgdsi www.inteco.es
2. Ministry of Interior (Home Office) — Secretary of Security (SES)	NRA for cybercrime law enforcement and critical information infrastructure protection. National Police Force and Guardia Civil: Brigada de Investigación Tecnológica Grupo de Delitos Telemáticos	www.mir.es www.mir.es/SES/ https://www.policia.es/bit/index.htm www.guardiacivil.org/seguridad
3. National Cryptologic Centre - Centro Criptológico Nacional	The National Cryptologic Centre, CCN, is the organization responsible for: Coordinating the different organizations' activities in the Public administration area using resources or encryption procedures and ensuring the security of the information technologies in all areas Keeping the different organizations informed concerning the coordinated acquisition of cryptologic material Providing training for Public Administration resources who specialise in this field. It is part of the National Intelligence Centre and reports to the Ministry of Defence.	www.ccn.cni.es
4. Ministry of Territorial Policy and Public Administration - Ministerio de Política Territorial y Administración Pública (MPTAP)	Responsible for public administrations, including their information security.	www.map.es
5. National Centre of Protection of Critical Infrastructures - Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)	The CNPIC is responsible for leading and coordinating activities concerning the protection of critical infrastructures.	www.cnpic-es.es
6. Spanish Data Protection Agency - Agencia Española de Protección de Datos	The public law entity overseeing compliance with the legal provisions on the protection of personal data. It enforces and promotes information security aspects related to data protection. It also performs awareness raising on security aspects of data processing	www.agpd.es
7. Higher Council for Electronic Administration - Consejo Superior de Aministración Electrónica (CSAE)	This Council is responsible for the development and implementation of ICT policy and strategy and e-government within the public administration.	http://administracionelectronica.gob.es
8. Certification Body (CB) of the Spanish Evaluation and Certification Scheme	The Certification Body (CB) of the Spanish Evaluation and Certification Scheme operates under the scope of the National Cryptologic Center, as laid out in the Act 11/2002, 6th May, regulating the National Intelligence Centre, and the Royal Decree 421/2004, 12th March, regulating the National Cryptologic Centre.	www.oc.ccn.cni.es/index_en.html
9. Council of Accreditation	This Council is an advisory instrument of the Certification	

National authorities	Role and responsibilities	Website
and Certification	Body integrated by representatives of the Administration, the Evaluation Laboratories and the Industry as stated in its legal basis.	
10. INTECO	INTECO's mission is to promote and develop innovation projects in the Information Society that are related to Information and Communication Technologies (ICT), which will improve the position of Spain and increase its competitiveness, expanding its capacities within the European and Latin American environment. INTECO has the following objectives: • To develop projects of applied research and innovation related to the Information Society and Information and Communication Technologies. • To promote academic proposals that add value to the position of Spain and Europe, regarding the Information Society. • To develop projects with contents linked to the intensive use of Information and Communication Technologies. • To create a new ICT Cluster in León, defined by its high capacity to innovate. To facilitate the technological transversality between different activity sectors (e.g. Administration, Police, Health, Agri-Foodstuffs, etc.) and/or areas of ICT knowledge based on a high geographical location of intensive knowledge and its connection with other centres of the world.	www.inteco.es
11. Sectoral Committee for eGovernment	Committee dedicated to the co-operation between the national government and the other government tiers, and established for this purpose (as indicated in section 4 of Law 11/2007)	No website available
12. Advisory Council on e-Government (Consejo Asesor de Administración Electrónica)	Committee created to assist in the development of an integrated strategy for e-Government	No website available

Computer Emergency Response Teams (CERTs)

