CCN

Centro Criptológico Nacional

2008 2009 2010

INFORME DE ACTIVIDADES

ACTIVITY REPORT

CCN

Centro Criptológico Nacional

2008 2009 2010

INFORME DE ACTIVIDADES
ACTIVITY REPORT

Carta del Secretario de Estado Director

Letter from the Secretary of State Director

Querido lector:

Con el desarrollo y uso masivo por todos los ámbitos de la sociedad de las Tecnologías de la Información y las Comunicaciones (TIC), se ha creado un nuevo espacio, el ciberespacio, donde no hay barreras de distancia y tiempo y donde las fronteras nacionales han quedado diluidas. Este nuevo escenario ha incrementado, sin lugar a dudas, las posibilidades de progreso de la población pero también las amenazas, acrecentadas por la paulatina dependencia cibernética de las sociedades avanzadas.

La rentabilidad económica, política o de otro tipo que se obtiene; la facilidad y bajo coste en el empleo de las herramientas utilizadas, así como el bajo riesgo para el atacante, que lo puede hacer de forma anónima y desde cualquier lugar del mundo, han posibilitado esta situación. Nadie duda de que en el ciberespacio se podrían producir y se producen conflictos y agresiones, y existen ciberamenazas que pueden atentar contra la seguridad nacional, el Estado de Derecho, la prosperidad económica, el Estado del Bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), le encomienda a éste el ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información en su artículo 4.e) y de protección de la información clasificada en su artículo 4.f), a la vez que se confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2f), cuya memoria de actividades tienen ante sí.

Es precisamente a través del CCN (regulado por el RD 421/2004, de 12 de marzo, y reforzado por el RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, ENS), y partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades, como se está haciendo

Dear Reader,

With the development and massive use of the Information and Communication Technologies (ICT) a new space has emerged, the cyberspace, where there are no barriers of distance and time and where national borders have been diluted. This new scenario has increased the likelihood of progress for the population but it also increases the number of threats, due to the gradual dependence of advanced societies on the cybernetic world.

The advantages provided by the cyberspace have enabled this situation: the economic and political profitability, the ease and low cost for the tools used in cyberspace, and the low risk posed to the attacker, who can act anonymously and from anywhere in the world. In cyberspace there is also room for conflicts and aggressions, and some cyber threats could even pose a threat against national security, the rule of law, economic prosperity, the welfare state and the normal functioning of society and government.

Act 11/2002 of May 6, which regulates the National Centre of Intelligence (CNI), confers upon the CNI the functions relating to Information Technology security in its article 4.e) as well as the functions relating to the protection of classified information, according to Article 4-f), at the same time it invests the Secretary of State Director with the responsibility to lead the National Cryptologic Centre (CCN) by means of its article 9.2f), whose activity report is included in this document.

It is precisely through the CCN (regulated by RD 421/2004, March 12, and reinforced by RD 3/2010 of January 8, which regulates the National Security Framework - ENS), and on the basis of its knowledge and experience on threats and vulnerabilities, how we are facing the emerging risks orig-

inating from cyberspace. The CCN is responsible for coordinating the activities of different government agencies that use encryption methods or procedures; for ensuring ICT security in this area; for reporting on the coordinated procurement of cryptology equipment and for training the Administration staff specialised in this field.

As it can be seen from this report, the CCN has adapted its activity to new risks, promoting not only defensive but also preventive, remediation and containment measures. The CCN is mindful of the importance of adopting measures which can respond to the steady increase of security incidents and which can prevent their further spreading and stop their impact quickly and efficiently. Thus, and responding to these threats, the CCN has opted to cooperate with all governments in the implementation of the ENS, in enhancing early warning capabilities, in strengthening the management and incident response capabilities (through the CCN-CERT) and in the use of secure and certified products and systems in accordance with the most internationally renowned rules and standards (CCN itself is the Certification Body).

We are aware of the significance of the challenges that characterize today's world, of what we need to confront them and of the level of efficiency society demands of us. However, the work and effort already undertaken (the results of which are presented in this report) encourage us in our commitment and future dedication.

frente a los riesgos emergentes del ciberespacio. No en vano, el CCN es responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad TIC en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

Como podrá comprobarse en este informe, la actividad del CCN ha ido adecuándose a los nuevos riesgos, potenciando las acciones no sólo defensivas, sino primordialmente preventivas, correctivas y de contención. Sabedores de la importancia de adoptar medidas que permitan reaccionar ante el constante incremento de incidentes de seguridad y, sobre todo, que prevengan su propagación y atajen su impacto de la forma más rápida y eficaz posible. Así, y ante estas amenazas, el CCN ha apostado por colaborar con todas las administraciones en la implantación del ENS, en la potenciación de las capacidades de alerta temprana, en el fortalecimiento de la gestión y respuesta a incidentes (a través del CCN-CERT), y en la utilización de productos y sistemas seguros y certificados de acuerdo a las normas y estándares de mayor reconocimiento internacional (el propio CCN es el Organismo de Certificación).

Somos conscientes de la entidad de los desafíos que caracterizan al mundo actual, de las exigencias que implica afrontarlos y del nivel de eficacia que en esa tarea se nos demanda por parte de la sociedad. Sin embargo, el trabajo y el esfuerzo ya realizado (cuyos frutos se presentan en este informe) nos animan en nuestro compromiso y vocación de futuro.

Félix Sanz Roldán
Secretario de Estado Director del CNI
Director del CCN
Secretary of State Director of the CNI
Director of the CCN

6

CENTRO CRIPTOLÓGICO NACIONAL

ORGANISMOS Y CAPACIDADES DEL CCN
CCN ORGANIZATIONS AND CAPABILITIES

CRONOLOGÍA CCN
CCN CHRONOLOGY

6 CENTRO CRIPTOLÓGICO NACIONAL, CCN

¿QUIÉNES SOMOS?

WHO ARE WE?

El Centro Criptológico Nacional (CCN), perteneciente al Centro Nacional de Inteligencia (CNI), es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo. Así lo recoge el Real Decreto 421/2004, de 12 de marzo, que regula su funcionamiento y que señala al Director del CCN como la autoridad de certificación de la seguridad de las Tecnologías de la Información y autoridad de certificación criptológica. Asimismo, continúa el RD, es responsable de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en los aspectos de los sistemas de información y telecomunicaciones, de acuerdo a lo señalado en la Ley 11/2002, de 6 de mayo, reguladora del CNI.

También hace mención a las funciones del CCN, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. En este RD se dedica todo su Capítulo VII a la Capacidad de Respuesta a Incidentes de Seguridad del propio Centro, el CCN-CERT, y establece el papel de coordinador a nivel público estatal del CCN con el resto de capacidades de respuesta a incidentes de seguridad que se creen en el resto de administraciones públicas, a las que ofrecerá un programa de información, formación, recomendaciones y herramientas necesarias para dicho desarrollo (art. 37.2).

De igual forma, el RD 3/2010, en lo referente a la adquisición de productos de seguridad, en su artículo 18, señala que en las adquisiciones de productos que vayan a ser utilizados por las administraciones públicas se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición. Dicha certificación deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, y que será el OC/CCN quien dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados.

Por último, el RD refuerza el papel de formador y garante de la seguridad de los sistemas de la Administración del CCN al recoger, en su artículo 29, la conveniencia de utilizar Guías de Seguridad de las Tecnologías de la Información y las comunicaciones elaboradas y difundidas por el propio Centro Criptológico Nacional.

The National Cryptologic Centre, CCN, assigned to CNI (National Centre of Intelligence) is the organization responsible for: coordinating the activity of Government organizations which use encryption means or procedures; ensuring the security of the information technologies in all areas; keeping informed concerning the coordinated acquisition of the cryptologic material and it is also responsible for providing training for the Administration staff who specialise in this field. This is specified by the Spanish Royal Decree 421/2004, of March 12, which regulates its activity and appoints the CCN Director as the certification authority for Information and Communication Technologies security and as the cryptologic certification authority. Likewise, according to the RD, he is also responsible for implementing the regulation related to classified information in the field of Information and Communications Technologies (ICT), in accordance with Spanish Act 11/2002, of May 6, which regulates the CNI.

Royal Decree 3/2010, of January 8, regulates the National Security Framework in the field of eGovernment. Chapter VII of this RD describes the Incident Response Capabilities of this Centre, the CCN-CERT (which will be discussed later in this report), and it establishes the CCN's role as public-state coordinator for the rest of the incident response capabilities created in other public administrations, for which it will offer information, training, advice and whatever tools they may need for it (art.37.2).

Likewise, according to article 18 of RD 3/2010, products with the appropriate security certification will be positively valued for their acquisition by public administration. This certification should comply with international norms and standards, and the OC/CCN will determine the criteria to be followed, depending on the intended use of the product, on the evaluation level, and on other security certifications required by regulations.

Finally, the RD reinforces the trainer's role of the CCN for the security of government systems by means of its article 29 where it recommends the use of Security Guides for Information Technologies created and issued by the National Cryptologic Centre.

Esquema Nacional de Seguridad

El 29 de enero de 2010 aparecía publicado en el Boletín Oficial del Estado, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, tal y como quedaba establecido en el artículo 42 de la Ley 11/2007, de 22 de junio. El citado RD fue elaborado después de un proceso coordinado por el Ministerio de la Presidencia, actual Ministerio de Política Territorial y Administración Pública (MPT), con el apoyo del CCN, en el que participaron todas las administraciones públicas, a través de los órganos colegiados con competencia en materia de Administración Electrónica (Comisión Permanente del Consejo Superior de Administración Electrónica, Conferencia Sectorial de Administración Pública, Comisión Nacional de Administración Local) y fue sometido al previo informe de la Agencia Española de Protección de Datos. Se recibió además la opinión de numerosos expertos a través de las asociaciones profesionales del sector de la industria de Tecnologías de la Información y las comunicaciones.

La finalidad del ENS es establecer los principios básicos y los requisitos mínimos requeridos para una protección adecuada de la información. Por ello, debe ser aplicado por las administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos que gestionan.

El ámbito de aplicación del Esquema Nacional de Seguridad es el de las administraciones públicas, los ciudadanos en sus relaciones con las mismas y el de las relaciones entre ellas (tal y como se recoge en la Ley 11/2007). Están excluidos de su ámbito de aplicación los sistemas que tratan información clasificada regulada por Ley 9/1968 de 5 de abril, de Secretos Oficiales y normas de desarrollo.

La disposición transitoria del Real Decreto señala que los sistemas de las administraciones deberían haberse adecuado al Esquema en el plazo de doce meses (cumplidos el pasado 29 de enero de 2011). No obstante, esa misma disposición señala que si hubiese circunstancias que impidan la plena aplicación, se dispondrá de un plan de adecuación que marque los plazos de ejecución, en ningún caso superiores a 48 meses desde la entrada en vigor (el 29 de enero de 2014).

El CCN, y siguiendo con lo establecido en el artículo 29 de este RD, junto con el Ministerio de Política Territorial y Administración Pública, ha venido elaborando durante el año 2010 una serie de guías, englobadas en la nueva serie 800, con las que fijar un marco de referencia que ayude a todas las administraciones públicas a implantar de forma adecuada el ENS y, principalmente, facilite un mejor cumplimiento de los requisitos mínimos exigibles en el citado Esquema.

National Security Framework

Royal Decree 3/2010, of January 8, which was released on January 29, 2010, regulates the National Security Framework in the field of eGovernment, as it is established by article 42 of the Spanish Act 11/2007, of June 22. This RD was the result of a process coordinated by the Ministry of the Presideny (which currently is the Ministry of Territorial Policy and Public Administration) with the support of the National Cryptologic Centre (CCN), and in which all the public administrations participated by means of professional associations with competence in eGovernment, (Council's Standing Committee of e-Government Supreme Council, e-Government Conference, National Commission on Local Administration) and it was previously presented to the Spanish Data Protection Agency. Opinions from several experts were also taken into account by means of the professional associations of the information and communication technologies sector.

The ENS purpose is to establish the basic principles and minimum requirements for the appropriate protection of information. Therefore, it must be implemented by public administrations to ensure the access, integrity, availability, authenticity, confidentiality, accountability and storage of the information and services used in the electronic media they handle.

The National Security Framework applies to public administrations, to their interaction and to citizens who interact with them (as it is established by Act 11/2007). Systems that deal with classified information regulated by Spanish Act 9/1968 of April 5 are excluded from the scope of this regulation.

The transitory provision of the RD stated that the administration systems should comply with the Framework in twelve months (date which expired on January 29, 2011). However, the same provision establishes that if there were

circumstances that prevent full implementation, an adjustment plan could be applied to extend deadlines, which in no case will exceed 48 months from the entry into force (on January 29, 2014).

The CCN, and in accordance with the Article 29 of this Royal Decree, together with the Ministry ofTerritorial Policy and Public Administration, created a series of guides in 2010, encompassed in the new series 800, which set a framework reference that will help all public authorities to properly implement the ENS and, primarily, it will aid compliance with the minimum requirements specified in that Framework.

Centro Nacional de Inteligencia (CNI)

El Centro Criptológico Nacional está adscrito al Centro Nacional de Inteligencia (CNI) con quien comparte medios, procedimientos, normativa y recursos.

El CNI, según la Ley 11/2002, de 6 de mayo, reguladora del Centro, es el Organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de Derecho y sus instituciones.

El CNI se rige por el principio de sometimiento al ordenamiento jurídico y lleva a cabo sus actividades específicas en el marco de las facultades expresamente establecidas en la citada Ley 11/2002 y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del CNI.

National Centre of Intelligence, CNI

The National Cryptologic Centre is assigned to the National Centre of Intelligence (CNI) with which it shares means, procedures, regulations and resources.

The main mission of the CNI, in accordance with Act 11/2002, of May 6, is to provide the Prime Minister and the Government with the information, analysis, studies and proposals which allow preventing and avoiding any danger, threat or aggression against the independence or territorial integrity of Spain, the national interests and the stability of the Rule of law and its institutions.

The CNI is governed by the principle of submission to the law and carries out its activity in compliance with Act 11/2002 and Act 2/2002, of May 6, which regulates prior judicial review from National Intelligence Centre.

Funciones del Secretario de Estado-Director del CNI
Functions of Secretary of State-Director for the CNI

- **Director del Centro Criptológico Nacional** | Director of the National Cryptologic Centre
- **Autoridad Nacional de Seguridad Delegada de la Información Clasificada OTAN/UE/ Acuerdos Internacionales** | Delegated National Security Authority for Classified Information NATO/EU/international Agreements
- **Miembro de la Comisión Delegada del Gobierno para Asuntos de Inteligencia** | Member of the Government Delegate Commission for Intelligence Affairs
- **Autoridad de Inteligencia y Contrainteligencia** | Intelligence and Counterintelligence authority
- **Miembro de la Comisión Delegada del Gobierno para Situaciones de Crisis** | Member of the Government Delegate Commission for situations of crisis

Oficina Nacional de Seguridad (ONS)

La Oficina Nacional de Seguridad (ONS) se crea en 1983, dentro del servicio de inteligencia, como órgano de trabajo del Director del CNI para auxiliarle en el cumplimiento de sus cometidos relativos a la protección de la Información Clasificada. La ONS tiene por misión fundamental la de velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud deTratados o Acuerdos internacionales suscritos por España (artículo 4f de la Ley 11/2002, de 6 de mayo, Reguladora del CNI).

Funciones más destacadas:

1. Realización de Acuerdos para protección de la Información Clasificada.
2. Participación en Comités y Grupos de Trabajo.
3. Relaciones con otras Autoridades Nacionales de Seguridad.
4. Expedición de Habilitaciones Personales de Seguridad.
5. Expedición de Habilitaciones de Empresa y Establecimiento.
6. Acreditación y autorización de los Órganos, Instalaciones y Sistemas que manejan Información Clasificada.

National Security Office (ONS)

The National Security Office (ONS, Oficina Nacional de Seguridad) was created in 1983 as part of the intelligence service in order to assist the CNI Director in carrying out his duties concerning the protection of classified information. The ONS essential mission is to ensure compliance with regulations concerning the protection of classified information: national regulations and those that apply to the Administration or companies under international treaties or agreements signed by Spain (Article 4f of Spanish Act 11/2002 of May 6).

Main functions:

1. Making arrangements for the protection of classified information.
2. Participation in Committees and Working Groups.
3. Relations with other National Security Authorities.
4. Dispatching of personal security clearances.
5. Dispatching of company and establishment clearances.
6. Accreditation and approval of the bodies, facilities and systems that handle classified information.

ÁMBITO DE ACTUACIÓN Y FUNCIONES DEL CCN

10

SCOPE OF ACTION AND FUNCTIONS OF THE CCN

Tal y como recoge el Real Decreto 421/2004 por el que se regula al Centro Criptológico Nacional, su ámbito de actuación comprende:

- La seguridad de los Sistemas de las Tecnologías de la Información de la Administración que procesan, almacenan o transmiten información en formato electrónico, que según la normativa requieren protección, y que incluyen medios de cifra.
- La seguridad de los Sistemas de las Tecnologías de la Información que procesan, almacenan o transmiten información clasificada.

Dentro de dicho ámbito de actuación, el CCN realiza las siguientes funciones:

1. Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los Sistemas de las Tecnologías de la Información y las Comunicaciones (TIC) de la Administración. La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función (también recogida en el RD 3/2010, de 8 de enero, por el que se regula el ENS).
2. Formar al personal de la Administración especialista en el campo de la seguridad de los Sistemas TIC.
3. Constituir el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de Información, de aplicación a productos y sistemas en su ámbito.
4. Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las Tecnologías de la Información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.
5. Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas mencionados.
6. Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia, para evitar el acceso a ésta de individuos, grupos y Estados no autorizados, tal y como se recoge en la Ley11/2002, de 6 de mayo. Su campo de actuación son los sistemas y las Tecnologías de la Información que procesan, almace-

As it is established by Royal Decree 421/2004, the CCN's scope encompasses:

- Security of Information Technology Systems of the Administration, who process, store or transmit information on electronic support. In accordance with the regulations, these systems require protection and include means of encryption.
- Security of the Information Technology Systems which process, store or transmit classified information.

Within the said scope of action the CCN carries out the following functions:

1. Create and disseminate standards, instructions, guidelines and recommendations to ensure the security of Information and Communication Technologies (ICT) Systems within the Public Administration. The series of documents CCN-STIC was created to fulfil this function (also described in RD 3/2010, of January 8, which regulates the ENS).
2. Provide training for public Administration staff specialised in the security of Systems.
3. Create the Certification Body for the Spanish Evaluation and Certification Scheme of information technologies, which apply to products and systems in this area.
4. Asses and accredit the capability of encryption products and Information Technologies Systems, which include means of encryption, to process, store and transmit information in a secure way.
5. Coordinate the promotion, development, acquisition, operation and use of security technology of the aforementioned systems.
6. Ensure the regulations regarding the protection of classified information in their area of competence are enforced, in order to avoid access by individuals, groups and non-authorized States, as it is established under the Act 11/2002, May 6th, which regulates the National Centre of Intelligence. The scope also covers the Information Technology Systems that process, store and/or

transmit national, European Union and NATO classified information as well as international agreements. The CCN participates in this process of accreditation as a board organization for the National Authority of Delegated Security, ANS-D, in the aspects regarding the evaluation of the logical security of CIS systems, including the corresponding TEMPEST studies. Furthermore, a research on the incidents of security related to systems which manage classified information is also being carried out.

7. Establish the necessary relationships and sign the relevant agreements with similar organizations from other countries. Thus, the CCN attends the INFOSEC committees and accreditation panels to ensure the security of the Information Technologies Systems of the Administration. It also attends other forums related to ICT Security.
8. Provide a response to security incidents (article 36 of RD, 3/2010) by means of the CCN-CERT (CCN's National Computer Emergency Response Team) and coordinate this response at a national and international level, as well as its relation with the rest of incident response capabilities within public administration, to which it will offer an information and training program and the necessary tools and recommendation for doing so.
9. It will determine, through the Certification Body, the criteria to be followed for the certifications of security products that will be used by public administrations, depending on the intended use of the product, on the evaluation level, and on other security certifications required by regulations as well as, exceptionally, in cases where there are no certified products (article 18 of RD, 3/2010).

nan o transmiten información clasificada Nacional, OTAN, UE y de acuerdos internacionales. El CCN participa en dicho proceso de acreditación como órgano de trabajo de la Autoridad Nacional de Seguridad Delegada, ANS-D, en los aspectos relativos a evaluar la seguridad lógica de los sistemas TIC, incluyendo los estudios TEMPEST pertinentes. Además, se realiza la investigación de los incidentes de seguridad relacionados con sistemas que manejan información clasificada.

7. Establecer las relaciones necesarias y firmar los acuerdos pertinentes con organizaciones similares de otros países. El CCN asiste como responsable de garantizar la seguridad de las Tecnologías de la Información en la Administración a los comités y paneles de acreditación INFOSEC y a otros foros que se constituyen en materia de seguridad TIC.
8. Articular la respuesta a los incidentes de seguridad (artículo 36 del RD, 3/2010) en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Response Team) y coordinar a nivel nacional e internacional esta respuesta, así como la relación con el resto de capacidades de respuesta a incidentes de seguridad que se creen en el resto de administraciones públicas, a las que ofrecerá un programa de información, formación, recomendaciones y herramientas necesarias para dicho desarrollo.
9. En la certificación de productos de seguridad de las Tecnologías de la Información y comunicaciones que vayan a ser utilizados por las administraciones públicas, a través de OC, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados (artículo 18 del RD, 3/2010).

Ámbito de actuación del CCN
Scope of action of the CCN

IV Jornada STIC-CCN-CERT. inaugurada por el Secretario de Estado Director del CNI | 4th conference STIC CCN-CERT, opened by the CNI's Secretary of State Director

Formación

Tal y como dicta el RD 421/2004, el CCN tiene la responsabilidad de formar al personal de la Administración especialista en el campo de la seguridad de las Tecnologías de la Información.

Esta tarea se realiza a través de diferentes actividades, entre las que destacan los cursos STIC (presenciales, a distancia y *on-line*), jornadas de sensibilización, participación en ponencias y mesas redondas, etc. Dicha actividad se ha visto reforzada de manera notable durante estos tres últimos años. En este período de tiempo se han ofertado un total de 3.800 horas lectivas repartidas en 52 cursos presenciales (17 cursos STIC anuales, actualizados año tras año), a los que han acudido 1.330 alumnos procedentes de las diferentes administraciones (general, autonómica y local). Además, se han organizado nueve jornadas de sensibilización, entre las que destaca la Jornada STIC CCN-CERT, cuya cuarta edición se celebró el 14 de diciembre de 2010. Esta Jornada, que reúne a los principales expertos en materia de seguridad de la información, brinda al personal de la Administración una información muy valiosa y actualizada con la que afrontar las amenazas que se ciernen sobre sus sistemas, compartiendo el conocimiento y los recursos disponibles con el CCN-CERT.

Training

As it is established by RD 421/2004, the CCN has the responsibility to train the staff of the Administration specialized in the field of security of Information Technologies.

Training is performed through different activities, the most relevant of which are STIC courses (distance learning, online and face-to-face courses), awareness conferences, participation in conferences, roundtables, etc. This activity has been remarkably reinforced during the past three years. During this time, the CCN has offered 3.800 hours of lessons distributed in 52 face-to-face courses (17 annual STIC courses, updated every year). A total of 1.330 individuals from different administrations (general, regional and local) attended to these courses. Besides, the CCN has organized nine awareness conferences, of which the STIC CCN-CERT conference is a notable example (the fourth conference was celebrated on December 14, 2010). This conference offers valuable information for the Administration staff to confront threats that may affect their systems.

Evolución de la oferta formativa del CCN
Evolution of training offer of the CCN

	2008	2009	2010	Total
Alumnos Students	380	450	500	1.330
Cursos Presenciales Face-to-face courses	17	18	17	52
Horas Lectivas Cursos Presenciales Hours of training (face-to-face courses)	1.200	1.400	1.200	3.800
Jornadas de Sensibilización Awareness conferences	2	4	3	9
Participación en Jornadas / Mesas redondas Participation in conferences/roundtables	8	10	15	33

CURSOS STIC

Entre de los cursos presenciales ofertados por el CCN, existen cuatro modalidades: informativos y de concienciación, básicos, específicos y de especialización. Estos cursos, desarrollados en colaboración con el Instituto Nacional de la Administración Pública (INAP), son ampliados y/o actualizados anualmente. De este modo, en el año 2010, se impartieron los siguientes:

A. Cursos Informativos y de Concienciación de Seguridad (bianuales)
   - VII Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)

B. Cursos Básicos de Seguridad
   - V Curso Básico STIC – Entornos Windows
   - V Curso Básico STIC – Entornos Linux
   - V Curso Básico STIC – Base de Datos
   - V Curso Básico STIC – Infraestructura de Red

C. Cursos Específicos de Gestión de Seguridad
   - III Curso STIC – Common Criteria
   - VII Curso de Gestión STIC. Aplicación al ENS
   - XXII Curso de Especialidades Criptográficas (CEC)

D. Cursos de Especialización en Seguridad
   - VII Curso Acreditación STIC – Entornos Windows
   - V Curso STIC – Redes Inalámbricas
   - VI Curso STIC – Cortafuegos
   - VI Curso STIC – Detección de Intrusos
   - III Curso STIC – Búsqueda de Evidencias y Control de Integridad
   - V Curso STIC – Inspecciones de Seguridad
   - I Curso STIC – Seguridad en Aplicaciones Web (nuevo en 2010)
   - I Curso STIC – Herramienta PILAR (nuevo en 2010)

STIC COURSES

Face-to-face courses offered by the CCN are distributed in four different categories: informative and awareness courses; basic, specific and specialized. These courses, developed in collaboration with the Instituto Nacional de la Administración Pública (INAP), are annually extended and/or updated. In 2010, the following courses were offered:

A. Security Information and Awareness Courses (biannual)
   - VII Security Information and Communication Technologies Course (STIC)

B. Basic security courses
   - Basic STIC Course- Windows Environments
   - V Basic STIC Course- Linux Environments
   - V Basic STIC Course- Databases
   - V Basic STIC Course- Network Infrastructure

C. Specific Courses on Security Management
   - III STIC Course – Common Criteria
   - VII STIC Management Course. Application to ENS
   - XXII Cryptology Specialized Course (CEC)

D. Courses Specializing on Security
   - VII STIC Accreditation Course- Windows Environment
   - V STIC Course- Wireless Network
   - VI STIC Course – Firewall
   - VI STIC Course- Intrusion Detection
   - III STIC Course –Search for Evidence and Integrity Control
   - V STIC Course – Security Inspections
   - I STIC Course – Security in Web Applications (new in 2010)
   - I STIC Course – PILAR Tool (new in 2010)

Se han ofertado un total de 3.800 horas lectivas, repartidas en 52 cursos presenciales, a los que han acudido 1.330 alumnos procedentes de las diferentes administraciones públicas (general, autonómica y local). The CCN has offered 3.800 hours of lessons distributed in 52 face-to-face courses, to which 1.330 individuals from different administrations (general, regional and local) attended.

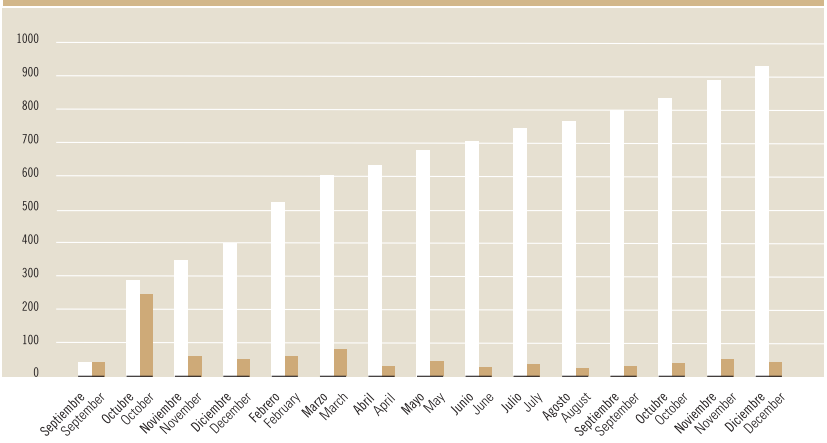
FORMACIÓN *ON-LINE*

En el año 2009, el CCN quiso facilitar al personal de la Administración una nueva forma de aprendizaje y desarrolló un método de *e-learning*. De este modo, y a través del portal del CCN-CERT, se ofrece el Curso Informativo y de Concienciación: *Seguridad de las Tecnologías de la Información y las Comunicaciones*) en el que se ofrece una visión global de la Seguridad TIC y cuyo contenido está basado en la Guía CCN-STIC 400.

Orientaciones de seguridad, gestión de incidentes, política de seguridad, acreditación de sistemas, organización y gestión de seguridad, *software* dañino, protocolos de red, seguridad en redes inalámbricas o herramientas de seguridad perimetral, son algunos de los catorce temas que aborda este curso.

En apenas un año de funcionamiento, el curso cuenta ya con 891 alumnos matriculados y ha tenido un total de 5.430 accesos.

Alumnos registrados en el curso *on-line* a través del portal CCN-CERT
Students registered in the on-line course



Número de usuarios inscritos en el curso *on-line*
Number of users registered in the on-line course
Número de nuevos usuarios inscritos en el curso *on-line*
Number of new users registered in the on-line course

ON-LINE TRAINING

In 2009, the CCN started to offer a new e-learning method. Therefore, and through the CCN-CERT portal, the CCN offers the Security Information and Awareness course: Security of Information and Communications Technologies course, which provides an overview of ICT security. Its content is based on the Guide CCN-STIC 400.

Security guidelines, incident management, security policy, accreditation of systems, organization and management of security, malware, network protocols, wireless security, security tools and perimeter security are some of the fourteen topics addressed in this course.

In just one year, 891 students have already enrolled in the course and it has had a total of 5.430 accesses.

OTROS CURSOS *ON-LINE*

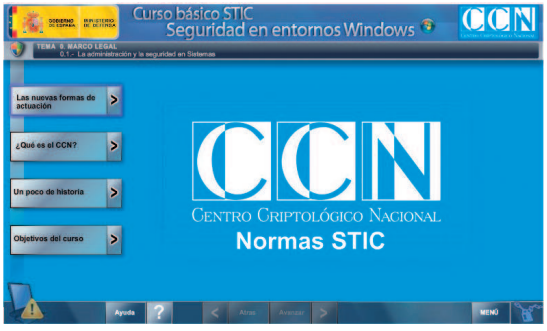
Dado el éxito del anterior curso, el CCN va a ampliar su oferta formativa *on-line* con la incorporación de cuatro nuevos temarios: Seguridad en Entornos Windows, Seguridad en Entornos Linux, Herramienta PILAR de análisis de riesgos y un curso sobre el Esquema Nacional de Seguridad.

Con esta ampliación de su oferta educativa, el CCN-CERT continúa con el compromiso de formar al personal de la Administración Pública y avanza en su propósito de mejorar la concienciación y preparación de los responsables TIC en esta materia.

OTHER ON-LINE COURSES

Given the success of the previous course, the CCN will expand its on-line training offer by adding four new subjects: Security in Windows Environments, Security in Linux Environments, Security Risk Analysis Tool PILAR and a course on National Security Framework.

With the expansion of its educational offer, the CCN-CERT shows its commitment to train the public administration staff and it improves awareness and preparedness of those responsible for ICT in this area.



Guías CCN-STIC

Una de las funciones más destacables que el Real Decreto 421/2004 asigna al CCN, es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las Tecnologías de la Información y las comunicaciones de la Administración. Precisamente, estas Guías CCN-STIC inspiraron el contenido del RD 3/2010, del ENS, y a su vez se recogen en su artículo 29 en donde se establece la elaboración y difusión, por parte del CCN, de las correspondientes guías de seguridad de las Tecnologías de la Información y las comunicaciones para el mejor cumplimiento de lo establecido en el Esquema.

Estos documentos se dividen en nueve series que son ampliadas y actualizadas anualmente, de tal forma que, en la actualidad, el CCN cuenta con 153 guías (a las que hay que sumar 21 que están pendientes de publicar). De hecho, desde 2007 se han creado 65 nuevas Guías CCN-STIC de las cuales 37 se publicaron en 2010. De ellas, la serie 800 es de nueva instauración, ya que se creó para cumplir con lo establecido en el Esquema Nacional de Seguridad, según el Real Decreto 3/2010 anteriormente mencionado.

- Serie CCN-STIC-000. Políticas: conjunto de normas que desarrolla el RD 421/2004.
- Serie CCN-STIC-100. Procedimientos STIC: marco común de actuación en los procesos de acreditación, certificación TEMPEST, gestión de material de cifra y de cualquier otro campo que se considere.
- Serie CCN-STIC-200. Normas STIC: reglas generales que deben seguirse, o a las que se deben ajustar las conductas, tareas o actividades de las personas y organizaciones, en relación con la protección de la información cuando es manejada por un Sistema.
- Serie CCN-STIC-300. Instrucciones Técnicas STIC: objetivo de seguridad específico, estableciendo los requisitos de seguridad generales a implantar en un Sistema y sus interconexiones asociadas.
- Serie CCN-STIC-400. Guías Generales: recomendaciones para los responsables de seguridad relativas a aspectos concretos de la seguridad de las TIC (seguridad perimetral, redes inalámbricas, telefonía móvil, herramientas de seguridad, etc.).
- Serie CCN-STIC-500. Guías Entornos Windows: normas desarrolladas para entornos basados en el sistema operativo Windows de Microsoft.

CCN-STIC Guides

One of the most remarkable functions assigned by the Spanish Royal Decree 421/2004 of March 12 to the National Cryptologic Centre is the creation and diffusion of standards, instructions, guides and recommendations to ensure the security of Information and Communication Technologies systems for the Public Administration. Indeed, these CCN-STIC guides inspired the contents of RD 3/2010 and the ENS. In turn, they are reflected in its Article 29 which establishes the development and dissemination, by the CCN, of the relevant security guidelines on information and communication technologies to better comply with the provisions in the Scheme.

These documents are divided into nine series which are expanded and updated annually. Up to date, the CCN has created 153 guides (plus 21 guides which are still to be published). In fact, since 2007, it has created 65 new CCN-STIC guides, 37 of which were published in 2010. The 800 series is a new series which it was created to meet the provisions of the National Security Framework, according to Royal Decree 3/2010.

- Series CCN-STIC-000. Policies: Set of standards that set forth in RD 421/2004.
- Series CCN-STIC-100. STIC procedures: Common framework of performance in the process of accreditation, TEMPEST certification, and of encryption material management and of any other relevant area.
- Series CCN-STIC-200. STIC Standards: General rules that must be adhered to, and for which people's attitudes, jobs or activities and organizations must adapt to in terms of information protection as it is managed by a System.
- Series CCN-STIC-300. STIC Technical Instructions: These norms are created in accordance with a specific security objective, and will mainly be technical. They will establish the general security requirements to be implemented in a System.
- Series CCN-STIC-400. General Guides: These are recommendations for those people in charge of security with specific ICT security (wireless networks, mobile telephone system, firewalls, security tools...).
- Series CCN-STIC-500: Windows Environments Guidelines. These guides will establish the minimum security configurations for Windows-based technology elements.

- Serie CCN-STIC-600. Guías otros entornos: configuraciones mínimas de seguridad de otras tecnologías como HP-UX, SUN SOLARIS, LINUX, Equipos de Comunicaciones, etc.
- Serie CCN-STIC-800. Esquema Nacional de Seguridad: establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS (RD 3/2010). Esta nueva serie, creada en el año 2010, es de acceso público.
- Serie CCN-STIC-900. Informes Técnicos: recogen el resultado y las conclusiones de un estudio o evaluación teniendo por objeto facilitar el empleo de algún producto o aplicación de seguridad.

Las series 000-100-200-300 son de obligado cumplimiento para los sistemas que manejan información clasificada nacional o internacional.

- Series CCN-STIC-600. Guidelines for other OS: These guides will establish the minimum security configurations for other technologies (HP-UX, SUN-SOLARIS, LINUX, communication equipment...)
- Series CCN-STIC-800. National Security Framework: It establishes the appropriate policies and procedures for the implementations of the measures specified in the ENS (RD 3/2010). This new series was created in 2010 and is publicly accessible.
- Series CCN-STIC-900. Technical Reports: These guides are of a technical nature and include the results and conclusions of a study and evaluation in order to facilitate the use of products and security applications.

The 000-100-200-300 series are compulsory for systems that deal with national or international classified information.

Top 10 guías descargadas del portal CCN-CERT en 2010
Top 10 downloads guides of the portal CCN-CERT, 2010

Guía | Guide		Nº descargas | No. downloads
001	Seguridad de las TIC en la Administración ICT Security in the Public Administration	1.558
801	Responsabilidades en el ENS Responsibilities in the ENS	524
804	Medidas de implantación del ENS Implementation Measures in the ENS	521
806	Plan de adecuación ENS Security Policy in the ENS	395
470B	Manual de usuario PILAR 4.3 Risk Analysis Tool Manual PILAR 4.3	379
002	Coordinación Criptológica Cryptology Coordination	272
402	Organización y gestión STIC ICT Security Organization and Management	252
201	Estructura de seguridad Security Organization	220
472	Manual de usuario PILAR BASIC 4.4 Risk Analysis Tool Manual PILAR BASIC v.4.4	216
400	Manual STIC ICT Security Manual	183
	Total	**4.520**

Existen 174 Guías CCN-STIC (21 de ellas pendientes de publicar), divididas en nueve series, una de las cuales, la serie 800 es de nueva instauración, creada para cumplir con lo establecido en el ENS. There are 174 CCN-STIC guides (21 of them still to be published), divided in nine series, one of which, the 800 series was created recently to fulfil the requirements established by the ENS.

Listado de Guías CCN-STIC 2010

List of CCN-STIC Guides 2010

Serie 000: Políticas
| Serie 000: Policies

001 Seguridad de las TIC en la Administración
ICT Security in the Public Administration
002 Coordinación Criptológica
Cryptology Coordination*
003 Uso de Cifradores Certificados
Use of Certified Cipher Equipment
004 Seguridad de Emanaciones (TEMPEST)
Emanation Security (TEMPEST)*

Serie 100: Procedimientos
| Serie 100: Procedures

101 Procedimiento de Acreditación Nacional
| National Accreditation Procedure
103 Catálogo de Productos Certificados
Certified Products Catalogue*
150 Evaluación y Clasificación TEMPEST de Cifradores con Certificación Criptológica
TEMPEST Evaluation and Classification of Equipment with Cryptology Certification
151 Evaluación y Clasificación TEMPEST de Equipos | TEMPEST Evaluation and Classification of Equipment
152 Evaluación y Clasificación ZONING de Locales | Facility ZONING, Evaluation and Classification
153 Evaluación y Clasificación de Armarios Apantallados | Evaluation and Classification of Shielded Cabinets*
154 Medidas de Protección TEMPEST para Instalaciones | Protection TEMPEST Measures for Facilities*

Serie 200: Normas
| Serie 200: Standards

201 Estructura de Seguridad
Security Organization*
202 Estructura y Contenido DRS
SSRS. Structure and Content
203 Estructura y Contenido POS
SecOps. Structure and Content
204 CO-DRES-POS Pequeñas Redes
Concept of Operation, SSRS and SecOps for Little Networks*
205 Actividades Seguridad Ciclo Vida CIS
Security Life Cycle Activities (CIS)
207 Estructura y Contenido del Concepto de Operación | Concept of Operation. Structure and Content

Serie 300: Instrucciones Técnicas
| Serie 300: Technical Instructions

301 Requisitos STIC
IT Security Requirements
302 Interconexión de CIS
CIS Systems Interconnection*
303 Inspección STIC
IT Security Inspection*
304 Baja y Destrucción de Material Criptológico | Destructing and Taking Cryptology material out of Circulation
307 Seguridad en Sistemas Multifunción
Security in Multifunction Systems*

Serie 400: Guías Generales
| Serie 400: General Guides

400 Manual STIC | ICT Security Manual
401 Glosario / Abreviaturas
Glossary / Abbreviations*
402 Organización y Gestión STIC
ICT Security Organization and Management
403 Gestión de Incidentes de Seguridad
Security Incidents Management
404 Control de Soportes Informáticos
Computing Devices Control
405 Algoritmos y Parámetros de Firma Electrónica | Electronic Signature: Algorithms and Parameters
406 Seguridad en Redes Inalámbricas
Wireless Security
407 Seguridad en Telefonía Móvil
Mobile Phone Security
408 Seguridad Perimetral – Cortafuegos
Perimeter Security – Firewalls*
409 Colocación de Etiquetas de Seguridad
Security Labels*
410 Análisis de Riesgos en Sistemas de la Administración | Risk Analysis in the Administration
411 Modelo de Plan de Verificación STIC
Plan Model of ICT Security verification*
412 Requisitos de Seguridad en Entornos y Aplicaciones Web | Security Requirements for Environments and Web Applications*
414 Seguridad en Voz sobre IP
VoIP Security*
415 Identificación y Autenticación Electrónica | Electronic Identification and Authentication
416 Seguridad en VPN,s | VPN Security
417 Seguridad en PABX | PABX Security*
418 Seguridad en Bluetooth
Bluetooth Security*
419 Configuración Segura con IPtables
Secure Configuration with IPtables
430 Herramientas de Seguridad
Security Tools*
431 Herramientas de Análisis de Vulnerabilidades | Tools for Vulnerabilities Assessment
432 Seguridad Perimetral – IDS
Perimeter Security – Intrusion Detection Systems*

* Guías elaboradas o actualizadas en el período 2008-2010 | Guides created or updated during 2008-2010

434 Herramientas para el Análisis de Ficheros de Logs | Tools for Log Files Analysis*
435 Herramientas de Monitorización de Tráfico Tools for Data Flow Monitoring
436 Herramientas de Análisis de Contraseñas Password Analysis Tools
437 Herramientas de Cifrado Software Encrypted Software Tools
438 Esteganografía | Steganographia
440 Mensajería Instantánea Instant Messaging
441 Configuración Segura de VMWare Secure Configuration of VMWare*
443 RFID | RFID*
444 Seguridad en WiMAX | WiMax Security*
445A Curso de Especialidades Criptológicas (correspondencia) – Probabilidad Cryptology Specialised Course (CEC) – Probability*
445B Curso de Especialidades Criptológicas (correspondencia) – Principios digitales CSC- Digital Principles*
445C Curso de Especialidades Criptológicas (correspondencia) – Teoría de números CEC – Numbers Theory*
450 Seguridad en Dispositivos Móviles Security on Mobile Devices*
451 Seguridad en Windows Mobile 6.1 Security on Windows Mobile 6.1*
452 Seguridad en Windows Mobile 6.5 Security on Windows Mobile 6.5*
470A Manual de la Herramienta de Análisis de Riesgos PILAR 4.1 | Risk Analysis Tool Manual PILAR 4.1
470B Manual de la Herramienta de Análisis de Riesgos PILAR 4.3 | Risk Analysis Tool Manual PILAR 4.3*
470C Manual de la Herramienta de Análisis de Riesgos PILAR 4.4 | Risk Analysis Tool Manual PILAR 4.4*
470D Manual de la Herramienta de Análisis de Riesgos PILAR 5.1 | Risk Analysis Tool Manual PILAR 5.1*
471B Manual de Usuario de RMAT 4.3 Handbook for RMAT 4.3*
472A Manual de la Herramienta de Análisis de Riesgos PILAR BASIC 4.3 | Risk Analysis Tool Manual PILAR BASIC v.4.3*
472B Manual de la Herramienta de Análisis de Riesgos PILAR BASIC 4.4 | Risk Analysis Tool Manual PILAR BASIC v.4.4*
473A Manual de la Herramienta de Análisis de Riesgos μPILAR | Risk Analysis Tool Manual (μPILAR)*
480 Seguridad en Sistemas SCADA Security on SCADA systems*
480A Seguridad en Sistemas SCADA – Guía de Buenas Prácticas | SCADA- Best Practices*
480B Seguridad en Sistemas SCADA – Comprender el Riesgo del Negocio | SCADA- Understanding Business Risks*
480C Seguridad en Sistemas SCADA – Implementar una Arquitectura Segura SCADA- Implementing Secure Architecture*
480D Seguridad en Sistemas SCADA – Establecer Capacidades de Respuesta SCADA- Establishing Response Capabilities*
480E Seguridad en Sistemas SCADA – Mejorar la Concienciación y las Habilidades SCADA- Improving Awareness and Capabilities*
480F Seguridad en Sistemas SCADA – Gestionar el Riesgo de Terceros SCADA- Dealing with Risks Derived from Third Parties*
480G Seguridad en Sistemas SCADA – Afrontar Proyectos | SCADA- Confront Projects*
480H Seguridad en Sistemas SCADA – Establecer una Dirección Permanente SCADA – Establishing a Permanent Address*
490 Dispositivos Biométricos de Huella Dactilar | Biometric Fingerprints Devices
491 Dispositivos Biométricos de Iris Iris Biometric Devices*
492 Evaluación de Parámetros de Rendimiento en Dispositivos Biométricos | Evaluation of Performance Parameters in Biometric Devices*

Serie 500: Guías de entornos Windows
| Serie 500: Windows Environments Guides

501A Seguridad en Windows XP SP2 (cliente en dominio) | Windows XP SP2 Security (client within a domain)
501B Seguridad en Windows XP SP2 (cliente independiente) | Windows XP SP2 Security (independent client)
502 Seguridad en Aplicaciones Cliente. Navegador y Correo Electrónico Client Windows Security: Browser and E-mail*
502B Seguridad en Aplicaciones Cliente Windows Vista. Navegador y Correo Electrónico | Client Windows Vista Security. Browser and E-mail*
503A Seguridad en Windows 2003 Server (controlador de dominio) | Windows 2003 Server Security (domain controller)
503B Seguridad en Windows 2003 Server (servidor independiente) | Windows 2003 Server Security (independent server)
504 Seguridad en Internet Information Server Internet Information Server Security
505 Seguridad en Bases de Datos SQL 2000 BD SQL Security
506 Seguridad en Microsoft Exchange Server 2003 | MS EXCHANGE Server 2003 Security
507 Seguridad en ISA Server | ISA Server Security
508 Seguridad en Clientes Windows 2000 Windows 2000 Clients Security

509 Seguridad en Windows 2003 Server. Servidor de Ficheros | Security on Windows 2003 Server. File Server

510 Seguridad en Windows 2003 Server. Servidor de Impresión | Security on Windows 2003 Server. Printing Server*

512 Gestión de Actualizaciones de Seguridad en Sistemas Windows | Windows Security Updates Management

517A Seguridad en Windows Vista (cliente en dominio) | Windows Vista Security (client within a domain)*

517B Seguridad en Windows Vista (cliente independiente) | Windows Vista Security (independent client)*

519A Configuración Segura del Internet Explorer 7 y Outlook en Windows XP Secure Configuration of Internet Explorer 7 and Outlook in Windows XP*

521A Seguridad en Windows 2008 Server (controlador de dominio) | Windows 2008 Server Security (domain controller)*

521B Seguridad en Windows 2008 Server (servidor independiente) | Windows 2008 Server Security (independent server)*

521C Seguridad en Windows 2008 Server Core (controlador de dominio) | Windows 2008 Server Core Security (domain controller)

521D Seguridad en Windows 2008 Server Core (servidor independiente) | Windows 2008 Server Core Security (independent server)