CERT		Role and responsibilities • FIRST[50] member • TI[51] listed	Website
13.	CCN-CERT	CCN-CERT is the Computer Security Incident Response Team of the National Cryptologic Centre. Created in 2006. CCN-CERT is the Spanish Governmental CERT. The CCN-CERT's main objectives are as follows: • Provide centralized Security Incident Management • Coordinate the response to specific security incidents • Provide direct technical support as required • Provide references in security configurations • Force providers to give an appropriate response to detected vulnerabilities • Establish relationships with other CERTs Establish relationships with organizations responsible for criminal research. CCN-CERT is: • A full member of FIRST • TI accredited	https://www.ccn-cert.cni.es
14.	CSIRT-CV	CSIRTCV is the Centro de Seguridad TIC de la Comunidad Valenciana . CSIRT/CERT aims the prevention, detection, advising, pursuit and coordination necessary to fight against computer security incident. The incidents which they face are very diverse, from the detection of virus, worms and troyans, to the detection of activities realized by organized groups, such as terrorism or coordinated attacks to the infrastructures of Internet. CSIRT-CV is: • Not a member of FIRST • TI listed	https://www.csirtcv.es
15.	e-LC CSIRT	e-LaCaixa CSIRT is the CSIRT for the La Caixa financial institution. e-LC is: • A member of FIRST • Not TI listed	www.lacaixa.es
16.	esCERT-UPC	esCERT-UPC is the CERT for the Technical University of Catalunya.This is a private CERT, Catalonia Polytechnic University spin-off. The purpose of the esCERT is to assist members of UPC University community in responding to such incidents when and if they occur. esCERT is also committed to proactively reduce the risk of computer security providing vulnerability alters, proactive network scans, ID's deployment and related measures. esCERT-UPC is: • A member of FIRST • TI accredited	http://escert.upc.edu/index.php/web/es/index.html
17.	INTECO-CERT	INTECO-CERT is the INTECO IT Incident Response Center. Public entity belonging to the Secretary of Telecommunications and Information Society. INTECO operates an information security centre providing services for citizens and SMEs: Computer Emergency Response Team (INTECO -Cert); National Security Helpdesk for Citizens Information Security Observatory INTECO-CERT is: • A member of FIRST • TI accredited INTECO-CERT is also a member of CERT/CC.	http://cert.inteco.es www.osi.es http://observatorio.inteco.es

[50] *See : http://www.first.org/members/teams/*

[51] *See : http://www.trusted-introducer.nl/*

CERT	Role and responsibilities	Website
	• FIRST[50] member • TI[51] listed	
18. IRIS-CERT	IRIS-CERT is RedIRIS' security service, and is aimed to the early detection of security incidents affecting RedIRIS centers, as well as the coordination of incident handling with them. Proactive measures are in constant development, involving timely warning of potential problems, technical advice, training and related services. IRIS-CERT also acts as a last point of contact for incident handling coordination for emergency or high priority security matters affecting the .es domain, accepting any incident of this kind as for informational purposes and to better support our community. IRIS-CERT is: • A member of FIRST • TI accredited	www.rediris.es/cert
19. CESICAT	The Catalan Government agency in charge of executing the National Plan for IT security. CESICAT is: • A member of FIRST • TI accredited	www.cesicat.cat/
20. S21sec CERT	Managed security services provider. S21sec CERT is: • Not a member of FIRST • TI accreditation candidate	https://cert.s21sec.com

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
21. CONETIC (Spanish Electronics, Information Technology and Telecommunications Industry Association)	CONETIC wants to promote the participation of Spanish ICT companies in cooperation projects with Latin-America.	www.conetic.info
22. ISMS Forum Spain	Spanish forum for the promotion of Information Security	https://www.ismsforum.es/
23. Fundación Círculo de Tecnologías para la Defensa y la Seguridad	Initiative that encourages initiatives aimed at the creation and development of a national technology applicable to the Defence and Security, especially in the areas of electronics, computers and telecommunications.	www.fundacioncirculo.es
24. AETIC (Spanish Electronics, Information Technology and Telecommunications Industry Association)	AETIC wants to promote the development of the sector of the Electronics, Information Technologies and Telecommunications, especially with the generation of value added and industrial or service activity. In addition, AETIC wants to strengthen the development of Information Society in Spain and offering business support in the areas they represent. In October 2010, Spanish electronics and ICT associations AETIC and ASIMELEC have merged into a single body called AMETIC (Multi-Sector Association of Electronics, Information Technologies and Communication, Telecommunication and digital content).	www.aetic.es
25. ASIMELEC (Spanish Electronic and Communications Multisectorial Industry Association)	ASIMELEC encompasses all sectors of the Macro-ICT. Its purpose is to encourage and support the development of businesses in Information Technology, Communications and Electronics in Spain, by defending its partners and the development of the ICT sector. In October 2010, Spanish electronics and ICT associations AETIC and ASIMELEC have merged into a single body called AMETIC (Multi-Sector Association of Electronics, Information Technologies and Communication, Telecommunication and digital content).	www.asimelec.es
26. AMETIC	In October 2010, Spanish electronics and ICT associations	www.ametic.es