522A Seguridad en Windows 7 (cliente en dominio) | Windows 7 Security (domain client)

522B Seguridad en Windows 7 (cliente independiente) | Windows 7 Security (independent client)*

Serie 600: Guías de otros entornos | Serie 600: Guidelines for other OS and Equipment Security

601 Seguridad en HP-UX v 10.20 HP-UX v 10.20 Security

602 Seguridad en HP-UX 11i HP-UX 11i Security

603 Seguridad en AIX-5L | AIX-5L Security*

610 Seguridad en Red Hat Linux 7 Red Hat Linux 7 Security

611 Seguridad en Suse Linux SUSE Linux Security

612 Seguridad en Debian | Debian Security

613 Seguridad en Entornos basados en Debian Security on Debian-based Environments

614 Seguridad en Red Hat Linux (Fedora) Red Hat Linux (Fedora) Security

615 Seguridad en Entornos basados en Redhat Security on Redhat-based Environments

621 Seguridad en Sun Solaris 8.0 Sun-Solaris 8.0 Security

622 Seguridad en Sun Solaris 9.0 para Oracle 8.1.7 | Sun-Solaris 9.0 Security for Oracle 8.1.7

623 Seguridad en Sun Solaris 9.0 para Oracle 9.1 | Sun-Solaris 9.0 Security for Oracle 9.i

624 Seguridad en Sun Solaris 9.0 para Oracle 9.2 | Sun-Solaris 10 Security for Oracle 9.2

625 Seguridad en Sun Solaris 10 para Oracle 10g | Sun-Solaris 10 Security for Oracle 10g*

626 Guía de Securización de Sun Solaris 10 con NFS | Security Guide for Sun Solaris 10 with NFS

627 Guía de Securización de Sun Solaris 9 con Workstation | Security Guide for Sun Solaris 9 with Workstation

628 Guía de Securización de Sun Solaris 9 con NFS | Security Guide for Sun Solaris 9 with NFS

629 Guía de Securización de Sun Solaris 10 con Workstation | Security Guide for Sun Solaris 10 with Workstation

631 Seguridad en Base de Datos Oracle 8.1.7 sobre Solaris | Security for DB Oracle 8.1.7 on Solaris

633 Seguridad en Base de Datos Oracle 9i sobre Red Hat 3 y 4 | Security for DB Oracle 9i on Red Hat 3 y 4

634 Seguridad en Base de Datos Oracle 9i sobre Solaris 9 y 10 | Security for DB Oracle 9i on Solaris 9 y 10

635 Seguridad en Base de Datos Oracle 9i sobre HP-UX 11i | Security for DB Oracle 9i on HP-UX 11i

636 Seguridad en Base de Datos Oracle 10gR2 sobre Red Hat 3 y 4 | Security for DB Oracle 10gR2 on Red Hat 3 y 4

637 Seguridad en Base de Datos Oracle 10gR2 sobre Solaris 9 y 10 | Security for DB Oracle 10gR2 on Solaris 9 y 10

638 Seguridad en Base de Datos Oracle 10gR2 sobre HP-UX 11i | Security for DB Oracle 10gR2 on HP-UX 11i

639 Seguridad en Base de Datos Oracle 10g sobre Windows 2003 Server | Security for DB Oracle 10g on Windows 2003 Server*

641 Seguridad en Equipos de Comunicaciones. Routers Cisco | Security for Communication Equipment. Routers Cisco

642 Seguridad en Equipos de Comunicaciones. Switches Enterasys | Security for Communication Equipment. Switches Enterasys

644 Seguridad en Equipos de Comunicaciones. Switches Cisco | Security for Communication Equipment. Switches Cisco

645 Sistemas de Gestión de Red (Cisco Works LMS) | Network Management systems (Cisco Works LMS)*

655 Guía de Securización para Sun Solaris 9 con Oracle 10 | Security Guide for Sun Solaris 9 with Oracle 10

656 Guía de Securización para Sun Solaris 9 con Oracle 10 y VCS 4.1 | Security Guide for Sun Solaris 9 with Oracle 10 and VCS 4.1
660 Seguridad en Proxies | Proxies Security*
661 Seguridad en Firewalls de Aplicación Application Firewalls Security*
671 Seguridad en Servidores Web Apache Security of Web Apache Server
672 Seguridad en Servidores Web Tomcat Security of Web Tomcat Server*
681 Seguridad en Servidores de Correo Postfix | Security of Postfix Email Server
682 Configuración Segura de Sendmail Secure Configuration for Sendmail*
691 Guía de Securización de Oracle Application Server 10gR2 para Red Hat 3 y 4 | Security in Oracle Application Server 10gR2 for Red Hat 3 y 4
692 Guía de Securización de Oracle Application Server 10gR2 para Solaris 9 y 10 | Security in Oracle Application Server 10gR2 for Solaris 9 y 10
693 Guía de Securización de Oracle Application Server 10gR2 para HP-UX 11i Security in Oracle Application Server 10gR2 for HP-UX 11i

Serie 800: Esquema Nacional de Seguridad | Serie 800: National Security Framework

800 Glosario de Términos y Abreviaturas (borrador) | Glossary of Terms and Abbreviations*
801 Responsabilidades en el ENS Responsibilities in the National Security Framework*
802 Auditoría del Esquema Nacional de Seguridad | Audit for the National Security Framework*
803 Categorización de los Sistemas en el ENS Systems Evaluation in the National Security Framework*
804 Implementación de Medias en el ENS (borrador) | Implementation Measures in the National Security Framework*
805 Modelo de Política de Seguridad Security Policy in the National Security Framework*
806 Modelo de Plan de Adecuación al ENS Adaptation Plan in the National Security Framework*
807 Criptología de Empleo en el ENS (borrador) | Encryption in the National Security Framework*
808 Verificación del Cumplimiento de las Medidas en el ENS (borrador) | Verification of Compliance with Measures Established by the National Security Framework*
809 Declaración de Conformidad con el ENS | Statement of Conformity in the National Security Framework*
810 Guía de Creación de CERTs | Guide for the Creation of CERTs*

Serie 900: Informes técnicos | Serie 900: Technical Reports

903 Configuración Segura de HP-IPAQ HP-IPAQ Secure Configuration
951 Recomendaciones de Empleo de la Herramienta Ethereal/Wireshark Recommendations for Using Ethereal/Wireshark Tool
952 Recomendaciones de Empleo de la Herramienta Nessus | Usage Recommendations for Nessus Tool
953 Recomendaciones de Empleo de la Herramienta Snort | Usage Recommendations for Snort Tool*
954 Recomendaciones de Empleo de la Herramienta Nmap | Usage Recommendations for Nmap Tool
955 Recomendaciones de Empleo de GnuPG | Usage Recommendations for GnuPG Tool
956 Entornos Virtuales | Virtual Environments
970 Interconexión de Sistemas Mediante Cifradores IP. Redes Públicas | Use of IP Cyphers in Public Networks*

Herramienta PILAR de Análisis de Riesgos

Evaluar el estado de seguridad de un Sistema requiere un examen del mismo, identificando y valorando sus activos y las amenazas que se ciernen sobre ellos. De este modelado se deriva una estimación del riesgo inherente al sistema, riesgo que podemos modificar introduciendo una serie de medidas de seguridad que protejan al sistema preventivamente o permitan reaccionar a los incidentes que ocurran. Cuando un sistema entra en operación, siempre es un compromiso entre usabilidad, seguridad y coste, compromiso conocido como riesgo residual del sistema.

Precisamente, con el fin de realizar un examen rápido y eficaz a los sistemas, y disponer de información para tomar decisiones, el Centro Criptológico ha desarrollado y financiado parcialmente la herramienta PILAR (Procedimiento Informático Lógico para el Análisis de Riesgos) actualizada continuamente.

Esta herramienta sigue la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAGERIT, elaborada por el Consejo Superior de Administración Electrónica y las recomendaciones internacionales de ISO 27005 sobre análisis de riesgos e ISO 31000 sobre gestión de riesgos.

PILAR se ha convertido en una herramienta indispensable para los organismos de la Administración Pública española que la utilizan, así como para otras organizaciones internacionales como la Unión Europea y la OTAN (ha sido traducida a ocho idiomas).

NUEVA VERSIÓN PARA ANÁLISIS RÁPIDOS: µPILAR

En el año 2010, se ha desarrollado una versión de PILAR reducida, µPILAR, destinada a la realización de análisis de riesgos muy rápidos. Esta herramienta se distribuye con perfiles específicos y analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (*accountability*). Para tratar el riesgo se proponen salvaguardas (o contramedidas), analizándose el riesgo residual.

Gestionar los riesgos es llegar a un equilibrio entre los riesgos que se asumen y las misiones que se acometen. Para gestionar riesgos necesitamos

PILAR risk analysis tool

Evaluating the security level of a System requires examination and the identification and assessment of assets and the threats involved. The assessment generates an estimate of the risks inherent to the System, risks that can be modified by introducing certain security measures that protect the system or allow to provide a response to security incidents.

Precisely, in order to perform an effective and rapid exam of the systems and to collect the necessary information to take decisions, the CCN has developed and partially financed the PILAR (Computer and Logic Procedure for Analysis of Risks) tool, which is constantly updated.

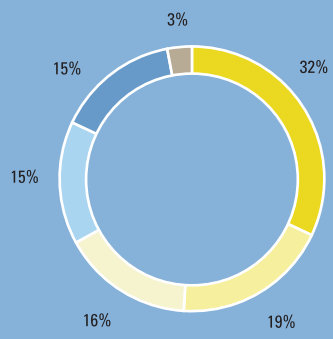
This tool is based on the Risk Analysis and Management Methodology for Information Systems (MAGERIT), developed by the Superior Council of Electronic Administration) and the international recommendations of ISO 27005 on risk analysis and ISO 31000 on risk management.

PILAR has become an essential tool for the organizations of the Spanish Public Administration, as well as for other international organizations such as the European Union and the NATO. It has been translated into eight languages.

NEW VERSION FOR RAPID ANALYSIS: µPILAR

A new reduced version of PILAR appeared in 2010, µPILAR, designed for the performance of rapid risk analysis. This tool is distributed for specific profiles and risk analyses performed from different perspectives: confidentiality, integrity, availability, authenticity and accountability. To confront these

Distribución de usuarios de la herramienta PILAR (2005-2010)
Distribution of PILAR's users (2005-2010)



Distribución de Licencias PILAR | PILAR license distribution	
Solicitante | Applicant	**Nº licencias** | License Number
Administración Central Central Administration	407
Administración Autonómica Regional Administration	253
Administración Local (Ayuntamientos) Local Administration (city councils)	201
Organismos de la Administración Organizations within the administration	215
Universidades Universities	40
Otros Others	202
Total	**1.318**

un análisis rápido y certero de varios escenarios para tomar decisiones bien informadas.

μPILAR es una herramienta que busca poder realizar análisis muy ágiles, en menos de cuatro horas, proporcionando una orientación que puede ser suficiente para sistemas sencillos, o puede ser el primer paso para determinar qué sistemas o partes de un sistema requieren un análisis más profundo y preciso.

Acreditación de sistemas

Se entiende por Acreditación, la autorización otorgada a un Sistema de Información por la Autoridad responsable de Acreditación para manejar información clasificada hasta un grado determinado, o, en unas determinadas condiciones de integridad y/o disponibilidad, con arreglo a su Concepto de Operación (CO). La acreditación de sistemas CIS que manejen información clasificada OTAN/UE o de otros Estados con los que España tiene suscrito acuerdos bilaterales es responsabilidad de la Autoridad Nacional de Seguridad (definida en la persona del Secretario de Estado Director del CNI), mientras que los aspectos técnicos de la acreditación son responsabilidad del CCN.

La acreditación de un Sistema que maneje información clasificada se realiza conforme al procedimiento recogido en la guía CCN-STIC-101:

1. Envío de la solicitud de acreditación y del CO.
2. Validación del CO e inicio del proceso de acreditación.
3. Entrega de la documentación de seguridad (AR, DRS y POS).
4. Revisión y validación de la documentación de seguridad.
5. Implementación de requisitos.
6. Verificación del cumplimiento de los requisitos de emanaciones.
7. Verificación del cumplimiento de los requisitos de seguridad del entorno de operación.
8. Verificación del cumplimiento de los requisitos de seguridad criptológica.
9. Verificación del cumplimiento de los requisitos STIC.
10. Comunicación de la acreditación.

El CCN, como organismo de acreditación, ha realizado durante el año 2010, 14 inspecciones de Seguridad TIC a diferentes sistemas, tanto públicos como privados, cuyo resultado ha sido variable (acreditación, autorización temporal o imposibilidad de acreditación por mostrar deficiencias graves el sistema), tanto para revisar sistemas pendientes de reacreditación como para afrontar nuevas acreditaciones. En total se han expedido 33 autorizaciones temporales (IATO) y 22 autorizaciones para operar, en el ámbito nacional, OTAN o UE, desde Difusión Limitada/NATO Restricted/UE Restricted a Reservado/NATO Secret/EU Secret.

risks the tool recommends safeguards (or countermeasures), analyzing the residual risk.

Risk management consists of achieving a balance between the assumed risks and the missions pursued. To handle these risks we need a rapid and precise analysis on several scenarios to take the appropriate decisions.

μPILAR is a tool designed to make rapid analysis, in less than four hours, providing advice for simple systems, or it can also be used as a first step to determine which systems or parts of a system may require a deeper analysis.

Systems accreditation

Accreditation, as it is understood, is the authorization (issued to a system of Information by the Authority responsible for the Accreditation) of the ability to deal with classified information to a certain degree, or under certain conditions of integrity or availability, in accordance with its Concept of Operation (CO).

The accreditation of CIS systems that deal with classified information from NATO/EU or other States with which Spain

Durante el año 2010, el CCN realizó 14 inspecciones de Seguridad TIC a diferentes sistemas, tanto públicos como privados, cuyo resultado ha sido variable, expidió 33 autorizaciones temporales (IATO) y 22 autorizaciones para operar. During 2010, the CCN performed 14 ICT security inspections to different systems, both public and private, the results of which has been variable, and it issued 33 temporary authorizations (IATO) and 22 authorizations to operate.

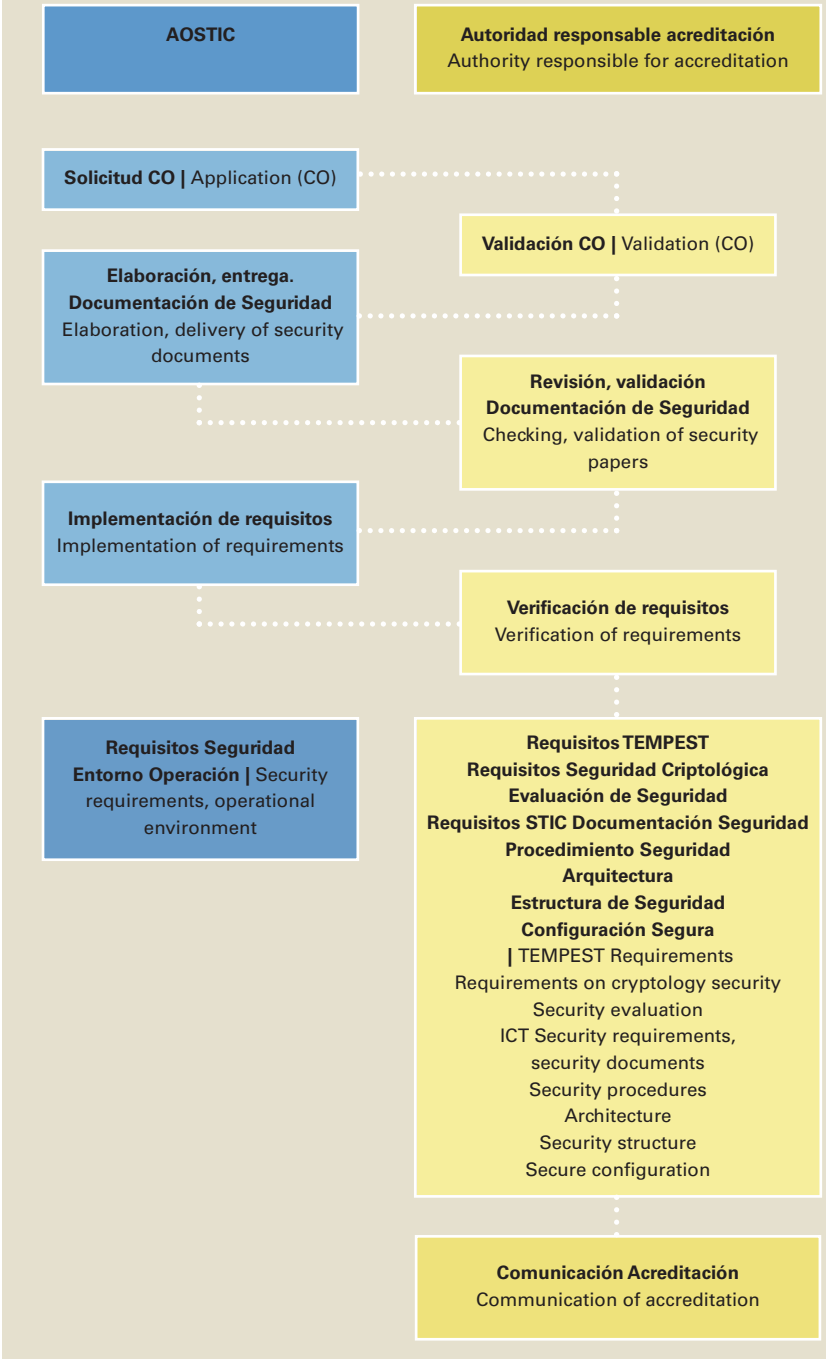
has bilateral agreements, is the responsibility of the National Security Authority (the Secretary of State Director of the CNI), while the technical aspects of the accreditations are the responsibility of the National Cryptologic Centre.

System accreditation is achieved through the following process which is included in the CCN STIC-101 guide:

1. Expedition of Request for Accreditation and for the CO.
2. Validation of the CO and start of the accreditation process.
3. Delivery of security papers.
4. Checking and validation of security papers.
5. Implementation of requirements.
6. Verification of requirements of emanations compliance.
7. Verification of requirements for the security of the operational environment.
8. Verification of requirements for cryptology security.
9. Verification of ICT Security requirements.
10. Communication of the accreditation.

During the course of 2010, the CCN, as an accreditation organization, has performed 14 ICT security inspections for different Systems, both public and private, the results of which have been variable (accreditation, provisional authorization or impossibility of accreditation due to serious system deficiencies, both to analyse systems that have to be reaccredited and systems that will be accredited for the first time. In total, the CCN has issued 33 temporary authorizations (IATO) and 22 authorizations to operate, in a national, NATO or EU level, from Difusión Limitada/NATO Restricted/EU Restricted to Reservado/NATO Secret/EU Secret.

Procedimiento para la acreditación de un Sistema
Process for the accreditation of a system



Desarrollo y promoción de productos

El artículo 2, 2.e del RD 421/2004, señala como una de las funciones del CCN la de coordinar la promoción, desarrollo, obtención, adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los Sistemas TIC que incluyan cifra, para procesar, almacenar o transmitir información de forma segura. El desarrollo de estos productos tiene como objetivo garantizar la seguridad de los sistemas TIC de la Administración. Para tal fin los productos de seguridad deben ser sometidos a un riguroso proceso de evaluación y certificación que permita garantizar que se trata de productos de seguridad confiables.

Dentro del marco de desarrollo de productos de seguridad y de cifra el CCN se encarga, a partir de los fondos de I+D asignados, de cubrir las necesidades operativas de la Administración General del Estado (fundamentalmente del entorno de Defensa y Seguridad Nacional) para desarrollo de productos de las Tecnologías de la Información y las comunicaciones que incluyan cifra y que permitan las comunicaciones seguras de información clasificada.

En este sentido, el CCN ha promovido el desarrollo de diferentes equipos de cifra con tecnología nacional, con recursos de I+D del Ministerio de Defensa (principalmente del CNI y de la Dirección General de Armamento y Material, DGAM), con el fin de mantener una industria nacional que permita a España ser un país productor no sólo a nivel nacional, sino también en el marco de la OTAN y la Unión Europea.

Los desarrollos de productos de cifra abordados en los últimos años han permitido disponer de capacidad para proteger información en redes IP con un nuevo cifrador con mejores prestaciones que los actuales, así como preservar la seguridad de las transmisiones de voz sobre el sistema satélite IRIDIUM con capacidad de interoperar con países OTAN y de las comunicaciones de los usuarios móviles. Por otra parte, los últimos desarrollos de productos para seguridad de la información tratan de garantizar la seguridad del intercambio de información entre dominios de seguridad diferentes y su propio almacenamiento.

Los productos de cifra y para seguridad de las TIC desarrollados en el periodo 2008-2010 más destacados se muestran en la siguiente tabla:

Development and promotion of products

The Article 2,2.e of the RD 421/2004, states that one of the functions of the CCN is to coordinate the promotion, development, acquisition, operation and use of the security technologies for the Systems which include encryption, to process, store or transmit information in a secure way. The purpose of these products is to ensure the security of the information technology systems within the Public Administration. To this end, products are subject to a strict evaluation and certification process to determine their reliability.

Within the area of development of security and encryption products, the CCN covers the operational needs of the State's general administration investing its R&D assigned budget, (mainly in the area of Defence and National Security) by developing ICT products which include encryption and that allow secure communication when dealing with classified information.

In this sense, the CCN has developed more than 50 different crypto equipment with national technology, with the R&D resources of the Ministry of Defence (mainly the CNI and the Directorate General for Armament and Material, DGAM), with the aim of sustaining a national industry that allows Spain to become a producer country, not only at a national level, but also within the NATO and the EU.

The development of crypto equipment during the past years has allowed the protection of IP networks, with a new encryptor that provides a better service and it has also allowed secure voice communications over the satellite system IRIDIUM enabling interoperation with NATO countries. The development of the latest information security products try to guarantee a secure information exchange among different security domains and their own storage.

The most relevant Crypto and ICT products developed during 2008-2010 are:

Producto | Product	**Características** | Characteristics	**Situación** | Situation
CIFIPEVOL 	**Nueva familia de cifradores IP con arquitectura de seguridad mejorada y velocidad de 1 Gbit/s. El módulo criptológico del cifrador es intercambiable dependiendo del nivel de clasificación de la información que maneje (Nacional/OTAN/UE).** New family of IP encryptors of 1 Gbit/s. The crypto module is exchangeable depending on the classification level of the information handled (National/NATO/EU).	**Prevista Certificación Nacional (Secreto) durante 2011, y OTAN (hasta NATO SECRET) y UE (UE SECRET) en 2012.** National certification (Secreto) is expected for 2011, and NATO (up to NATO SECRET) and EU (EU SECRET) is expected for 2012.
CriptoPer Iridium SW 	**PDA para transmisión de voz segura a través del canal Iridium utilizando el protocolo de interoperabilidad SCIP (Secure Communications Interoperability Protocol) de la OTAN.** PDA for the secure transmission of voice and data which has the NATO SCIP (Secure Communications Interoperability Protocol) protocol implemented.	**Producto disponible y Certificado hasta Difusión Limitada.** Available and certified product up to RESTRICTED level.
CriptoPer Iridium HW 	**Mejora del CriptoPer Iridium SW mediante la utilización de un módulo HW de cifrado de voz. El Centro de gestión asociado también es una mejora del anterior con HW de cifrado.** It improves CriptoPer Iridium SW by using a HW module for voice encryption. The associated management centre is also an improvement of the previous version with HW encryption.	**Producto disponible y certificado hasta nivel CONFIDENCIAL. Producto adquirido por OTAN.** Available product and certified up to CONFIDENTIAL level. Product acquired by NATO.
TMSDef 	**Terminal Móvil Seguro basado en PDA comercial securizada para permitir las comunicaciones de voz sobre redes móviles IP.** Secure Mobile Terminal based in secured commercial PDA to allow voice communications over IP mobile networks	**Proyecto en fase final de desarrollo. Prevista certificación hasta Difusión Limitada en 2011.** Project under development. Certification expected for RESTRICTED level throughout 2011.
EP830 	**Sistema multidominio seguro que se puede utilizar para procesar información de diferentes dominios de seguridad.** Secure Multilevel system which can be used to process information from different domains of security	**Desarrollo finalizado. Certificado Common Criteria (EAL 4+).** Development completed. Common Criteria certificate (EAL 4+)
EP1140 	**Ordenador seguro basado en el sistema multinivel (EP830) que proporciona un entorno de ejecución seguro.** Secure computer based on multilevel system (EP830) which provides a secure execution environment	**Desarrollo finalizado. En proceso de evaluación.** Development completed. Under evaluation process.
Pasarela de Correo Seguro 	**Sistema que permite el intercambio de correo electrónico de forma segura entre dos redes TCP/IP separadas.** System that allows the secure exchange of e-mails between two TCP/IP networks	**Desarrollo finalizado. Finalizada evaluación Common Criteria (EAL 4+).** Development completed. Common Criteria Evaluation completed (EAL 4+).

26 ORGANISMOS Y CAPACIDADES DEL CCN
CCN ORGANIZATIONS AND CAPABILITIES

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional. Este servicio se creó a finales del año 2006 como CERT gubernamental español, y sus funciones quedan recogidas en el capítulo VII del RD 3/2010, de 8 de enero, regulador del ENS. Este texto legal señala los servicios que el CCN-CERT ya prestaba desde su constitución (en parte recogidos en el RD 421/2004 de regulación del CCN), y que ahora quedan establecidos en el artículo 37 de este RD:

- Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan la Administración General del Estado, las administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas.

  El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información de las administraciones públicas.

  Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar los informes de auditoría de los sistemas afectados.
- Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las administraciones públicas. Con esta finalidad, las series de documentos CCN-STIC ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el ENS y para garantizar la seguridad de los sistemas de Tecnologías de la Información en la Administración.
- Formación destinada al personal de la Administración especialista en el campo de la seguridad TIC, al objeto de facilitar la actualización de conocimientos y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.
- Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

Además, el CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las administraciones públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquél, será coordinador a nivel público estatal.

The CCN-CERT is the CCN's Computer Emergency Response Team. This service was created at the end of 2006 as the Government Spanish CERT and its functions are specified in chapter VII of RD 3/2010, of January 8. This chapter includes the services the CCN-CERT has offered since its creation (which are in part specified in RD 421/2004), and that are now contained in article 37 of this RD:

- Support and coordination for vulnerabilities management and for the resolution of security incidents suffered by the State's General Administration, by the regional and local administrations and the public-sector bodies with their own legal personality or dependent on any of the aforementioned administrations.

  The CCN-CERT, through its technical support and coordination service, will act quickly to face any targeted attack against the Public Administration's Information Systems.

  For the fulfillment of these objectives the CCN-CERT can gather the audit reports for the affected systems.
- Research and diffusion of the best practices on information security among all the members of Public Administrations. To this end, the CCN-STIC Series will offer standards, instructions, guidelines and recommendations to implement the ENS and to ensure the security of ICT systems within the Public Administration.
- Training aimed at specialised Public Administration staff in the area of ICT security in order to update the staff's knowledge and to raise awareness and improve the staff's ability to detect and handle incidents.
- Information about vulnerabilities, alerts and advice on new threats targeted at Information Systems, compiled from different renowned and prestigious sources, including their own.

Besides, the CCN will develop a program that will offer information, training, recommendations and the tools that public administrations may need to develop their own incident response capabilities.

Funciones del CCN-CERT
Functions of CCN-CERT

Las funciones especificadas en el RD han sido establecidas para servir al objetivo principal del CCN-CERT: contribuir a la mejora del nivel de seguridad de los sistemas de información de las tres administraciones públicas existentes en España (general, autonómica y local). De hecho, su misión es convertirse en el centro de alerta nacional que coopere y ayude a todas las administraciones públicas a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir, y afrontar de forma activa las nuevas amenazas a las que hoy en día están expuestas.

Servicios

GESTIÓN DE INCIDENTES

Cualquier organismo público que sufra un ataque en sus sistemas puede solicitar la colaboración del CCN-CERT para su resolución. Este equipo proporcionará asistencia técnica directamente o pondrá en contacto al solicitante con otros sitios involucrados en el mismo incidente, señalará documentos técnicos relevantes o sugerirá medidas para restaurar la seguridad del sistema. Hay que tener en cuenta que el Equipo recibe informes de incidentes de todas las partes del mundo que, en muchos casos, tienen similares características o involucran a los mismos atacantes, por lo que, al centralizar la gestión, es mucho más rápida y eficaz su resolución.

En este sentido, la política del CCN-CERT es mantener siempre la confidencialidad sobre cualquier información específica de la Administración solicitante de ayuda.

The functions specified in the Royal Decree serve to the CCN-CERT's main objective: improve the security level of the information systems of the three public administrations in Spain (general, regional and local). In fact, its mission is to become the National Alert Centre and cooperate or help Public Administration to respond rapid and efficiently to security incidents that may arise and to actively confront new threats to which they are currently exposed.

Services

INCIDENT MANAGEMENT

Any public organization that suffers an attack against its system can request the CCN-CERT's collaboration.This team will provide direct technical support or will put the organization in contact with other affected systems, or will provide it with relevant technical documents or will suggest it to adopt certain measures to restore the security of their systems.The CCN-CERT receives incident reports from all parts of the world, and sometimes, these incidents have similar characteristics or involve the same attackers, so by centralizing its incident management capabilities, CCN-CERT can provide a faster and more efficient response. CCN-CERT's policy is to keep the confidentiality on the information provided by the public administration that asks for its help.

INFORMATION, ALERTS, ADVICE AND VULNERABILITIES

CCN-CERT offers all type of information to all its Community, among which we can highlight vulnerabilities, alerts and

advice on new threats targeted at Information Systems, based on the work of their own analysts and on the work of different renowned and prestigious collaborating sources, both at a national and international level. These vulnerabilities are classified according to their risk, confidence level, the impact they may have or the difficulty of its resolution.

Through the www.ccn-cert-cni.es portal, any civil servant can subscribe to this service and receive the following information:

- Daily newsletter with vulnerabilities, alerts, advice on new threats. In the last three years, around 300 zero-day vulnerabilities have been detected and more than 21.600 vulnerabilities of different criticality.
- Daily news on ICT security coming from different sources and concerning a wide range of subjects: standards and legislation, cyber security, personal data protection and privacy, on-line fraud and phishing, spam, virus, Trojans, reports or statistics from third parties, events of interest and critical infrastructures.
- Releases of interest published by CCN-CERT.
- Biweekly Reports, Malicious Code Reports and Threat Reports that provide current information on security, threat levels or a deep analysis on certain subjects (hacking, critical infrastructures, etc.) at national and international level. During the past three years, the CCN-CERT portal has released 23 Threat Reports, 93 Biweekly Reports and 9 Malicious Code reports.
- Annual Threat ad Trends Reports describe the most important threats and vulnerabilities of the past year, as well as expected trends for the following year.

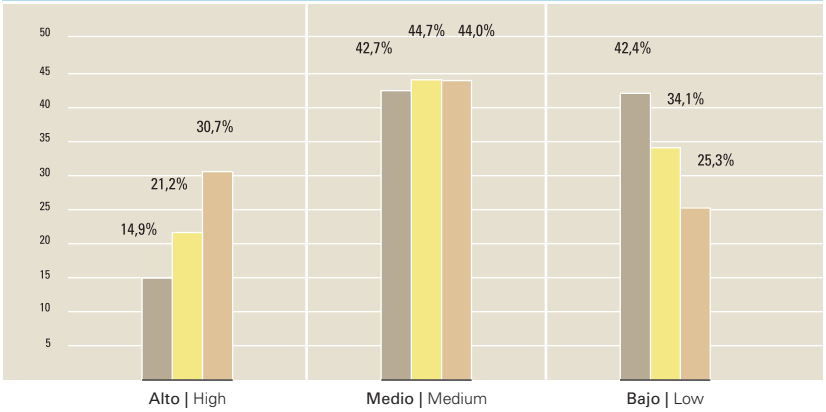
INFORMACIÓN, ALERTAS, AVISOS Y VULNERABILIDADES

El CCN-CERT ofrece diferente información a toda su Comunidad, entre la que destacan las vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, basadas tanto en el trabajo de sus propios analistas como en las contribuciones procedentes de muy diversas fuentes de reconocido prestigio, nacionales e internacionales. Estas vulnerabilidades se clasifican según su riesgo, su nivel de confianza, el impacto que pueden tener o la dificultad de su resolución.

Además, a través del portal **www.ccn-cert.cni.es**, cualquier usuario de Internet puede acceder y recibir directamente por suscripción la siguiente información:

- Boletines diarios de vulnerabilidades, alertas y avisos de nuevas amenazas. En los últimos tres años se han detectado alrededor de 300 vulnerabilidades de Día 0 y más de 21.600 con diferente criticidad.
- Noticias diarias sobre seguridad TIC de distintas fuentes y de muy diferente temática: normativa y legislación, ciberseguridad, protección de datos personales y privacidad, fraude *on-line* y *phishing*, *spam*, virus, troyanos, informes o estadísticas de terceros, eventos de interés e infraestructuras críticas.
- Comunicados de interés emitidos por el propio CCN-CERT.

Vulnerabilidades recogidas por nivel de criticidad
Vulnerabilities classified by level of criticality
[2008 | 2009 | 2010]



- Informes de Actualidad, Código Dañino y Amenazas donde se proporciona información actual sobre la seguridad, nivel de amenaza, nivel de riesgo o análisis exhaustivos de algún tema (*hacking*, infraestructuras críticas, etc.) tanto a nivel nacional como internacional. En los tres últimos años se han publicado en el portal del CCN-CERT, 23 informes de amenazas, 93 informes de actualidad y 9 informes de código dañino.
- Informes de Amenazas y Tendencias anuales en los que a raíz del trabajo y experiencia del CCN-CERT se hace un balance de las amenazas y vulnerabilidades detectadas en el año anterior, así como las tendencias previstas para el siguiente.

2008-2010	**Número de Informes CCN-CERT elaborados y difundidos en el portal** CCN-CERT portal has released	
	Informe Amenazas | Threat Reports	23
	Informe Actualidad | Biweekly Reports	93
	Informe Código Dañino Malicious Code Report	9

AUDITORÍAS WEB

El equipo CCN-CERT lleva a cabo auditorías a páginas web de distintos organismos de las administraciones públicas en busca de posibles vulnerabilidades críticas, con el fin de establecer las pautas adecuadas para reducirlas o eliminarlas.

Estas auditorías demuestran que los problemas de seguridad en las diferentes sedes electrónicas son similares y siguen patrones parecidos a las estadísticas publicadas por el CCN-CERT. En este sentido, destacan las vulnerabilidades de inyección de código SQL, las vulnerabilidades del tipo XSS (*Cross Site Scripting*) y las deficiencias de configuración del equipamiento.

Estas vulnerabilidades pueden provocar alteraciones no autorizadas de la base de datos y ejecución remota de procesos en el servidor, permitiendo, entre otros ataques, la denegación de todo el servicio web (DDoS), la posibilidad de sustitución total o parcial de los contenidos web en el servidor (*Defacement*), o, como resultado de los procesos anteriores, la escalada de privilegios y compromiso de los sistemas accesibles.

WEB AUDITS

The CCN has carried out the audit of webs from different Organizations of the Public Administration in search of possible risks and vulnerabilities, in order to establish the appropriate guidelines to reduce or eliminate them.

These audits demonstrate that the security problems that affect different websites are similar and follow similar patterns to the statistics published in organizations such as the one mentioned above about web services. In this sense, we could highlight SQL injection vulnerabilities, XSS (Cross Site Scripting) vulnerabilities and equipment configuration deficiencies. These vulnerabilities can produce non-authorized alterations in the database and the remote execution of processes within the server, allowing, among other attacks, the denial of service in the web, the partial or total substitution of the web content (defacement) or, as a result of the previous processes, privilege escalation and compromise of accessible systems.

During 2008 and 2010, CCN-CERT has performed technical analysis, web audits, security studies or vulnerability analysis for a large number of webs from different organizations. Among others, it has made interventions for webs from the AGE: Ministry of Presidency, Spanish Presidency of the EU, La Moncloa, State's Official Gazzet, Ministry of Justice, Ministry of Foreign Affairs and Cooperation, Ministry of Industry, Tourism and Commerce, Ministry of Culture, Spanish Ministry of General Directorate of Traffic (DGT), 060, TECNIMAP or Spanish National Research Council (CSIC). Besides, it has performed audits for the Spanish Federation of Municipalities and Provinces (FEMP), Andalucía, Valencia and La Rioja's Regional Government and the Autonomous city of Melilla.

El CCN-CERT recibe informes de incidentes de todas las partes del mundo que, en muchos casos, tienen similares características o involucran a los mismos atacantes, por lo que, al centralizar la gestión, es mucho más rápida y eficaz su resolución. The CCN-CERT receives incident reports from all parts of the world, and sometimes, these incidents have similar characteristics or involve the same attackers, so by centralizing its incident management capabilities, CCN-CERT can provide a faster and more efficient response.

New services of CCN-CERT

EARLY WARNING SYSTEM

In order to guarantee an appropriate security level in the systems of public administrations it is necessary to act before incidents occur or, at least, to detect them as soon as possible in order to minimize its impact and scope. Therefore, since 2008, the CCN-CERT has been developing an Early Warning System (SAT) for the rapid detection of incidents and anomalies within the Administration's scope, a system which allows the implementation of preventive, corrective and containment action.

At first, the development of the SAT for the SARA network was started, in collaboration with the Ministry of Public Administrations (today's Ministry of Territorial Policy and Public Administration). Subsequently, in 2010, the CCN initiated the implementation of this incident detection service, with the deployment of intrusion detection systems (IDS) in the Internet outputs (Internet Sensors) of those public organizations that decide to join.

Through both systems, the CCN, in collaboration with the subscribed agency, can detect a wide range of attacks, avoiding its expansion, responding rapidly to the incidents that may arise and, generally, establishing performance standards which may help to prevent future incidents. The Early Warning System, through its portal, offers reports and

En el período comprendido entre los años 2008 y 2010, el CCN-CERT ha realizado análisis técnicos, auditorías web, estudios de seguridad o análisis de vulnerabilidades a un buen número de páginas web de distintos organismos. Entre otros, se han realizado acciones con las páginas de la AGE: Ministerio de la Presidencia, Presidencia Española de la Unión Europea, La Moncloa, Boletín Oficial del Estado, Ministerio de Justicia, Ministerio de Asuntos Exteriores y Cooperación, Ministerio de Industria, Turismo y Comercio, Ministerio de Cultura, Dirección General de Tráfico, 060, TECNIMAP o CSIC. Además, se han realizado auditorías a la Federación Española de Municipios y Provincias (FEMP), a la Junta de Andalucía, Gobierno de La Rioja, Generalitat Valenciana y a la Ciudad Autónoma de Melilla.

Nuevos servicios del CCN-CERT

SISTEMA DE ALERTA TEMPRANA

Para garantizar el nivel de seguridad adecuado en los sistemas de las administraciones públicas es necesario actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance. Por este motivo, desde el año 2008 el CCN-CERT viene desarrollando un Sistema de Alerta Temprana (SAT) para la detección rápida de incidentes y anomalías dentro del ámbito de la Administración, que permite realizar acciones preventivas, correctivas y de contención.

En un primer momento, se inició el desarrollo del SAT de la Red SARA, en colaboración con el Ministerio de Administraciones Públicas (actual Ministerio de Política Territorial y la Administración Pública). Posteriormente, en 2010, comenzó la implantación de este servicio de detección de incidentes

Servicios de Alerta Temprana
Early warning services

de seguridad, con el despliegue de sistemas de detección de intrusos (IDS) en las salidas de Internet (Sondas de Internet) de los organismos públicos que deciden adherirse.

A través de ambos sistemas, el CCN, en colaboración con el organismo adscrito, puede detectar un amplio abanico de ataques, evitando su expansión, respondiendo de forma rápida ante el incidente detectado y, de forma general, generar normas de actuación que eviten futuros incidentes. El SAT, a través de su portal web, ofrece, además, informes y estadísticas sobre el número de eventos e incidentes en cada área de conexión. Estas métricas se pueden utilizar para medir el estado general de la seguridad de un Organismo.

Sistema de Alerta Temprana de la Red SARA. Este sistema está basado en la correlación de *logs* (registro de datos) sobre las áreas de conexión de la red SARA, que proporciona un compromiso constante de seguridad y emite alarmas ante cualquier incidente. El sistema permite detectar de manera proactiva las anomalías y los ataques en el tráfico que circula entre los diferentes Ministerios y Organismos conectados a la citada Red y ofrece una visión en tiempo de real del estado de la seguridad de la red, mediante diferentes sensores.

El sistema cataloga las alertas con diferentes niveles de criticidad, pasando a niveles superiores las alertas que han sido procesadas y escaladas por el motor de correlación y convirtiéndose en incidentes de seguridad en función de la evaluación que se realiza de ellas a través de un equipo de expertos en seguridad.

Desde su puesta en marcha en 2008, se han desplegado 30 sondas de recolección en las áreas de conexión y se han integrado un gran número de fuentes de datos (sistema de detección de intrusos o cortafuegos perimetrales de la red SARA, entre otras). De igual modo, se ha implantado un sistema central de correlación y se han adaptado reglas al IDS. De hecho, en estos tres años se ha conseguido una gran estabilidad y maduración dentro del Sistema y de la propia red, lo que permite una detección más fiable, eliminando los falsos positivos propios de cada red.

statistics about the number of events registered through its web portal. These metrics can be used to measure the security level of an organization.

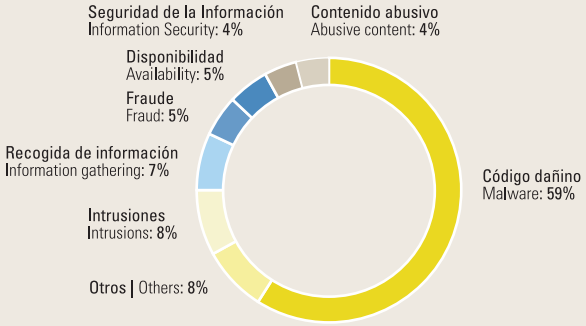
Early Warning System of SARA network. This system is based in log correlation (data registry) for the areas of connection of the SARA network that provides a constant commitment to security and t issues alerts for all types of incidents. The system allows the proactive detection of anomalies and attacks on traffic that flows among Ministries and Organizations connected to the aforementioned network and offers a real time vision of the network security level, using different sensors.

The system classifies the alerts by different levels of critically, taking to a superior level the alerts that have been processed and escalated by the correlation engine and transforming them into security incidents, depending on the evaluation performed by the team of security experts.

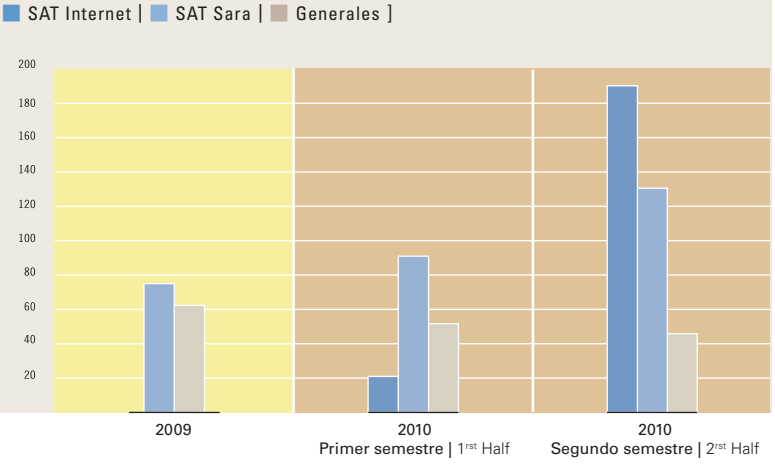
Since its inception in 2008, 30 collecting sensors have been deployed in the connection areas and a large number of data sources have been integrated (intrusion detection system, perimeter firewalls of the SARA network, among others). Likewise, a central correlation system has been implemented and some rules have been adapted for the IDS. In fact, in the past three years, great stability and maturity have been achieved within the System and the network itself, allowing for a more reliable detection and eliminating false positives for each network.

El número de incidentes que recogen cada año los Sistemas de Alerta Temprana del CCN, tanto la Red SARA como las Sondas individuales de Internet, no ha parado de crecer. Te number of incidents annually registered by SARA network and by Internet individual sensors has been constantly growing.

Tipo de Incidentes
Incident Types



Incidentes gestionados por el CCN-CERT
Incidents Handled by CCN-CERT



Internet Early Alert System (individual probes). This system consists of the introduction of an individual probe in the Organization's Internet output which is responsible for collecting relevant security information, and, after a first filtrate, it sends the security events to the Central System which performs a correlation among the different elements and domains.

This system was implemented in mid-2010 and, from then until now, it has experienced an enhancement in the incorporation of sources in the probe itself and in the reliability of detections by the central system.

On March 30, 2011, the Internet SAT had 13 sensors, which cover the Ministry of Industry, the Ministry of Defense, the Ministry of Foreign Affairs, the Ministry of Territorial Policy and Public Administration, the National Library, the Ministry of Economy, the Royal House the Ministry of Health, the National Police Force, the Ministry of Culture, the Ministry of Labor, the Ministry of the Interior and the Official State Gazette. By 2011, it is expected to have 25-30 probes installed. The more frequently detected events are those related to policy violations with a 50% detection rate. The Internet EWS also detects other type of events such as scans, malicious code, Spyware, Trojans or exploits.

The number of incidents annually registered by SARA network and by Internet individual sensors has been constantly growing.

Sistema de Alerta Temprana de Internet (sondas individuales). En este caso se trata de la implantación de una sonda individual en la salida de Internet del Organismo adscrito al sistema que se encarga de recolectar la información de seguridad relevante que se detecte y, después de un primer filtrado, envía eventos de seguridad hacia el Sistema Central que realiza una correlación entre los distintos elementos y entre los distintos dominios.

Este sistema se implantó a mediados del año 2010 y, desde entonces hasta la actualidad se ha desarrollado una mejora en la incorporación de fuentes en la propia sonda y la fiabilidad de la detección del sistema central.

Con fecha 30 de marzo de 2011, el SAT de Internet tenía desplegadas 13 sondas, que dan cobertura al Ministerio de Industria, Ministerio de Defensa, Ministerio de Asuntos Exteriores, Ministerio de Política Territorial y Administración Pública, Biblioteca Nacional, Ministerio Economía, Casa Real, Ministerio Sanidad, Cuerpo Nacional de Policía, Ministerio de Cultura, Ministerio de Trabajo, Ministerio de Interior y Boletín Oficial del Estado, A finales del 2011 se prevé tener instaladas de 25 a 30 sondas. Los eventos más detectados son los relacionados con la violación de políticas de seguridad con un 50% de los casos. Escaneos, código dañino, *Spyware*, troyanos o *exploits* son otro tipo de eventos frecuentes que recoge el SAT de Internet.

El número de incidentes que recogen cada año tanto la Red SARA como las Sondas individuales de Internet no ha parado de crecer.

Beneficios aportados a la Administración Pública. Los servicios de alerta temprana tienen como principal función la protección proactiva (aplicación de medidas antes de que se produzca un incidente o sea detectado) y protección reactiva (en el caso de producirse un incidente, la rápida detección del sistema permite la aplicación de medidas de contención y eliminación de la amenaza necesaria para evitar el incidente).

En el caso de los sistemas descritos, estas ventajas podrían resumirse en las siguientes:

- Detección avanzada interdominio (detección de un incidente antes de que llegue a introducirse en un determinado dominio).
- Información de gran valor para los responsables TIC de las Administración, que pueden ver, en tiempo real, los eventos de seguridad generados en su red, así como acceder a informes estadísticos.
- Detección de un amplio espectro de ataques y, con ello, una respuesta rápida y eficaz a los incidentes.
- Detección de código dañino, evitando su expansión a través de toda la infraestructura interministerial.
- Protección adicional hacia los ciudadanos que acceden a los distintos servicios ofrecidos por los organismos públicos.
- Normalización de la información, unificando los eventos que se recogen de las distintas fuentes, su lenguaje y su tratamiento posterior, ofreciendo modelos para una lectura adecuada de la misma.
- Ajuste de herramienta de correlación (sintonía) y enriquecimiento de patrones de firma de los diferentes elementos de seguridad.
- Consolidación y centralización. Todos los eventos se consolidan y centralizan en un único sistema, realizando una revisión a través de una única consola.
- Correlación. Con la utilización de técnicas avanzadas de correlación, el sistema central no sólo detecta incidentes importantes de forma individual, sino que se llega a la detección de eventos más complejos que pueden involucrar a distintos organismos.

Advantages for Public Administration. The main purpose of the early warning services is to provide a proactive protection (implementation of preventive measures before incidents occur or before their detection) and reactive protection (in case an incident takes place, the rapid detection allows the application of containment measures and the threat's elimination in order to avoid the incident).

In the case of the described systems, these advantages are:

- Advanced crossdomain detection (detection of an incident before it is introduced in a specific domain).
- Valuable information for CIS administrators who could see, in real time, the security events that arise in their network, and they can also access to statistical reports.
- Detection of a wide range of attacks and, therefore a rapid and efficient response to incidents.
- Malicious code detection, preventing its expansion in all the interministerial infrastructure.
- Additional protection for citizens who access services offered by public organizations.
- Standarization of information, unifying events collected from different sources, its language and its subsequent treatment, providing models for an appropriate interpretation of the same.
- Adjustment of correlation tool and enrichment of signature patterns for different security elements.
- Consolidation and centralization. All the events are consolidated and centralized in a single system, undertaking a review from a single console.
- Correlation. By using advanced correlation techniques, the central system not only detects important incidents individually, but it also detects more complex events that may affect several organizations.

SISTEMA MULTIANTIVIRUS / ANÁLISIS DE CÓDIGO DAÑINO

El Sistema Multiantivirus (MAV) permite analizar todo tipo de código, haciendo uso de múltiples motores antivirus, actualizados en tiempo real. De este modo, cualquier Organismo de la Administración (general, autonómica o local) que disponga de un archivo sospechoso de estar infectado, puede cargarlo en el interfaz web de la página del CCN-CERT. Al cabo de unos instantes, y tras haberse realizado el análisis, el usuario recibirá un informe sobre el citado archivo en su correo electrónico.

En caso de incidentes de cierta relevancia, el CCN-CERT también analiza de forma minuciosa el código dañiño remitido por el personal de la Administración Pública o detectado a través de sus servicios SAT. Este mismo análisis se efectúa en el caso de especímenes novedosos. En ambos casos, el personal del Centro elabora un informe sobre el comportamiento del código, sus capacidades y el procedimiento de eliminación, así como recomendaciones para evitar incidentes futuros. Llegado el caso, el CCN-CERT genera las correspondientes reglas Snort para incorporarlas a sus servicios de Alerta Temprana.

SISTEMA DE ANÁLISIS WEB

El Sistema de Análisis Web (SAW) es un servicio desarrollado e implantado por el CCN-CERT, el cual ofrece a los responsables TIC una visión en tiempo real del estado de seguridad de sus sitios web, detectando posibles incidentes. Para ello, elabora un análisis de los contenidos hospedados en los diferentes sitios webs de la Administración.

El análisis se realiza en dos niveles: un primer nivel de análisis de cada página para detectar los contenidos sospechosos, y un segundo nivel para identificar los diferentes enlaces que aparecen en cada página para visitarlos y analizarlos de forma recursiva.

El sistema proporciona un interfaz web para poder monitorizar la actividad en tiempo real, y para poder ver la información de las alertas emitidas.

MULTIANTIVIRUS SYSTEM/ MALICIOUS CODE ANALYSIS

The multiantivirus system (MAV) can perform analysis for all kinds of code, by using different antivirus engines, updated in real time. This way, any agency within the Public Administration (general, regional or local) which has a suspicious file that may be infected, can upload it to the web interface. After a while and upon the completion of the analysis, the user will receive an e-mail including a report about the suspicious file.

In the case of significant incidents, the CCN-CERT thoroughly analyzes the malicious code sent by the Public Administration staff or detected through its EWS services. This analysis is also applied to new samples. In both cases, the CCN-CERT draws up a report about the code's behavior, its capabilities and its elimination procedure, and it includes certain recommendations to prevent future incidents. If necessary, the CCN-CERT creates the relevant Snort rules to include them in its Early Warning services.

WEB ANALYSIS SYSTEM

The Web Analysis System (SAW) is a service developed and implemented by the CCN-CERT, which provides ICT managers with a real time overview of the security level of its webs, detecting possible incidents. In order to achieve it, it performs an analysis of the contents included in the Administration webs.

The analysis is performed in two levels: a first analysis to detect suspicious contents and a second analysis to identify the links included in each web.

The system provides a web interface to monitor activity in real time, and to see the information on the alerts issued.

Cualquier Organismo de la Administración pública (general, autonómica o local) que disponga de un archivo sospechoso de estar infectado, puede cargarlo en el interfaz web de la página del CCN-CERT. Al cabo de unos instantes, y tras haberse realizado el análisis, el usuario recibirá un informe sobre el citado archivo en su correo electrónico. Any agency within the Public Administration (general, regional or local) which has a suspicious file that may be infected, can upload it to the web interface. After a while and upon the completion of the analysis, the user will receive an e-mail including a report about the suspicious file.

Portal www.ccn-cert.cni.es

La principal herramienta que ha desarrollado el CCN-CERT para coordinar y dar soporte a los responsables TIC de las distintas administraciones es el portal **www.ccn-cert.cni.es**. A través de este portal se ofrece, entre otros, información actualizada diariamente sobre amenazas, vulnerabilidades, guías de configuración de las diferentes tecnologías, herramientas de seguridad, cursos de formación o indicaciones para mejores prácticas de seguridad.

Dado el carácter crítico de algunos de los aspectos recogidos en el portal, existe una parte de acceso restringido exclusivo para los responsables de seguridad TIC de la Administración. En ella se encuentra toda la información, productos y servicios puestos a su disposición por el CCN-CERT. Asimismo, en esta zona se pueden obtener las directrices para notificar incidentes al Equipo.

El área restringida ha ido incrementando paulatinamente su número de usuarios. Así, si al finalizar el año 2009, el portal contaba con 1.867 usuarios registrados (lo que supuso 609 nuevos respecto al año anterior), en 2010 esta cifra se elevó hasta los 2.591, un 38% más que en el ejercicio anterior.

De los usuarios registrados, el 58% pertenecen a la Administración General del Estado, el 18% a la autonómica y el 16% a la local.

Portal www.ccn-cert-cni.es

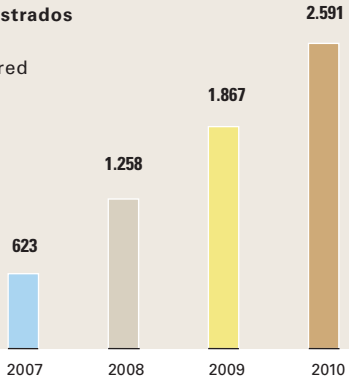
www.ccn-cert.cni.es portal is the main tool developed by the CCN-CERT to coordinate and give support to ICT managers. The Web offers, among other things, daily updated information concerning threats, vulnerabilities, configuration guidelines for several technologies, security tools, training or instructions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

Given the critical nature of some of the issues included in the portal, there is a restricted access section which is only available to ICT security Administration staff and contains information, products and services offered by the CCN-CERT. Likewise, this area provides guidelines for the reporting of incidents.

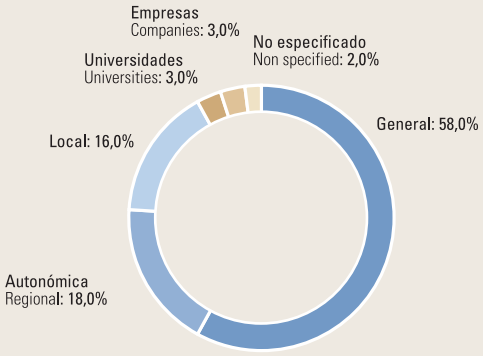
The number of users who have access to this restricted area has steadily increased. By the end of 2009, the portal had 1.867 registered users (which meant an increase of 609 new users compared to previous year), while in 2010 this figure increased to 2.591 users, an increase of 38% compared to the previous year.

58%of these registered users are employees of the State's General Administration, 18% work for the Regional Administration and 16% for the local administration.

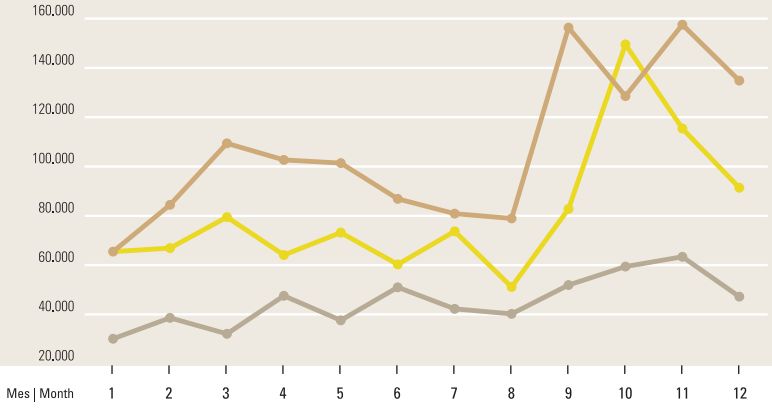
Número de usuarios registrados en el Portal por año
Number of users registered by year



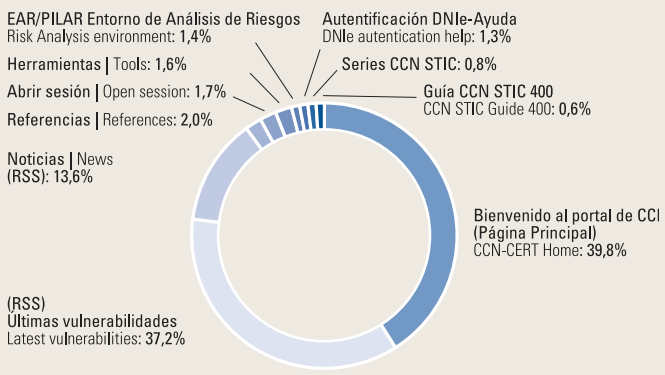
Organización a la que pertenecen los usuarios registrados
Organization to which the registered users belong



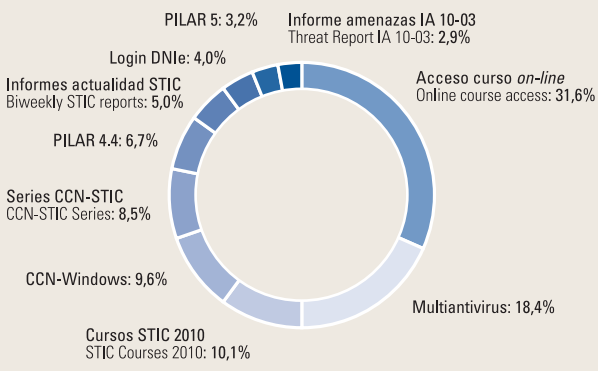
Número de accesos al portal www.ccn-cert.cni.es
Number of access to portal www.ccn-cert.cni.es
[2008 | 2009 | 2010]



Las 10 páginas públicas más visitadas
The 10 more visited public webs



Las 10 páginas privadas más visitadas
Top 10 most visited private webs



ORGANISMO DE CERTIFICACIÓN OC

CERTIFICATION BODY (OC)

El Organismo de Certificación (OC) del Centro Criptológico Nacional se rige por la normativa del CNI, por el RD 421/2004, que regula el propio CCN, por el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información y las Comunicaciones, aprobado por Orden PRE/2740/2007, y por su propia normativa interna adaptada a los requisitos necesarios para ser reconocido tanto a nivel nacional, según la norma EN45011, como a nivel internacional, de acuerdo con el «Arreglo de Reconocimiento de Certificados de Criterios Comunes, CCRA», como entidad de certificación de la seguridad de las TIC.

El OC/CCN viene operando desde finales del año 2004 con diversas normas de evaluación de la seguridad de las TIC, entre ellas la de mayor reconocimiento internacional, la denominada Common Criteria (ISO-15408). De ella se han venido recibiendo y tramitando diversas solicitudes de certificación de productos para su posible uso en la Administración electrónica española. Esta norma define niveles de evaluación entre EAL1 y EAL7, siendo el CCRA el acuerdo internacional que da cobertura al reconocimiento mutuo de certificados entre los niveles EAL1 a EAL4.

El ámbito de actuación del OC comprende a las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TIC en el marco del Esquema, y a las entidades públicas o privadas fabricantes de productos o sistemas de TI que quieran certificar la seguridad de dichos productos en el marco del Esquema y cuando dichos productos o sistemas sean susceptibles de ser incluidos en el ámbito de actuación del CCN.

El Director del CCN es la autoridad de certificación de la seguridad de las Tecnologías de la Información y autoridad de certificación criptológica en el ámbito de la Administración y, como tal, es el responsable del desarrollo de la normativa para la protección de los equipos/sistemas y las instalaciones donde se procesa información clasificada, según el citado RD de 2004.

The certification body (OC) of the National Cryptologic Center is subject to the CNI regulations, to the RD 421/2004, that regulates CCN, to the Evaluation and Certification of Information Technologies Regulation, which was approved by Order PRE/2740/2007, and to its own internal regulation adapted to the requirements needed to be recognized at a national level, in accordance with standard EN45011, and at an international level, in accordance with the Common Criteria Recognition Arrangement (CCRA) as a certification body for ICT security.

The OC/CCN has been operating since 2004 with several evaluation standards for ICT security, including the Common Criteria (ISO-15408), which is the most internationally renowned. This standard is used for the certifications of products to be used in the Spanish eGovernment. This standard defines assessment levels between EAL7 and EAL1, being the CCRA international agreement the one that covers the mutual recognition of certificates between levels EAL1 to EAL4.

The OC's scope includes public or private entities who wish to function as evaluation laboratories for ICT security, as well as public or private entities manufacturers of ICT systems or products who wish to certify the security of these products or systems, as long as these products or systems can be included in the CCN's scope.

CCN's Director is the authorized certification body for the security of ICT and the cryptology certification body for the Administration and as such, he is responsible for the development of regulations for the protection of equipment/systems that process and store classified information, in accordance with RD of 2004.

Esquema Nacional de Seguridad

Este Real Decreto, en su artículo 18, en lo referente a la adquisición de productos de seguridad, indica que en las adquisiciones de productos que vayan a ser utilizados por las administraciones públicas se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición. Dicha certificación deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, y será el OC/CCN quien dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados.

Además el OC/CCN proporcionó para el Anexo II «Medidas de Seguridad» del ENS, la especificación de en qué tipos de sistemas se deben utilizar componentes certificados según su nivel de riesgo. Finalmente, en el Anexo V, se incluyó un modelo de cláusula administrativa particular que puede usarse para incluir estos requisitos en las adquisiciones públicas.

National Security Framework

This RD points out in its article 18 that security products with the appropriate security certification will be positively valued for their acquisition by public administration. This certification should comply with international norms and standards, and the OC/CCN will determine the criteria to be followed, depending on the intended use of the product, on the evaluation level, and on other security certifications required by regulations.

Besides, the OC/CCN specifies which type of systems should use certified components (Annex II «Security Measures » of the ENS). Finally, Annex V includes a model administrative clause that could be used to include those requirements within public administrations.

Ámbito de actuación del OC
OC field of action

Common Criteria Recognition Arrangement (CCRA)

El OC/CCN se mantiene desde el año 2006 hasta la actualidad como emisor autorizado de certificados bajo el CCRA, que es el acuerdo de reconocimiento mutuo internacional para la seguridad «funcional» de productos TIC, y al que pertenecen actualmente veintiséis países de los más industrializados del mundo (**http://www.commoncriteriaportal.org**). Este certificado es el resultado del análisis de la seguridad de los productos y sistemas considerando cómo son sus funciones o las funciones destinadas a proporcionar seguridad al propio objeto de evaluación (OE).

La certificación y evaluación funcional se centra en qué hace el OE y cómo lo hace, analizando si en su propio comportamiento o en la manera que está construido hay alguna vulnerabilidad susceptible de provocar un problema de seguridad; bien sea por una incorrecta implementación de las funciones del OE, bien sea porque dichas funciones no sean suficientemente efectivas para alcanzar los objetivos de seguridad propuestos. Se evalúa tanto la corrección como la efectividad de las funciones del OE.

Por ejemplo, un OE que consistiese en un programa *software* que presentase una función de control de acceso basada en clave secreta de usuario (alfanumérica), podría presentar problemas de seguridad como:

- Problema de corrección: el desarrollo del programa no ha contemplado el uso de caracteres alfanuméricos especiales y, al introducirlos el usuario, la función falla y permite el acceso no autorizado del mismo.
- Problema de efectividad: la función se ejecuta correctamente pero se ha diseñado usando sólo cuatro caracteres de longitud, lo que hace que ataques de fuerza bruta puedan ser posibles en periodos de tiempo más cortos que los previstos al plantear los objetivos de seguridad del OE.

Los métodos de evaluación de seguridad funcional han sido tradicionalmente los más desarrollados a nivel internacional. En un primer momento el Departamento de Defensa de los EE.UU. (1985), cuya iniciativa dio lugar a los llamados Trusted Computer System Evaluation Criteria (TCSEC), conocidos como «Orange Book», de donde se derivaron otros criterios federales desarrollados por el National Institute of Standards and Technology (NIST) y la National Security Agency (NSA). Fueron los Federal Criteria for Information Technology Security.

Common Criteria Recognition Arrangement (CCRA)

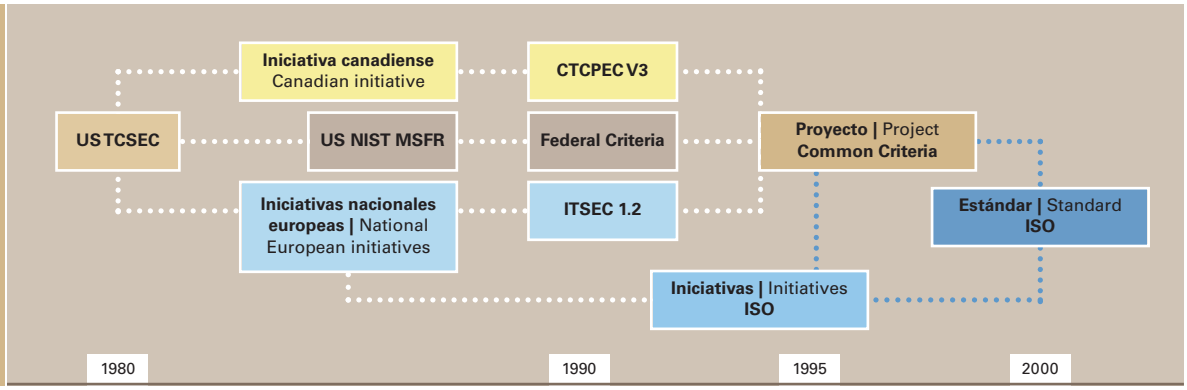
The OC/CCN is, since 2006, an issuing agency for CCRA certificates. The CCRA is an agreement for the international recognition of "functional" security on ICT products, and twenty-six countries are member (http://www.commoncriteriaportal.org). The certificate is the result of the analysis of products and systems, evaluating their functions or the functions aimed at providing security to the Target of Evaluation (TOE) itself.

Functional certification and evaluation focuses on what the TOE does and how it does it, and tries to determine whether there is any vulnerability in its own behavior that could cause a security problem, either due to an incorrect implementation of TOE functions, or because these functions are not effective enough to meet security objectives. Both the correction and the effectiveness of the TOE functions are evaluated. For example, a TOE that consists of a software program with an access control based on the user secret password (alphanumeric) could pose these security issues:

- Correction problem: the program development did not take into account the use of special and alphanumeric characters, and when the user introduces them, the function fails and allows unauthorized access to it.
- Effectiveness problem: the function is executed correctly, but is was designed to use only four characters of length, making it easier to execute brute force attacks in shorter periods of time than those proposed for TOE security.

Methods for evaluating functional security have traditionally been the most developed worldwide. Firstly (1985), the US Defense Department initiatives became in the development of the so-called Trusted Computer System Evaluation Criteria (TCSEC), known as "Orange Book", which gave rise

Evolución histórica de los criterios y métodos de evaluación
Historical evolution of evaluation methods and criteria



to other federal criteria developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA): the Federal Criteria for Information Technology Security.

In Europe, several nations also made their own developments, such as UK (CESG Memorandum Number 3, developed for government use, and the so-called "Green Book" to be used by commercial products) or Germany (Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems).

Several of these European nations joined their efforts in this regard, resulting in their own criteria and methods: the Information Technology Security Evaluation Criteria (ITSEC) in the early nineties. In this decade, the international CCRA project was initiated at an international level for the development of common criteria and methods at a global level: the Common Criteria for IT Security Evaluation (CC) and the Common Methodology for IT Security Evaluation (CEM). These criteria and methods have been the most widely spread and internationally recognized to date, and they are still under development. Two ISO standards were created in parallel and contain them directly: ISO/IEC 15408 and ISO/IEC 18045.

En Europa varias naciones hicieron también sus desarrollos propios, como por ejemplo Reino Unido (CESG Memorandum Number 3 desarrollado para uso gubernamental, y el llamado «Green Book» para uso por productos comerciales) o Alemania (Criteria for the Evaluation of Trustworthiness of Information Technology [IT] Systems).

Varias de estas naciones europeas unieron sus esfuerzos a este respecto dando lugar a unos criterios y métodos propios, los Information Technology Security Evaluation Criteria (ITSEC) a principios de los años noventa. En esta década se inició el proyecto CCRA a nivel internacional para el desarrollo de uno criterios y métodos comunes a nivel global: los Common Criteria for IT Security Evaluation (CC) y la Common Methodology for IT Security Evaluation (CEM). Estos criterios y métodos han sido los de más amplia difusión y reconocimiento internacional hasta la fecha, y continúan actualmente su desarrollo. En paralelo se crearon dos estándares ISO que los recogen directamente: el ISO/IEC 15408 y el ISO/IEC 18045.

SOGIS MRA

Mientras que el CCRA limita el reconocimiento mutuo a niveles de evaluación intermedios (hasta EAL4), en Europa se desarrolló y firmó el llamado SOGIS MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement) que busca el reconocimiento también para los más altos niveles de seguridad posibles (hasta EAL7), por ejemplo, el caso de las certificaciones de los productos tipo tarjeta inteligente como el pasaporte electrónico o el DNIe (EAL4+ ó EAL5+). Además este SOGIS MRA incluye la anterior norma ITSEC europea para todos sus niveles E1-E6.

El SOGIS MRA fue originalmente desarrollado a finales de los años noventa y tiene una directiva de la UE que lo respalda. Fue firmado por España en su inicio y durante el periodo 2008-2009 fue reactivado, con Alemania como secretaria del grupo, iniciándose contactos con los Esquemas europeos de certificación, entre ellos el OC/CCN. Durante esta reactivación se desarrolló un nuevo acuerdo actualizado, el SOGIS MRA v3. Tras su revisión técnica y jurídica, se procedió en febrero de 2010 a su firma por el Secretario de Estado Director del CNI como Director del Organismo de Certificación del CCN. En esta primera fase de adhesión al MRA v3, el esquema español se ha incorporado como emisor de certificados reconocidos hasta nivel EAL4.

Coincidiendo con la Presidencia española de turno del Consejo de Ministros de la Unión Europea, el CCN anunció en el TECNIMAP 2010 la incorporación del Esquema Nacional de Evaluación y Certificación de la Seguridad TIC a este acuerdo europeo SOGIS MRA v3 de reconocimiento de certificados.

La puesta en vigor de este acuerdo, así como la incorporación de España al mismo, es y será un factor clave de referencia a la hora de fijar los requisitos de garantías de seguridad para los productos que se adquieran para uso en la Administración española, conforme a los requisitos establecidos por el nuevo Esquema Nacional de Seguridad (ENS) que desarrolla los aspectos de seguridad de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

SOGIS MRA

While the CCRA limits mutual recognition to intermediate levels of evaluation (up to EAL4), the so-called SOGIS MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement), was developed and signed in Europe which looks for the recognition of highest security levels (up to EAL7 level). For example, the certification of smart card-type products, such as the electronic passport or DNIe (EAL4 + or EAL5 +). Furthermore, SOGIS MRA includes the former ITSEC European standard for all levels, E1-E6.

SOGIS MRA was originally developed in the late nineties and is supported by an EU directive. It was signed by Spain from the beginning.

During the period 2008-2009, it was reactivated with Germany as secretary of the group, initiating contacts with European certification schemes, including the OC/CCN. During this reactivation, a new updated agreement was developed, SOGIS MRA v3. After its technical and legal review, in February 2010, the Secretary of State Director of the CNI signed it as the Director of the CCN's Certification Body. In this first phase of adhesion to MRA v3, the Spanish Scheme has been incorporated as an issuer of qualified certificates up to EAL4 level.

Coinciding with the Spanish Presidency of the Council of Ministers of the European Union, the CCN announced in TECNIMAP 2010 the incorporation of the National Evaluation and Certification Scheme for IT security into this European SOGIS MRA v3 agreement.

The implementation of this agreement, and the incorporation of Spain into it, is and will be a key benchmark in setting the requirements for security assurances of security products that are purchased to be used in the Spanish Administration, in accordance with the requirements established in the new National Security Framework, which develops security aspects of Spanish Act 11/2007 on citizens' electronic access to public services.

Servicios de Certificación

El CCN realiza tres tipos de certificaciones en función de los aspectos de seguridad que se evalúen:

- Certificación Funcional de la seguridad de las Tecnologías de la Información. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información emite esta certificación funcional en base a criterios establecidos y reconocidos como estándar internacional: los llamados «Information Technology Security Evaluation Criteria (ITSEC)» y «Common Criteria for Information Technology Security Evaluation», estos últimos publicados también como norma ISO/IEC 15408. Esta certificación es la culminación de un proceso de evaluación de las funciones de seguridad de un producto o sistema (objeto de evaluación) que, siguiendo una metodología, también estándar, realiza un laboratorio independiente, acreditado y capacitado técnicamente para tal fin. Se trata de comprobar que el objeto de evaluación realiza correcta y eficazmente la funcionalidad de seguridad que se describe en su documentación. Tanto la acreditación de los laboratorios de evaluación como la certificación de los productos y sistemas se realizan de acuerdo a lo dispuesto en el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por la Orden PRE/2740/2007, de 19 de septiembre, y en los procedimientos propios del Esquema, todos públicos, establecidos por el OC.

- Certificación Criptológica. El CCN es el Organismo responsable de la elaboración del *Catálogo de Productos con Certificación Criptológica* que incluye los productos capaces de proteger la información nacional clasificada. De esta forma, tiene la consideración de cifrador nacional, con certificación Criptológica, aquel equipo de cifra que ha sido evaluado y ha obtenido dicha certificación del CCN.

  Para la obtención de este certificado es necesario que el producto disponga previamente de un certificado Common Criteria, cuyo informe técnico de evaluación será entregado al CCN. Posteriormente se realizará la evaluación criptológica, en la que se tiene en cuenta el análisis de los algoritmos de cifra, mecanismos de seguridad y el correcto funcionamiento del equipo, asignándole el máximo nivel de clasificación de la información que está autorizado a procesar.

Certification services

The National Cryptologic Centre is based on three types of certifications, depending on the security features evaluated:

- Functional certification of Information Technologies security. The Certification Body issues this functional certification in accordance with international standard criteria, the so-called "Information Technology Security Evaluation Criteria" (ITSEC) and "Common Criteria for Information Technology Security Evaluation", also published as the ISO/IEC 15408 regulation. This certification is the final step of an evaluation process for which the security functions of a product or system (objective of the evaluation) are evaluated, according to a methodology (also a standard), and is performed by an authorized and technically qualified independent laboratory. The objective is to check that the target being evaluated executes the security functions correctly and effectively as stated in the corresponding documentation. Both the laboratory accreditation evaluation and product/system certifications are done in accordance with the Evaluation and Certification Regulation of Information technologies Security and approved by the Order PRE/2740/2007, September 19th, and in the public procedures of the Scheme established by the Certification Body.

- Cryptology Certification. The CCN is the Organization responsible for creating the Catalogue of Products with Cryptologic Certification that includes products capable of protecting national classified information. This way, the evaluated encryption equipment that obtains the CCN's certification is considered as a national encryptor, and it obtains a cryptology certification.

  To obtain the certificate, the product must already have a Common Criteria certificate. The corresponding technical evaluation report is first delivered to the National Cryptologic Centre. Subsequently, the cryptology evaluation is carried out, during which the analysis of the encryption algorithms, security mechanisms and the proper functioning of the equipment is taken into account. The equipment is then assigned the maximum level of information classification for which it is authorized to handle.

Para cada producto con certificación criptológica se ha elaborado un procedimiento de empleo que es de obligado cumplimiento para mantener la aprobación para manejar información nacional clasificada hasta el máximo nivel de clasificación que se le haya dado al producto.

La política del CCN en esta materia es incrementar el uso de equipos de cifra nacionales certificados en los organismos de la Administración.

- Certificación TEMPEST. Al igual que sucede en otros países miembros de la OTAN y UE, las normas nacionales están basadas o se desarrollan para ser compatibles con las de estos organismos. En algunos casos, estas normas son particularizadas y extendidas para adecuarse a las necesidades propias de la Administración española, principalmente en lo relacionado con la evaluación de los equipos de cifra o la evaluación del riesgo presentado por instalaciones debido a su poca atenuación frente a las radiaciones indeseadas objeto del estudio TEMPEST. Estas normas permiten disponer de tres niveles diferentes de protección de los que derivan tres tipos de equipos/sistemas con diferentes grados de supresión de estas emisiones. Esta clasificación permite un uso racional de los medios sin reducir por ello los requisitos de seguridad necesarios.

  El CCN, como autoridad de certificación de seguridad de las Tecnologías de la Información en el ámbito EMSEC, ha participado activamente en el desarrollo de la normativa TEMPEST europea promovida por el Consejo de Seguridad de la Unión Europea de aplicación a todos los sistemas e instalaciones donde se procese información clasificada de la Unión Europea.

Every product with a cryptology certification has its own usage procedure which is mandatory to keep the authoritazon to handle national classified information up to the maximum level of classification given to the product.

The CCN policy on this matter is to increase the use of national encrypted equipment certified in Public Administration organizations.

- TEMPEST certification. As in other NATO member countries and other EU countries, the national regulations are designed to be compatible with regulations from these organizations. In some cases, these norms are extended to adapt to the needs of the Spanish Administration, especially in the evaluation of encryption equipment and risk assessment results that show undesired electromagnetic radiation in their facilities, this being the objective of the TEMPEST study.

  These norms make it possible to have three different levels of protection at their disposal, three types of equipment/systems with different levels to suppress the emissions deriving from them. This classification allows a rational use of the media without reducing the necessary security requirements.

  The CCN, as security certification authority for Information Technologies in EMSEC scope, has actively participated in the development of the TEMPEST regulation promoted by the EU Security Council which applies to all systems and installations where classified information of the European Union is being processed.

El CCN, como autoridad de certificación de seguridad de las Tecnologías de la Información en el ámbito EMSEC, ha participado activamente en el desarrollo de la normativa TEMPEST europea promovida por el Consejo de Seguridad de la Unión Europea. The CCN, as security certification authority for Information Technologies in EMSEC scope, has actively participated in the development of the TEMPEST regulation promoted by the EU Security Council

Evaluaciones de sistemas de apantallamiento
Evaluation of features for this type of shielding systems

TEMPEST evaluation models

Among the duties of the CCN one can find the evaluation of features for this type of shielding systems and the subsequent approval for their use.

ZONING EVALUATION

As in other NATO member countries, the CCN applies the ZONING Model for the identification of facilities and equipment that process classified information. This norm relates to premises attenuation evaluation and equipment classification depending on their levels of electromagnetic radiation, allow users to dispose of the necessary tools to carry out the correct installation of the environment without reducing security.

The CCN adapts this regulation in the guide CCN-STIC-152 "Facility ZONING, Evaluation and Classification".

During the past years, this activity has been widely increased thanks to the collaboration the CCN receives from accredited laboratories. These laboratories, which belong to the Ministry of Defense, are: the Laboratory of Engineers of the Army, which depends on the Ministry of Defence's General Infrastructure Department and the Air ForceTransmission Group. Both laboratories have evaluated and issued certifications for about 200 premises, and the CCN itself evaluated some other ones to be added to this amount.

The CCN is trying to promote the ZONING evaluation of equipment and systems, as it is the cheapest and fastest way to comply with the minimum requirements for electromagnetic security. In this sense, the Center has continued to develop the activity it initiated in 2007, extending the list of certified equipment and systems, which is published on CCN's web.

Modelos de evaluación TEMPEST

Entre las tareas del CCN se encuentra la evaluación de prestaciones de sistemas de apantallamiento y la posterior aprobación de los mismos para su uso.

EVALUACIÓN ZONING

Al igual que sucede en otros países de la OTAN, el CCN aplica el modelo ZONING para la caracterización tanto de instalaciones como de equipos que procesan información clasificada. Esta norma, establece diversos niveles en cuanto a la atenuación de locales, e igualmente clasifica la radiación electromagnética de los equipos o sistemas en otro conjunto de niveles que permitirán a los usuarios disponer de las herramientas necesarias para llevar a cabo la correcta instalación de los medios sin reducir la seguridad.

El CCN adapta esta normativa en la guía CCN-STIC-152 «Clasificación ZONING de locales».

Durante los últimos años, esta actividad se ha visto ampliamente incrementada gracias a la colaboración que el CCN recibe de los laboratorios acreditados para dichos trabajos. Estos laboratorios, pertenecientes al Ministerio de Defensa son el Laboratorio de Ingenieros del Ejército, dependiente de la Dirección General de Infraestructura del Ministerio de Defensa, y el Grupo de Transmisiones del Ejército del Aire. Se han realizado evaluaciones y generado los correspondientes certificados a cerca de 200 locales inspeccionados por ambos organismos, a los que se deben añadir los evaluados por el propio CCN.

Armarios apantallados
Shielded Cabinet

Plataforma de transporte aéreo militar A400M
Platform for the military air transport A400

En cuanto a la evaluación ZONING de equipos y sistemas, se trata de una de las actividades que el CCN está tratando de potenciar al ser en muchas ocasiones la forma más económica y rápida de poder cumplir con los requisitos mínimos de seguridad electromagnética. A este respecto se ha continuado con la actividad que viene desarrollando el Centro desde 2007 ampliando el listado con la clasificación de equipos y sistemas evaluados que son publicados en la página web del CCN para su consulta.

RECINTOS APANTALLADOS

En ocasiones, tras la evaluación ZONING de un local y de los equipos que están siendo utilizados se puede considerar que estos no cumplen con los requisitos mínimos exigibles para ser instalados en el mismo. En esas ocasiones deben barajarse soluciones alternativas como es la protección de un sistema completo mediante armarios apantallados, la adquisición de equipamiento certificado TEMPEST o la protección integral de un local.

Con la publicación de la norma CCN-STIC-153 «Evaluación y Clasificación de armarios apantallados», se establece el procedimiento de evaluación de prestaciones de este tipo de sistemas de apantallamiento así como para la obtención de una recomendación de uso por parte del CCN.

Estos años se han evaluado armarios de las empresas Pemac, S.L. y Equinsa Networking que se unen al catálogo de productos ya evaluados de estas empresas y de Sme, S.A. Por otra parte se han llevado a cabo medidas de Jaulas de Faraday para empresas privadas así como el asesoramiento sobre los requisitos que han de cumplir los organismos que las han adquirido.

SHIELDED ENCLOSURES

Sometimes, the ZONING evaluation for a premise and equipment reveals that they don't meet the minimum requirements to be installed. In those cases, some alternative options could be applied, such as the protection of a complete system through shielded cabinets the acquisition of certified TEMPEST equipment or the integral protection of a room.

The standard CCN-STIC-153 «Evaluation and Classification of Shielded Cabinet », establishes the process of evaluation for this type of shielding methods and the process to be followed to obtain usage recommendations by the CCN.

During past years, the CCN has performed evaluations of shielded cabinets for companies such as Pemac, S.L. and Equinsa Networking, which were added to the catalogue of already evaluated products of these companies and of Sme, S.A. Besides, shielding performance measurements have been implemented for private companies and the CCN advises these companies on how to meet mandatory requirements.

TEMPEST EVALUATION

In certain cases, an equipments must comply not only with the levels of radiation established by the ZONING regulation, but they must also meet special requirements that are feasible after the completeTEMPEST certification is performed. This is also the case for equipment that must be installed in platforms such as aircrafts, ships or tactical vehicles. Several organizations and companies have shown interest in the acquisition or development of thosei equipment.

Programa MRTT RAAF
MRTT RAAF Program

Avión de combate
europeo EF-2000
European combat
aircraft EF-2000

As a TEMPEST laboratory, the CCN has performed the evaluation of TEMPEST equipments manufactured by national companies such as Pemac, S.L. or Sme S.A., as well as several crypto device aimed for the protection of National Classified Information.

During 2009 and 2010, several products were certified: CRIPTOPER encryptor of Tecnobit, CRIPTO TOKEN USB of Datatech, data encryptor EP-430C or the multilevel system EP-830, of Epicom. The CCN has continued to take part in product certifications (for equipment and platforms) in several international programs, offering its support to the Armed Forces and private companies within the sector.

This way, and as a TEMPEST laboratory selected for the evaluation of the aircraft, it has continued to develop its activities aimed at the certification of the new platform for the military air transport A400M as well as it continued to monitortasks aimed at the TEMPEST evaluation of equipment and systems that will compound the platform, such as the audio management system AMS, of Tecnobit.

Other platforms, in which the CCN has supplied and supplies evaluation and assessment in the area of security and TEMPEST emanations, are the European combat aircraft EF-2000 or the programs for the development of Multi Role Tanker Transport aircraft for the Australian Air Force (MRTT RAAF Program) and British Air Force (FSTA Program). The CCN has insisted on establishing an accredited Laboratory in the Ministry of Defence, the mission of which is to perform TEMPEST evaluations at the same time it receives the required technical information.

EVALUACIÓN TEMPEST

En determinados casos, es posible que un equipo deba cumplir no sólo los niveles de radiación marcados de acuerdo a la normativa ZONING, sino que deben tener requisitos especiales que sólo son alcanzables tras un proceso de certificación TEMPEST completo. Este es también el caso de equipos que deban instalarse en plataformas como aviones, buques o vehículos tácticos. En este tiempo han sido varios los organismos y empresas que han mostrado su interés por la adquisición o desarrollo de este tipo de equipos.

Como laboratorio TEMPEST, el CCN ha llevado a cabo la evaluación de equipos TEMPEST fabricados por empresas nacionales como son Pemac, S.L. o Sme, S.A., así como diversos equipos de cifra para uso en la Administración que exigen un análisis exhaustivo por tratarse de equipos destinados a la protección de la información Clasificada Nacional.

Así, durante 2009 y 2010 se ha llevado a cabo la certificación, entre otros, del cifrador personal interoperable CRIPTOPER de Tecnobit, el CRIPTO TOKEN USB de Datatech, el cifrador de datos EP-430C o el sistema multinivel EP-830, éstos últimos de Epicom. El CCN ha proseguido con su participación en la certificación de productos (tanto equipos como plataformas) en distintos programas internacionales brindando su apoyo a las Fuerzas Armadas y a empresas privadas del sector.

De esta manera, y como laboratorio TEMPEST seleccionado para la evaluación del avión, se han continuado las actividades orientadas a la certificación de la nueva plataforma de transporte aéreo militar A400M así como el seguimiento de las tareas encaminadas a la evaluación TEMPEST de equipos y sistemas que compondrán la plataforma como es el sistema de gestión de audio AMS de la empresa Tecnobit.

Otras plataformas en las que el CCN ha aportado y aporta un continuo apoyo de evaluación y asesoramiento a la industria en el área de seguridad a emanaciones TEMPEST son el avión de combate europeo EF-2000 o los programas para el desarrollo de aviones de reabastecimiento en vuelo para las fuerza aérea australiana (Programa MRTT RAAF) y británica (Programa FSTA). Junto a estas actividades, el CCN ha proseguido en su empeño por establecer un laboratorio Acreditado en el Ministerio de Defensa cuya labor sea la evaluación TEMPEST y al que se proporcione la formación técnica necesaria.

Evaluación y Acreditación

ACREDITACIÓN DE LABORATORIOS

La acreditación del Organismo de Certificación requiere, como condición inicial, la verificación de la competencia técnica del mismo, conforme a la norma UNE-EN 17025, por una Entidad de Acreditación reconocida, como ENAC.

El OC requerirá para la acreditación de los laboratorios de evaluación de la seguridad de las Tecnologías de la Información el cumplimiento de los siguientes requisitos:

- Capacidad para la evaluación de la seguridad de las Tecnologías de la Información de productos, demostrada mediante acreditación de la competencia técnica en vigor, cuyo alcance incluya los criterios, métodos y normas de evaluación.
- Cumplimiento de los requisitos de la gestión de la seguridad. Requisitos de acreditación de laboratorios del Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
- El desarrollo de las evaluaciones de acuerdo a procedimientos que recojan las obligaciones de información y coordinación con el OC.

REQUISITOS PARA LA ACREDITACIÓN DE LABORATORIOS

La comprobación del cumplimiento de estos requisitos se realizará mediante el procedimiento de auditoría y seguimiento indicado en la regulación correspondiente. En todo caso, el alcance de la acreditación otorgada por el OC estará limitada por el alcance de la acreditación de la competencia técnica del laboratorio, y cualificada por el nivel de seguridad del mismo.

Salvo en los casos en que haya una compartimentación organizativa, de medios y procedimientos, aprobada por el OC, el laboratorio deberá cumplir con los requisitos de la gestión de la seguridad necesarios para la acreditación incluso en el desarrollo de aquellas evaluaciones cuyo objeto final no sea la certificación del producto evaluado por parte del OC.

Evaluation and accreditation

LABORATORIES ACCREDITATION

The accreditation by the Certification Bodyinitially requires the verification of its technical competence, in accordance with UNE-EN 17025 standard, by a recognized Entity of Authorization, such as ENAC. The Certification Body expects the fulfilment of the following requirements in order to authorise IT Security Evaluation Laboratories:

- The ability to evaluate the security of information technologyies products. This ability is verified through the accreditation of their technical competence,the extent of which includes evaluation criteria, methods and standards.
- Fulfilment of the requirements for Security Management. Accreditation requirements included in the Regulation on Security Evaluation and Certification of Information Technologies Regulation.
- Development of evaluations in accordance with the procedures that contain information and coordination obligations, towards the Certification Body.

REQUIREMENTS FOR THE ACCREDITATION OF LABORATORIES

The fulfilment of these requirements is verified through the audit and monitoring procedures. In any case, the extent of the accreditation issued by the Certfication Body is limited by the technical competence of the laboratory and is qualified according to its security level.

Except in cases in which there is a structural compartmentalisation of means and procedures approved by the OC, the laboratory shall comply with the necessary security requirements to obtain the accreditation, even in those cases in which the evaluation purpose is not to certify the product evaluated by the OC.

Relación de laboratorios acreditados en 2008-2010 | Accreditation of Laboratories 2008-2010

Laboratorio | Laboratory	**Acreditación** | Accreditation	**Resolución BOE** | BOE[1] Resolution
LGAI-APPLUS	Ampliación de alcance de la acreditación | Expansion of reach of accreditation. NORMA | STANDARD: Common Criteria 3.1. NIVEL DE GARANTÍA | GUARANTEE LEVEL: EAL1+ (ADV_FSP.4; ADV_TDS.3; ALC_CMS.4). NIVEL DE SEGURIDAD | SECURITY LEVEL: Productos No Clasificados | Unclassified products.	1A0/38033/2009, de 28 de enero
Applus	Ampliación de alcance de la acreditación | Expansion of reach of accreditation. NORMA | STANDARD: Common Criteria 3.1. NIVEL DE GARANTÍA | GUARANTEE LEVEL: EAL4+ (AVA_VAN.5; ADV_DVS.2) NIVEL DE SEGURIDAD | SECURITY LEVEL: Productos No Clasificados | Unclassified products.	1A0/38236/2009, de 31 de agosto
EPOCHE & ESPRI	Ampliación de alcance de la acreditación | Expansion of reach of accreditation NORMA | STANDARD: Common Criteria 3.1. NIVEL DE GARANTÍA | GUARANTEE LEVEL: EAL4+ (AVA_VAN.5; ALC_FLR.2; ALC_DVS.2). NIVEL DE SEGURIDAD | SECURITY LEVEL: Productos Clasificados | Classified products.	1A0/38113/2009, de 4 de mayo
EPOCHE & ESPRI		
INTA-CESTI	Ampliación de alcance de la acreditación | Expansion of reach of accreditation. NORMA | STANDARD: Common Criteria 3.1. NIVEL DE GARANTÍA | GUARANTEE LEVEL: EAL4+ (AVA_VAN.5; ALC_FLR.2) NIVEL DE SEGURIDAD | SECURITY LEVEL: Productos Clasificados | Classified products.	1A0/38264/2010, de 19 de noviembre
SECRETARIA DE ESTADO DE DEFENSA MINISTERIO DE DEFENSA Instituto Nacional de Técnica Aeroespacial		

[1] Spanish Official State Gazett

Certificación de productos

El OC certifica la seguridad de productos y sistemas de Tecnologías de la Información, según lo establecido en la Orden PRE/274/2007. Considerando, entre otras pruebas de la instrucción del procedimiento, los informes de evaluación emitidos por los laboratorios acreditados y realizados conforme a los criterios, métodos y normas de evaluación de la seguridad.

La certificación de la seguridad de un producto o sistema de las Tecnologías de la Información supone el reconocimiento de la veracidad de las propiedades de seguridad de la correspondiente Declaración de Seguridad.

La certificación de la seguridad de un producto o sistema no presupone sin embargo declaración de idoneidad de uso en cualquier escenario o ámbito de aplicación. Para valorar la idoneidad deberán tenerse en cuenta otras circunstancias, incluidas las restricciones establecidas en la Declaración de Seguridad para la correcta interpretación del certificado.

La certificación, una vez concedida, se mantiene de manera indefinida, salvo cambios en las condiciones que motivaron su concesión, tales como avances tecnológicos o aparición de vulnerabilidades explotables, incumplimiento de las condiciones de uso del certificado, cambios en el producto, o renuncia expresa del solicitante. Para mantener la vigencia de la certificación, el OC realizará de oficio las necesarias auditorías, inspecciones y análisis del producto, entorno y uso del certificado.

Products certification

The OC certifies the security of IT products and systems, according to the procedure set out in Chapter V. considering, among other evidence of institution of the procedure, the assessment reports issued by authorized laboratories and conducted in accordance with the criteria, methods and standards established by Chapter VI for the evaluation of security.

The security certification of a product or system implies the recognition of a variety of characteristics and properties contained in the Security Statement.

However, the security certification of a product or system does not imply the suitability acknowledgement for every scenario or implementation scope of application. Other circumstances should be taken into account in order to assess its suitability, such as the restrictions set forth in the Security Statement for the correct interpretation of the certificate.

The certification, once granted, is maintained indefinitely, unless there are changes in the conditions that led to its issuance, such as technological advances or the development of exploitable vulnerabilities, violation of license conditions, changes in the product, or in case there is an express waiver by the applicant. To monitor the validity period of the certification, the OC will automatically perform the necessary audits, inspections and analysis on the product and the environment.

La certificación de la seguridad de un producto o sistema de las Tecnologías de la Información supone el reconocimiento de la veracidad de las propiedades de seguridad de la correspondiente Declaración de Seguridad. The security certification of a product or system implies the recognition of a variety of characteristics and properties contained in the Security Statement.

Relación de productos certificados 2008-2010 | List of certified products 2008-2010

Producto | Product	**Solicitante** | Applicant	**Resolución BOE** | BOE[1] Resolution
ADVANTIS CRYPTO 3.1	SERMEPA	1A0/38248/2008, de 29 de octubre
ASF 4.1.5	TB SOLUTIONS	1A0/38072/2008, de 9 de abril
EF2000 IGS 2.1	EADS-CASA	1A0/38030/2008, de 25 de enero
EF2000 GSS 4.1	EADS-CASA	1A0/38179/2008, de 23 de junio
EP430C 1.31.18	EPICOM	1A0/38211/2008, de 1 de septiembre
EP430D 1.34.31	EPICOM	1A0/38049/2010, de 24 de febrero
LOGICA 2.1	ICA	1A0/38212/2009, de 20 de agosto
EP430S 1.26.40	EPICOM	1A0/38225/2008, de 29 de septiembre
EP830 1.03 rev.13	EPICOM	1A0/38199/2008, de 5 de agosto
BITÁCORA 4.0.2	S21SEC	1A0/38269/2008, de 29 de diciembre
Ms SDK for Open XML Formats, OpenXMLSDK.msi 1.0	MICROSOFT	1A0/38205/2009, de 28 de julio
SVS (SECUWARE VIRTUAL SYSTEM) 4.1.0.276	SECUWARE	1A0/38251/2008, de 10 de noviembre
SOS (SECURITY OPERATING SYSTEM) 4.1.0.276	SECUWARE	1A0/38252/2008, de 10 de noviembre
EF2000 OGSE-IGS 3.1	EADS-CASA	1A0/38103/2010, de 11 de marzo
SIST. ELEC. DE ID. AUT. DE CONTENEDORES POR RFID 1.0	DISTROMEL	1A0/38108/2009, de 17 de abril
EP430DE 1.03 rev.10	EPICOM	1A0/38209/2010, de 20 de agosto
EF2000 GSS 4.1 SP	EADS-CASA	1A0/38265/2008, de 27 de noviembre
SONY RC SMARTCARD RC-S251/So2 1.0	SONY	1A0/38246/2009, de 3 de septiembre
PP DNI-e SCVA TIPO 1 EAL1 2.0	INTECO	1A0/38066/2009, de 23 de febrero
PP DNI-e SCVA TIPO 1 EAL3 2.0	INTECO	1A0/38067/2009, de 23 de febrero
PP DNI-e SCVA TIPO 2 EAL1, 2.0	INTECO	1A0/38068/2009, de 23 de febrero
PP DNI-e SCVA TIPO 2 EAL3 2.0	INTECO	1A0/38069/2009, de 23 de febrero
KEYONE 2.1 ACTUALIZADO	SAFELAYER	1A0/38142/2009, de 7 de mayo
KEYONE 3.0 ACTUALIZADO	SAFELAYER	1A0/38213/2009, de 12 de agosto
AP.DESCARGA DE DAT. DEL TACÓGRAFO DIGITAL 5.0	FNMT-RCM	1A0/38235/2009, de 2 de septiembre
CRYPTOSEC+FW PKCS#11 1.0	REALIA TECH	1A0/38208/2010, de 25 de agosto
TRUSTEDX, 3.0.09S2R1_T	SAFELAYER	1A0/38215/2010, de 27 de agosto
EF2000 GSS 4.1.1	EADS-CASA	1A0/38141/2009, de 29 de mayo
KONA26CC 1.1	KEBT	1A0/38211/2010, de 16 de agosto
CRYPTO TOKEN USB TK02S1.48	DATATECH	1A0/38040/2010, de 12 de febrero
ERASE-IT LOOP 1.73	RECOVERY LABS	1A0/38210/2010, de 17 de agosto
PROCESA ENGINE 1.7.3	MNEMO	1A0/38212/2010, de 20 de agosto
BORRADO SEGURO ANOVA 1.0	ANOVA IT CONSULT	1A0/38139/2010, de 19 de abril
EF2000 GSS 4.2	EADS-CASA	1A0/38289/2009, de 30 de noviembre
AUTHENTEST 1.2.6	AUTHENWARE CORP	1A0/38207/2010, de 18 de agosto
SIAVAL MÓDULO CRYPTO 6.2.1	SIA	1A0/38214/2010, de 27 de agosto
EF2000 GSS 5.0	EADS-CASA	1A0/38281/2010, de 30 de noviembre

[1] Spanish Official State Gazett

Durante los últimos años, el Centro Criptológico Nacional ha continuado dando a conocer sus competencias derivadas del RD 421/2004, en materia de seguridad de las Tecnologías de la Información, a diversas instituciones y organismos de la Administración General, autonómica o local, al tiempo que ha mantenido las relaciones de cooperación y coordinación necesarias para el mejor cumplimiento de sus misiones.

De igual modo, y en el plano internacional, tal y como señala el citado RD, ha mantenido o ampliado las necesarias relaciones y acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

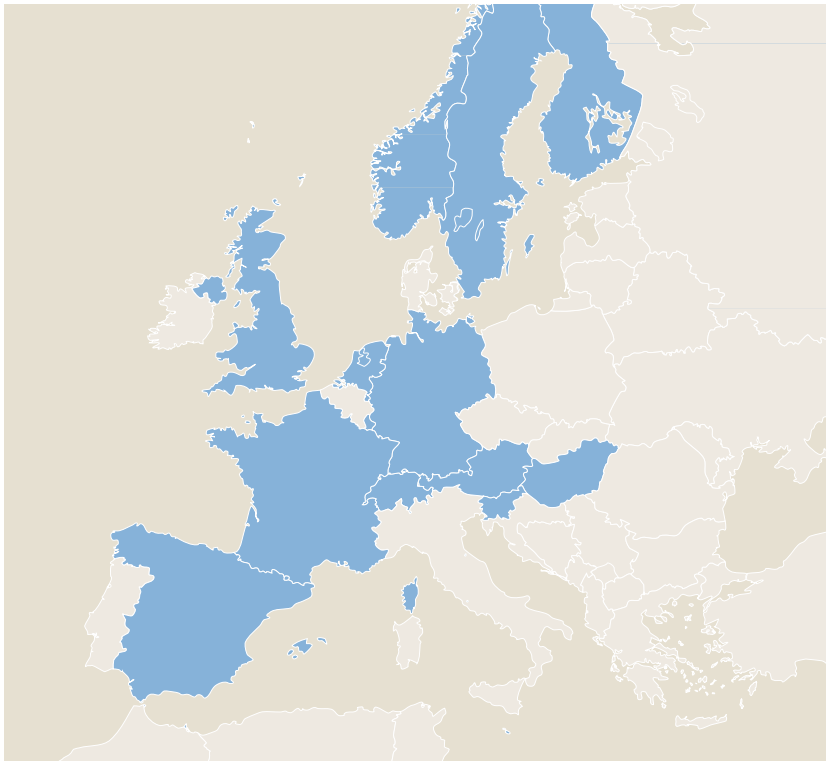
Presencia internacional

El CCN participa de forma activa en todos los organismos y foros internacionales de especial relevancia (particularmente los creados por la OTAN y la Unión Europea). Entre otros, destacan los siguientes:

In recent years, the National Cryptologic Centre has continued to raise awareness of their responsibilities, which are determined by Royal Decree 421/2004, on ICT security among different institutions and agencies from the General, Regional or Local Administration, at the same time it has maintained relationships of cooperation and coordination, where appropriate, to best fulfill its missions. Similarly, and at at international level, as stated by the RD, it has maintained or expanded its relationships and agreements with similar organizations in other countries for the development of these functions.

International presence

The CCN takes part in all organizations and international forums of special relevance (especially those from NATO and the EU), such as:



Miembros del European Government CERTs (EGC) Group
European Government CERTs (EGC) Group members

Participación del CCN en organismos y foros internacionales
Participation of the CCN in international organizations and forums

Organización | Organization	**Comisión-grupo** | Commission-group
OTAN | NATO	S/C4 Information Assurance & Cyber Defence y sus grupos de trabajo S/C4 Information Assurance & Cyber Defence and its INFOSEC policy working group
	Panel de Acreditación | Accreditation panel
	Grupo de trabajo nº1 sobre Information Assurance del Comité de Seguridad (AC/35 – WG/1). Group of work No.1 about Information Assurance for the Security Committee (AC/35 – WG/1)
	NATO Security Risk Assessment Group
	Grupo de Trabajo de Respuesta a Incidentes de OTAN -– NCIRC Working Group on response to NATO Incidents
	Grupos de Trabajo sobre Interoperabilidad Cripto | Working Group on Crypto interoperability: SCIP TF (Secure Communications Interoperability Protocol Task Force), NSG (NINE Steering Group), NCITF (NATO Crypto Interoperability Task Force)
	NATO CWID (Coalition Warrior Interoperability Demonstration)
OTAN-MULTINACIONAL NATO-MULTINATIONAL	International Interoperability Control Working Group IICWG (grupo internacional definición especificación protocolo interoperabilidad cripto SCIP) International Interoperability Control Working Group IICWG international group for crypto interoperability protocol SCIP
	Networking and Infomation Infraestructura (NII) Internet Protocol Specification Working Group - NISWG, grupo internacional definición especificación interoperabilidad cripto a nivel red (NINE: NII IP Network Encryption) Networking and Information Infrastructure (NII) Internet Protocol Specification Working Group – NISWG, international group crypto interoperability at network level (NINE: NII IP Network Encryption)
	STWG (Security Technical Working Group) de OCCAR: SDR (Software Defined Radio) dentro del programa ESSOR STWG (Security Technical Working Group) of OCCAR: SDR (Software Defined Radio) within the ESSOR program
UE | EU	Comité INFOSEC del Consejo de la Unión Europea INFOSEC Committee of the EU Council
	Panel de acreditación combinado (C-SAP) UE EU Combined accreditation panel (C-SAP) EU
	Paneles TEMPEST de la UE EU TEMPEST panels
	ENISA (European Network & Information Security Agency) ENISA (European Network & Information Security Agency))
PROGRAMA A400M PROGRAM A400M	Diferentes paneles del avión europeo de transporte A400M Different panels for the European transport aircraft A400M
EF2000	Diferentes grupos del EF2000/TCG (Grupo TEMPEST-COMSEC) Different groups of EF2000/TCG (TEMPEST-COMSEC group)
ESA	Comité INFOSEC para la protección de Información Clasificada de los sistemas de la Agencia Europea del Espacio INFOSEC committee for the protection of classified information from the systems of the European Agency of the Space
GALILEO	Diferentes comités y paneles de seguridad Different committees and panels
MULTINACIONAL MULTINATIONAL	Diferentes comités Common Criteria Different Common Criteria committees
	Grupos Internacionales de Equipos de Respuesta a Incidentes: FIRST, TF-CSIRT, CERT/CC International Groups of Incident Response Teams: FIRST, TF-CISRT, CERT/CC
	EGC Group (European Government CERTs)
	APWG (Anti-Phishing Working Group)
	Common Criteria Recognition Arrangement (CCRA): CCMB, CCDB, CCES, CCMC
	SOGIS MRA: MC, JIWG, ISCI WG1, JHAS, JTEMS

Relaciones nacionales

En el plano nacional, y en el ejercicio de sus funciones, el CCN ha mantenido una estrecha relación con organismos públicos y privados, además de contar con una presencia destacada en los principales foros del sector.

Entre otros, el CCN forma parte de los siguientes grupos de trabajo:

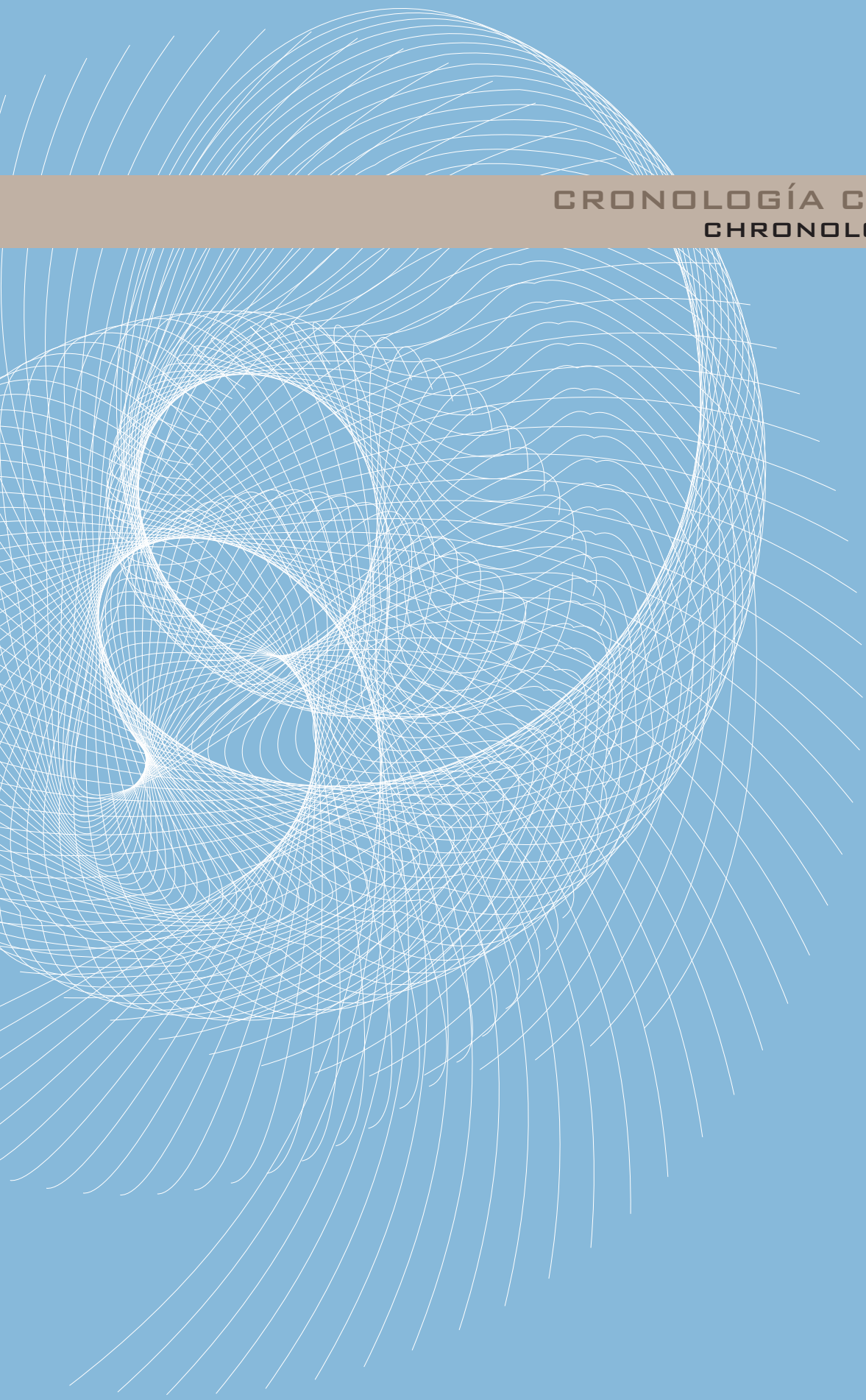
National relations

At national level, and in the performance of its duties, the CCN has maintained a close relationship with public and private organizations, besides having a significant presence in key industry forums.

Among others, the CCN takes part in the following working groups:

Participación del CCN en organismos y foros nacionales
CCN participation in National forums and organizations

Organización | Organization	**Comisión-grupo** | Commission-group
Ministerio de Política Territorial y Administración Pública Ministry of Territorial Policy and Public Administration	Consejo Superior de Administración Electrónica Superior Council of Electronic Administration
	Comisión Permanente del Consejo Superior para la Administración Electrónica y sus grupos dependientes Permanent commission for the Superior Council of Electronic Administration
	Grupos de trabajo sobre comunicaciones electrónicas seguras; transposición de la directiva europea de medios de pago (SEPA), identificación y autenticación y servicios WEB de la Administración | Working groups on secure electronic communication; transposing of the European Payment Directive (SEPA), identification and authentication and Web Administration services
	Grupo de Trabajo del Esquema Nacional Seguridad Working group for National Security Framework
Ministerio de Defensa Ministry of Defense	Grupos de trabajo INFOSEC y Cripto INFOSEC and Crypto working group
	Grupo de Trabajo sobre Seguridad de la Información y sobre cifra del Comité CIS de las Fuerzas Armadas (COMCISFAS) Working Group on Information Security and encryption of CIS Committee for the Armed Forces (COMCISFAS)
	Grupo Técnico C3 OTAN | NATO C3 Technical group
	Grupo de Trabajo de Apoyo al Sistema de Mando y Control Militar | Working Group of Support to the Military Command and Control System
	Grupo de Trabajo sobre Comunicaciones Tácticas Working Group on Tactical Communications
	Jornadas INFOSEC del EMAD y de Equipos de Inspección INFOSEC Conference for EMAD and Inspection Equipment
Ministerio de Industria Turismo y Comercio Ministry of Industry, Tourism and Commerce	Grupos de trabajo de los proyecto Rescata, Seguridad y Confianza, usabilidad del DNIe | Working Group: Rescata Security and Confidence project and Electronic Nationa ID (DNIe) usability
	Grupo de trabajo de INTECO | INTECO working group
Ministerio del Interior Ministry of the Interior	Grupo de Trabajo sobre DNI electrónico con la Dirección General de la Policía | Working Group on electronic National ID with Police Headquarters
	Grupo de Trabajo de Infraestructuras Críticas con la Secretaría de Estado de Seguridad | Working Group for Critical Infrastructures with the State Security Secretariat
Federación Española de Municipios y Provincias	Acuerdo de colaboración en materia de seguridad de la Información en los entidades locales | Collaboration Agreement on Information Security for local entities
Junta de Andalucía	Convenio de colaboración para el Impulso de la Sociedad de la Información | Collaboration agreement for the Promotion of the Information Society
Generalitat Valenciana	Convenio de colaboración con el CSIRT-CV en el marco de la Respuesta a Incidentes | Collaboration agreement with CSIRT-CV within an Incident Response framework
AENOR	Subcomités de seguridad TIC e identificación biométrica ICT security subcommittee and biometric identification
CSIRT.es	Grupo de Trabajo de CERT nacionales Working Group of National CERTs
Foro ABUSES	Grupo de Trabajo con Proveedores de Servicio de Internet (ISP) Working group with Internet Service Providers (ISP)
National Coalition Warrior Interoperability Demonstration	Demostraciones de tecnologías de carácter militar organizadas anualmente | Annual technological demonstrations of military nature



Año 2008

Enero

Inicio por parte del CCN-CERT del Sistema de Alerta Temprana de la Red SARA, en colaboración con el Ministerio de Administraciones Públicas (hoy Ministerio de la Política Territorial y Administración Pública).

Febrero

- El CCN-CERT se acredita en Trusted Introducer, principal foro europeo de Respuesta a Incidentes, donde compartir objetivos, ideas e información sobre seguridad informática.
- Acuerdo del CNI y Microsoft que permite al CCN-CERT unirse al programa SCP (Security Cooperation Program), un grupo de organismos públicos que cooperan de forma estrecha con Microsoft para prevenir, anticipar y mitigar los efectos de incidentes y ataques a los sistemas de la Administración.

Abril

Se celebra en Barcelona, del 16 al 18 de abril, el IX encuentro del grupo de trabajo de Capacidad de Respuesta a Incidentes de Seguridad TIC de la OTAN (NCIRC) organizado por el CCN, acogió a más de 180 especialistas en seguridad procedentes de los 26 países miembros de la Organización.

Junio

Se crea e imparte al personal de la Administración Pública el I Curso STIC - Common Criteria, dentro de los cursos específicos de Gestión de Seguridad. Su finalidad es proporcionar los conocimientos necesarios de la normativa Common Criteria en la que se basa la actividad central del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC.

Julio

El CCN presenta el Equipo de Respuesta ante Incidentes de Seguridad (CCN-CERT) y sus servicios a los responsables de seguridad de las tres administraciones públicas con presencia en Aragón (general, autonómica y local), en la sede del Departamento de Tecnología, Ciencia y Universidad del Gobierno de Aragón, en Zaragoza.

Septiembre

Creación del I Curso STIC - Búsqueda de Evidencias y Control de Integridad, destinado a ofrecer los conocimientos necesarios para que, realizando un reconocimiento previo de un Sistema de las TIC, se puedan encontrar rastros y evidencias de un ataque o infección.

Year 2008

January

Start of the Early Warning System of the SARA network by CCN-CERT, in collaboration with the Ministry of Public Administrations (today's Ministry of Territorial Policy and Public Administration)

February

- CCN-CERT is accredited in Trusted Introducer, the main European forum for Incident Response, where organizations exchange ideas and information on security.
- Agreement between the CNI and Microsoft that allows the CCN-CERT to join the SCP program (Security Cooperation Program), a group of public organizations that closely cooperate with Microsoft to prevent, anticipate and mitigate the impact of incidents and attacks against the Administration.

April

IX meeting for the working group NATO's Computer Incident Response Capability (NCIRC) was held in Barcelona, from the 16th to the 18th of April, and was attended by more than 180 security specialists coming from the 26 member countries of the Organization.

June

Development and delivery of the 1st STIC-Common Criteria Course for Public Administration, within specific courses on Security Management. Its purpose is to provide the knowledge required from Common Criteria regulation, which is the basis of the main activity of the National Evaluation and Security Certification Scheme for ICT.

July

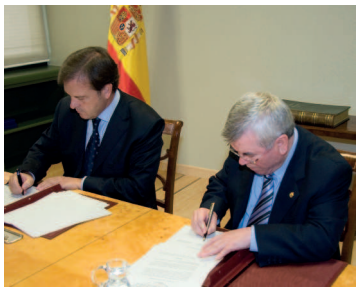
CCN presents CCN-CERT and its services to security managers within the three public administrations with presence in Aragón (General, Regional and Local), at the headquarters of the Department of Technology, Science and University of Aragón, in Zaragoza.

September

Creation of 1st STIC course - Search for Evidence and Integrity Control, aimed at providing the knowledge necessary to find traces and evidence of an attack or infection after executing a preliminary recognition of an ICT system.

El CCN-CERT es galardonado como «Mejor Servicio de Seguridad TIC del Año» por la revista Red Seguridad | The CCN-CERT has been named "Best ICT Security Service of the Year" by the magazine Red Seguridad

El Presidente de la FEMP, Pedro Castro, y el Secretario de Estado Director del Centro Nacional de Inteligencia (CNI) y Director del Centro Criptológico Nacional (CCN), Alberto Saiz, firman un convenio de colaboración | The President of FEMP, Pedro Castro, and the Secretary of State Director of the National Centre of Intelligence (CNI) and Director of the National Cryptologic Centre (CCN), Alberto Saiz, have signed a collaboration agreement



October

- CCN Conference, in collaboration with the Consejería de Administración Autonómica de la Junta de Castilla y León, is held in Valladolid in order to introduce the CCN-CERT services and raise awareness on the importance of preserving Security in the Government Systems.
- Attendance to de SCIP interoperability experimentation session at the NC3A facilities, The Hague, The Netherlands. Successfully tested interoperability between Tecnobit Criptoper SCIP implementation, General Dynamics´s Sectéra Wireline Terminal (SWT) and Rohde & Schwarz´s Elcrodat 5-4 over IP/Wifi networks.

November

- The 2nd STIC CCN-CERT conference is held in Madrid, and is attended by over 170 ICT security officers from Spanish public administrations.
- The National Cryptologic Center and the Department of Justice and Public Administrations of the Generalitat Valenciana jointly present in Valencia their respective Incident Response Teams: CCN-CERT and CSIRT-CV.
- CCN-CERT is awarded as Best ICT Security Service of the Year by the magazine "Network Security" in its Third Edition of Trophies for ICT Security, in recognition of its efforts to ensure the security on government systems and networks and therefore, citizens.

December

- The President of FEMP, Pedro Castro, the Secretary of State Director of the National Centre of Intelligence (CNI) and the Director of the National Cryptologic Centre (CCN), Alberto Saiz, signed a cooperation agreement aimed at promoting security within the framework of development of Information Society, through the exchange of information, the specialized training and the development of technological projects.
- Release, within series 400 of different guidelines about the new versions of PILAR tool, as well as «guide CCN-STIC 491 on Iris Biometric Devices" and Guide 502: Client Windows Security. Browser and e-mail.

Octubre

- Jornada del CCN, en colaboración con la Consejería de Administración Autonómica de la Junta de Castilla y León, en Valladolid, para presentar los servicios del CCN-CERT y concienciar de la importancia de preservar la Seguridad en los Sistemas de la Administración.
- Asistencia a la sesión de interoperabilidad SCIP celebrada en la sede de la NC3A en la Haya, Países Bajos. Se prueba con éxito la interoperabilidad entre implementación SCIP Criptoper de la empresa Tecnobit y los productos Sectéra Wireline Terminal (SWT) de General Dynamics y Elcrodat 5-4 de Rohde & Schwarz sobre redes IP/Wifi.

Noviembre

- Se celebra en Madrid la II Jornada STIC CCN-CERT, a la que asisten más de 170 responsables de seguridad TIC de las distintas administraciones públicas españolas.
- El Centro Criptológico Nacional y la Conselleria de Justicia y Administraciones Públicas de la Generalitat Valenciana presentan conjuntamente en Valencia los respectivos Equipos de Respuesta ante Incidentes de Seguridad de la Información: CCN-CERT y CSRIT.CV.
- El CCN-CERT es galardonado como «Mejor Servicio de Seguridad TIC del Año» por la revista Red Seguridad en su III Edición de Trofeos de la Seguridad TIC en su esfuerzo por garantizar la seguridad de los sistemas y redes de la Administración pública y, por ende, a los ciudadanos.

Diciembre

- El Presidente de la FEMP, Pedro Castro, y el Secretario de Estado Director del Centro Nacional de Inteligencia (CNI) y Director del Centro Criptológico Nacional (CCN), Alberto Saiz, firman un convenio de colaboración que tiene por objeto impulsar la seguridad en el marco del desarrollo de la Sociedad de la Información, mediante el intercambio de información, la formación especializada y el desarrollo de proyectos tecnológicos.
- Publicación, dentro de la serie 400, de diferentes Guías sobre las nuevas versiones de la Herramienta PILAR, así como la «Guía CCN-STIC 491 de Dispositivos Biométricos de Iris» y la Guía 502 - Seguridad en Aplicaciones Cliente. Navegador y Correo Electrónico.

Año 2009

Enero

- El CCN-CERT, como CERT gubernamental español, ingresa en el European Government CERTs (EGC) Group, la organización que reúne a los principales CERTs gubernamentales en Europa.
- Primera edición del Informe de Amenazas y Tendencias elaborado por el CCN-CERT en el que se recogen los principales riesgos y amenazas del año anterior y se hace una previsión para el año en curso.
- Aprobación para manejar información nacional clasificada con Criptoper CMAP V.1.2.
- Se elaboran y distribuyen 14 nuevas Guías de Seguridad CCN-STIC, centradas en diversos aspectos: CO-DRES-POS Pequeñas Redes, Inspección STIC, Seguridad en Sistemas Multifunción, Requisitos de Seguridad en Entornos y Aplicaciones Web o Seguridad en Voz sobre IP.

Febrero

- Demostración CWID 2009:Terminal seguro telefónico (Mossec SDM).
- Publicación de la Guía 153 - Evaluación y Clasificación de Armarios Apantallados.

Marzo

- Participación en el Grupo de Trabajo de Protección de Infraestructuras Críticas, coordinado por el Centro Nacional de Infraestructuras Críticas, (CNPIC), al que apoya en todo lo relativo a las IC de la Información.
- Aprobación para manejar información nacional clasificada con Criptoper SCAP V.1.2.2.
- Demostración CWID 2009: Cifrador IP EP430DE (Epicom), Herramienta de control de acceso y cifrado PC (Alcatel Lucent).

Abril

Implantación en el portal CCN-CERT de un mecanismo de autenticación basado en el DNI electrónico, que permite acreditar la identidad de los usuarios y asegurar la procedencia y la integridad de los mensajes intercambiados.

Mayo

El Centro Criptológico Nacional (CCN) pone a disposición de las distintas administraciones públicas 7 nuevas guías, incluidas en sus Series CCN-STIC, con las que mejorar los requisitos de seguridad exigibles en los sistemas de información y comunicaciones de la Administración.

Year 2009

January

- CCN-CERT, as the Spanish governmental CERT, joins the European Government CERTs (EGC) Group, the organization that brings together the main governmental CERTs in Europe.
- Release of the First Edition ofThreat Reports developed by the CCN-CERT, which describe the main risks and threats of previous year and includes predictions for the current year.
- Approval to handle national classified information with Criptoper CMAP V.1.2.
- 14 Drafting of new Security CCN-STIC guides, regarding several aspects: CO-DRES-POS Small Networks; Security in Multifunction Systems; Security Requirements in Environment and Web Applications or Security on Voice Over IP.

February

- CWID 2009 Demonstration: secure telephone terminal (Mossec SDM).
- Publication of guide 153 – Evaluation and Classification of Screened Rooms.

March

- Participation in the Working Group for the Protection of Critical Infrastructures, coordinated by the National Centre of Critical Infrastructures, (CNPIC), which receives our support in everything related to ICT Information.
- Approval to handle national classified information with Criptoper SCAP V.1.2.2.
- CWID 2009 demonstration: cypher IP EP430DE (Epicom), tool for the control of access and PC encryption (Alcatel Lucent).

April

Implementation in the CCN-CERT portal of an authentication mechanism based on the Electronic National ID (DNIe), which allows to verify the identity of users and the source and integrity of exchanged messages.

May

CCN provides public administrations with 7 new guides, included in its CCN-STIC series, aimed at improving security requirements for the Information and Communication system of the Administration.

Junio

- Desarrollo del servicio de Análisis de Portales Web Administración, a través del que se analiza y descarga el contenido, detectando automáticamente infección por código dañino y/o detección de vínculos a páginas externas (servidores *malware*).
- Publicación Guía - 434 Herramientas para el Análisis de Ficheros de Logs.

Septiembre

- Implantación en el portal del CCN-CERT de un sistema en línea de análisis de código dañino bajo demanda. El Sistema Multiantivirus (MAV) permite analizar todo tipo de código, haciendo uso de múltiples motores antivirus, actualizados en tiempo real.
- Presentación en Toledo de los servicios del CCN-CERT a todos los responsables de la Administración pública con presencia en Castilla-La Mancha.

Octubre

- Nuevo Curso On-Line de Seguridad de la Información, implementado en una nueva plataforma e-learning del CCN-CERT (curso informativo y de concienciación: Seguridad de las Tecnologías de la Información y las Comunicaciones en el que se ofrece una visión global de la Seguridad TIC y cuyo contenido está basado en la Guía CCN-STIC 400).
- Aprobación para manejar información nacional clasificada con Criptoper SCAP Procif V.3.0.
- Aprobación para manejar información nacional clasificada con Criptoper CMAP Procif V.3.0.
- Participación en el I Ejercicio de Ciberdefensa de las Fuerzas Armadas Españolas (FAS)
- Asistencia a la sesión de interoperabilidad SCIP celebrada en la sede de la NC3A en la Haya, Países Bajos. Se prueba con éxito la interoperabilidad entre implementación SCIP Criptoper de la empresa Tecnobit y los productos SWT y Edge de General Dynamics, sobre redes GSM, red telefónica básica e Iridium.

Noviembre

- El CCN-CERT participa en el equipo español participante en el International Cyber Defence Workshop organizado por el Gobierno de Estados Unidos.
- Participación del CCN-CERT en el Ejercicio de Ciberdefensa de la OTAN.

June

- Development of the analysis service for the Administration's web portals, which analyses and downloads the content, automatically detecting infections caused by malicious code and/or links to external webs (malware services).
- Release of Guide 434-Tools for log files analysis.

September

- Implementation in the CCN-CERT portal of an online analysis system for malicious code which works under request. The Multiantivirus System (MAV) allows the analysis of all type of codes, using multiple antivirus engines, which are updated in real time.
- Presentation of CCN-CERT services in Toledo to every official Public Administration with presence in Castilla-La Mancha.

October

- New online course on Information Security, implemented on a new e-learning platform of the CCN-CERT (Informative and Awareness course: ICT Security, which offers a global vision of ICT security. Its content is based on the CCN-STIC 400 guide.
- Approval to handle national classified information with Criptoper SCAP Procif V.3.0.
- Approval to handle national classified information with Criptoper CMAP Procif V.3.0.
- Participation in the 1st Cyberdefense Exercise of the Spanish Armed Forces.
- Attendance to de SCIP interoperability experimentation session at the NC3A facilities, The Hague, The Netherlands. Successfull tested interoperability between Tecnobit Criptoper SCIP implementation, General Dynamics´s SWT and General Dynamics´s Edge over GSM, PSTN and Iridium networks.

November

- The CCN-CERT takes part in the Spanish team within the International Cyber Defense Workshop, organized by United States.
- Participation of CCN-CERT in NATO's Cyberdefense Exercise.

Diciembre

- Organización de la III Jornada STIC del CCN-CERT en Madrid, con la asistencia de más de trescientos responsables de seguridad TIC de las diferentes administraciones públicas, provenientes de toda España.
- Presentación en Santiago de Compostela del CCN-CERT y sus servicios a los responsables de seguridad TIC de la Administración Pública (general, autonómica y local) con presencia en Galicia.
- El Sistema de Alerta Temprana de SARA, tras diversas incorporaciones, cierra el año con 23 sondas de recolección desplegadas (incluyendo los 17 Ministerios y otros cinco organismos públicos). Así, durante el año 2009 este sistema recibió y analizó más de un millón y medio de eventos recogidos de las distintas fuentes y organismos.
- Continuación de los trabajos de evaluación y certificación TEMPEST de equipos informáticos y de comunicaciones, tanto para Organismos de la Administración como para empresas fabricantes de equipos. Se continúan las misiones asignadas en diferentes programas de la industria nacional, principalmente en la evaluación y certificación TEMPEST de aviones para reabastecimiento en vuelo que la empresa AIRBUS MILITARY ha estado desarrollando. Se evalúa el primer avión A330-200 comercial, como paso previo a la modificación del mismo para misiones militares.
- Concluye el año con un total de 24 evaluaciones correspondientes a equipos y sistemas comerciales de Certificación ZONING. De igual modo, se certifican más de cien locales evaluados.

December

- Organization of the 3rd CCN-CERT STIC Conference in Madrid, attended by more than three hundred ICT officiers from public administrations, coming from all parts of Spain.
- Presentation in Santiago de Compostela of the CCN-CERT and its services to ICT officials from Public Administration (general, regional and local) with presence in Galicia.
- The Early Warning System of SARA, after several incorporations, ended the year with 23 collection sensors (including 17 ministries and other five public organizations). Thus, during 2009, the system analyzed more than one and a half million events reported by different sources and organizations.
- Further TEMPEST evaluation and certifications of computer and communications equipment, for both government agencies and equipment manufacturers. Continuation of the missions assigned in different programs, mainly in TEMPEST evaluation and certification of aircrafts with in-flight refueling that the company AIRBUS MILITARY has been developing. It evaluates the first A330-200 commercial aircraft, prior to its modification for military missions.
- 2009 concludes with a total of 24 evaluations for ZONING certification of commercial systems and equipment. More than a hundred premises were evaluated and certified.

Convenio de colaboración entre el CNI y la Junta de Andalucía para el impulso de la Seguridad de la Información
Cooperation agreement between the CNI and the Junta de Andalucía for the promotion of Information Security

Año 2010

Year 2010

January

- Release of Royal Decree 3/2010 of January 8, which regulates the National Security Framework within Public Administration. CCN actively collaborated in its drafting. Chapter VII focuses on the Incident Response Team, CCN-CERT.
- Approval to handle national classified information with Criptoper SCAP V.1.3.

February

- Double participation of the CCN in the 1st International CIIP Meeting (Cybersecurity and Protection of Critical Infrastructures) as a collaborator for the CNPIC and as contact point for EGC Group (CCN-CERT).
- Release of Security Guides for SCADA systems (CCN-STIC guide 480).

March

- CCN's Security Evaluation and Certification National Outline joins the European agreement SOGIS MRA v3 (Senior Officers Group for Information Systems, Mutual Recognition Agreement), of relevant importance for public organizations and private companies which are interested in the development, acquisition, use or evaluation of ICT security products. Its inclusion is a further step for the National Scheme within the European framework.
- CWIX 2010 demonstration: encryption of GSM/GPRS Communications in PDA (Tecnobit), Codelogin (GMV).

April

- The CCN participates in the 9th Conference on Information Technologies for the Modernization of Public Administrations (TECNIMAP) in Zaragoza, where it announced the incorporation of the National National Evaluation and Certification Schemeof Information Technologies Security (ENECSTI) into the European agreement SOGIS MRA v3. It organized an ad hoc session within the TECNIMAP framework.
- CWIX 2010 Demonstration: global security environment (EADS Defense & Security Solutions España) and Deimos API (Deimos Space S.L.)

Enero

- Se publica el Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en cuya redacción ha colaborado activamente el CCN y cuyo capítulo VII está centrado en la Capacidad de Respuesta a Incidentes, CCN-CERT.
- Aprobación para manejar información nacional clasificada con Criptoper SCAP V.1.3.

Febrero

- Participación doble del CCN en el I Encuentro Internacional CIIP (Ciberseguridad y Protección de Infraestructuras Críticas) como colaborador del CNPIC en la materia y como punto de contacto del EGC Group (CCN-CERT).
- Publicación de las Guías de Seguridad en Sistemas SCADA (Guía CCN-STIC 480).

Marzo

- El Esquema Nacional de Evaluación y Certificación del CCN se incorpora al acuerdo europeo SOGIS MRA v3 (Senior Officers Group for Information Systems, Mutual Recognition Agreement), de especial relevancia para todos los organismos públicos y empresas del sector privado, que se encuentran vinculadas al desarrollo, adquisición, uso o evaluación de productos de seguridad TIC. Su inclusión significa un paso adelante del Esquema Nacional en este campo dentro del marco europeo.
- Demostración CWIX 2010: Cifrado de Comunicaciones GSM/GPRS en PDA (Tecnobit), Codelogin (GMV).

Abril

- El CCN participa en la XI Jornadas sobre Tecnologías de la Información para la Modernización de las Administraciones Públicas (TECNIMAP) en Zaragoza, donde anuncia la incorporación del Esquema Nacional de Evaluación y Certificación de la Seguridad TIC (ENECSTIC) al acuerdo europeo SOGIS MRA v3. El organismo organiza una sesión ad hoc en el marco de TECNIMAP.
- Demostración CWIX 2010: Entorno global de seguridad (EADS Defense & Security Solutions España) y Deimos API(Deimos Space S.L.).

Mayo

- Convenio de colaboración entre el CNI y la Junta de Andalucía para el impulso de la Seguridad de la Información. Entre otros puntos, el acuerdo incluye el asesoramiento, soporte e intercambio de experiencias relativas al diseño, despliegue y operación de los procesos de detección, análisis, gestión y respuesta a los crecientes ataques que sufren los sistemas de la Administración.

- Instalación y despliegue de una sonda individual en la salida de Internet del Ministerio de Industria, Turismo y Comercio.
- Aprobación para manejar información nacional clasificada con GSMSec 351.
- Aprobación para manejar información nacional clasificada con Centro de Gestión GSMSec 351.
- Demostración CWIX 2010: Cifrador IP dual EP430G
- Publicación de la Guía CCN-STIC 417 - Seguridad en PABX

Junio

- Instalación y despliegue de una sonda individual en la salida de Internet del Ministerio de Defensa

Julio

- Siguiendo lo establecido en el artículo 29 del Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad (ENS), el Centro Criptológico Nacional (CCN) y el Ministerio de Política Territorial y Administración Pública elaboran una nueva serie de Guías (serie 800) para facilitar el cumplimiento del Esquema entre toda la Administración pública.
- Instalación y despliegue de una sonda individual en la salida de Internet de la Biblioteca Nacional y del Ministerio de Asuntos Exteriores y Cooperación.
- Se publican tres nuevas Guías dedicadas a la mejora en la implantación del ENSE (Guía 803 - Categorización de los sistemas en el ENS, Guía 804 - Implementación de Medias en el ENS y Guía 809 - Declaración de conformidad con el ENS).

Agosto

- Instalación y despliegue de una sonda individual en la salida de Internet del Ministerio de Política Territorial y Administración Pública (Red SARA).
- Publicación de cuatro nuevas Guías dedicadas al ENS: Guía 800 - Glosario de Términos y Abreviaturas del ENS; Guía 801 - Responsabilidades en el ENS; Guía 805 - Política de seguridad de la información y Guía 806 - Plan de Adecuación al ENS.

Septiembre

- Instalación y despliegue de una sonda individual en la salida de Internet del Ministerio de Economía y Hacienda.
- Aprobación para manejar información nacional clasificada con Criptoper SCAP V.3.20 PROCIF V.3.11.

May

- Cooperation agreement between the CNI and the Junta de Andalucía for the promotion of information security. Among other things, the agreement includes advice, support and exchange of experiences concerning the design, deployment and operation of detection, analysis, management and response capabilities against increasing attacks suffered by Goverment systems.
- Installation and deployment of an individual sensor in the Internet output of the Ministry of Industry, Tourism and Commerce.
- Approval to handle national classified information with Criptoper GSMSec 351.
- Approval to handle national classified information with Centro de Gestión GSMSec 351.
- CWIX 2010 Demonstration: dual IP encryptor EP430G.
- Release of CCN-STIC 417 PABX security

June

Installation and deployment of an individual sensor in the Internet output of the Ministry of Defense.

July

- In accordance with the provisions established in Article 29 of Royal Decree 3/2010 of January 8 for the development of the National Security Framework (ENS), the National Cryptologic Center (CCN) and the Ministry of Territorial Policy and Public Administration developed a new series of Guides (series 800) to facilitate the implementation of the Framework across the entire public administration.
- Installation and deployment of a single sensor at the Internet output of the National Library and the Ministry of Foreign Affairs and Cooperation.
- Release of three new guides aimed at improving the implementation of the ENS (Guide 803 - Systems evaluation in the National Security Framework, Guide 804 - Implementation measures in the National Security Frame–work 809 – statement of conformity in the ENS).

August

- Installation and deployment of a single sensor at the Internet Output by the Ministry of Territorial Policy and Public Administration Network (SARA).
- Release of four new guides focused on ENS: Guide 800 - Glossary of Terms and Abbreviations within the ENS, Guide 801 - Responsibilities in the ENS, Guide 805 -

Participación de CCN en Tecnimap 2010
CCN participation in Tecnimap 2010

Security Policy in the ENS and Guide 806 - Adaptation Plan in the ENS.

September

- Installation and deployment of a single sensor at the Internet output by the Ministry of Economy and Finance.
- Approval to handle national classified information with PROCIF Criptoper SCAP V.3.11.

October

- Installation and deployment of a single probe at the Internet Output of the Royal House Web.
- 1st STIC Course - Security in Web Applications, created to provide a detailed overview, of security threats and vulnerabilities that may affect online offices within the Administration.

November

- Installation and deployment of a single sensor at the Internet Output by the Ministry of Health, Social Policy and Equality.
- Attendance to the SCIP Dry Run Test at the NC3A facilities, The Hague, The Netherlands, to validate the SCIP conformance test procedure over Tecnobit implementation.

December

- CNI's Secretary of State Director, Felix Sanz, opens the 4th CCN-CERT STIC Conference in CESEDEN's headquarters in Madrid. It was attended by more than three hundred ICT security officers from public administrations from all over Spain.
- Significant increase in TEMPEST capabilities after the certification of the first in-flight refueling aircraft, manufactured for the Australian government by AIRBUS MILITARY. Sspecialists from Australian government were present during the tests.
- Installation and deployment of an individual sensor in the Ministry of Culture.
- A total of 29 equipment ZONING certifications were performed and more than seventy premises were evaluated by accredited laboratories and by the CCN itself.
- 1st STIC Course - PILAR tool, designed to provide the necessary knowledge and skills to assess the security level of a system, identifying and evaluating assets and identifying and assessing threats that may affect them.

Octubre

- Instalación y despliegue de una sonda individual en la salida de Internet de la Casa Real.
- Creación del I Curso STIC - Seguridad en Aplicaciones Web destinado a dar una visión detallada, actual y práctica de las amenazas y vulnerabilidades de seguridad que afectan a las sedes electrónicas de la Administración.

Noviembre

- Instalación y despliegue de una sonda individual en la salida de Internet del Ministerio de Sanidad, Política Social e Igualdad.
- Asistencia al SCIP Dry Run Test celebrado en la sede de la NC3A en la Haya, Países Bajos, con el objetivo validar el protocolo de pruebas de conformidad SCIP sobre la implementación de la empresa Tecnobit.

Diciembre

- El Secretario de Estado Director del CNI, Félix Sanz, inaugura la IV Jornada STIC CCN-CERT, en la sede del CESEDEN en Madrid, con la asistencia de más de trescientos responsables de Seguridad TIC de las diferentes administraciones públicas, provenientes de toda España.
- Se incrementa notablemente la capacidad TEMPEST tras la certificación del primer avión de reabastecimiento en vuelo, fabricado por la empresa AIRBUS MILITARY para el gobierno australiano, con la presencia de especialistas del gobierno de Australia durante los ensayos.
- Instalación y despliegue de una sonda individual en el Ministerio de Cultura.
- Se realizan un total de 29 certificaciones ZONING de equipos y más de setenta locales evaluados por laboratorios acreditados y el propio CCN.
- Creación del I Curso STIC - Herramienta PILAR destinado a proporcionar los conocimientos y habilidades necesarias para poder evaluar el estado de seguridad de un sistema, identificando y valorando sus activos e identificando y valorando las amenazas que se ciernen sobre ellos.

Edita: Centro Criptológico Nacional

Diseño | Design: Isolina Dosal
Fotografía | Photography: Centro Criptológico Nacional
Imprime | Print: Preimpresión Gala

D.L. M-19897-2011

CENTRO CRIPTOLÓGICO NACIONAL
Argentona, 20 - 28023 Madrid

www.ccn.cni.es
www.ccn-cert.cni.es
www.oc.ccn.cni.es