Industry Organisations	Role and responsibilities	Website
	AETIC and ASIMELEC have merged into a single body called AMETIC (Multi-Sector Association of Electronics, Information Technologies and Communication, Telecommunication and digital content).	
27. ASTEL (Competitive Telecommunications Association)	Represents telecommunications and Internet operators and services companies that have begun activities in Spain after the end of the monopoly (1996). Its fundamental activities are: • The maintenance and increase of the market's competition conditions. • The improvement of the telecommunications networks and services' legal framework.	www.astel.es
28. ANEI (National Association of Internet Enterprises)	ANEI collaborates with companies and institutions with the aim of boosting the Information Society.	www.a-nei.org
29. AECEM - FECEMD (Spanish Association for Electronic Commerce and Relational Marketing)	AECEM-FECEMD represents companies involved in activities related to electronic commerce and / or relationship marketing and acts as the opposition to governmental and legislative institutions in reference to electronic commerce and in everything affecting the relationship marketing, direct and interactive.	www.aecem.org
30. CNCCS – Consejo Nacional Consultor sobre Cyber-Seguridad (National Advisory Council for Cyber-security)	The National Advisory Council is a private initiative born in May 2009 resulting from the concern of the Spanish security industry. The Council brings together all the Spanish industry leaders in Computer Security: Panda Security, S21sec, Hispasec Systems and Secuware (amongst other). The Council has the following objectives: • Protecting consumer identity • Critical Infrastructure Protection • The creation of national legislation to combat cyber-crime • The protection of corporate information • The evolution of the government structure from the focus of the physical realm to cyberspace • The improvement and support, from the standpoint of the Council, of economic prosperity and national security	www.cnccs.es
31. eSec	Spanish Technology Platform for Security, Trust and Dependability, part of AETIC.	www.idi.aetic.es/esec/

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
32. Red Temática Iberoamericana de Criptografía y Seguridad de la Información CriptoRed (Latin American Thematic Network on Cryptography and Information Security CriptoRed)	Created in 1999, has over 800 members, professionals from 214 universities and 300 companies. Repository with some 500 documents, over a thousand hits per day and 1.0 GB served; divulges aspects of information security in Latin America, having released in 10 years more than a million and a half documents. Organizes the Iberoamerican Congress on Information Security CIBSI, biennial, since 2002.	www.criptored.upm.es
33. Cátedra UPM Applus+ de Seguridad y Desarrollo de la Sociedad de la Información (Cátedra UPM Applus + Security and Development of Information Society)	Created in 2006, organizes seminars and high-level security events. Every year, on November 30, organizes the Computer Security Day in Spain with the name of the International Day of Information Security DISI, which have attended as guests, among others, the Dr. Martin Hellman, Radia Perlman and Hugo Krwazcyk.	www.capsdesi.upm.es

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
34. Council of Consumers and Users	Consumer and user protection council.	www.consumo-ccu.es
35. Asociación de Usuarios de Internet (AUI) – Association of Internet Users	Association of individual and corporate Internet users whose goals are to influence Internet regulation and the Internet-related initiatives of the public administration.	www.aui.es
36. Asociación de Internautas – Association of "Internauts"	Association for individual Internet users whose goals are to influence Internet regulation and the Internet-related initiatves of the public administration.	www.internautas.org
37. Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI)	Spanish association for Information Society and Telecommunication users. AUTELSI aims to promote, in society in general and professional users in particular, the study, objective research and dissemination of knowledge in matters related to telecommunications services and the Information Society.	www.autelsi.es/cms
38. Protegeles	Hotline for dealing with harmful and illegal content over Internet. Awareness- raising node. Part of the European Internet safety network 'Insafe' under the 'Safer Internet' programme.	www.protegeles.com
39. Pantallasamigas	Non-profit web site for the promotion of a safe use of Internet among children and youth - also provides a hotline to report harmful content.	www.pantallasamigas.net
40. Chaval	Website for the promotion of a safe and beneficial use of the Internet targeted to parents and children, run by RED.es	www.chaval.es/
41. Defender of the e-Government users (Defensor del usuario de la administración electrónica)	The Defender is in charge of monitoring that the e-Government rights of citizens are respected. The Defender will publish an annual report gathering the complaints and suggestions received, together with proposals for actions and measures to be taken in order to ensure an adequate protection of users' rights.	No website available

References

- Plan Avanza: http://www.planavanza.es/InformacionGeneral/Executive/Paginas/ExecutiveSummary.aspx
- An overview of the eGovernment and eInclusion situation in Europe, available at http://www.epractice.eu/en/factsheets
- ENISA, Information security awareness in financial organisation, November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- Spain - ENISA CERT Directory: http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/spain

enisa
European Network and Information Security Agency

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu