Informe de Actividades

Activity Report

CCN
Centro Criptológico Nacional

2015 - 2016

Carta del Secretario de Estado director del CNI
Letter from the Secretary of State-director CNI

1

Querido/a lector/a,

En el seno del Centro Criptológico Nacional, organismo adscrito al Centro Nacional de Inteligencia, somos plenamente conscientes de la misión que se nos ha encomendado y de la necesidad de transmitirla a la sociedad española. El Informe de Actividades 2015-2016 que tengo el placer de presentarle es una de las herramientas más importantes para dar a conocer nuestras actividades, nuestras inquietudes y, sobre todo, el servicio que prestamos a España, sus organizaciones y sus ciudadanos.

Le invito a consultarlo y a repasar las principales acciones llevadas a cabo en los dos últimos años en el campo de la seguridad del ciberespacio y la protección de la información sensible, tanto del **sector público** español como de las **empresas de interés estratégico** para el país y de los sistemas que procesan, almacenan o transmiten **información clasificada**.

Un período de tiempo en el que la ciberseguridad se ha situado entre las principales preocupaciones de los gobiernos e instituciones de todo el mundo y en el cual las más importantes amenazas, detalladas en el presente informe, han crecido a un ritmo vertiginoso. Un ritmo que exige un trabajo continuo de renovación, investigación y adaptación constante.

En este sentido, el CCN mantiene cuatro grandes líneas de actuación. La primera consiste en fomentar la **formación y sensibilización** y, así, el CCN cuenta ya con una masa crítica de 6.130 funcionarios y empleados públicos formados presencialmente en los diferentes aspectos de la seguridad de las Tecnologías de la Información y la Comunicación (TIC). A ellos se unen los más de 20.200 alumnos inscritos en alguno de los nueve cursos ***online*** disponibles en el portal del CCN-CERT y la difusión de informes y boletines de seguridad que con distinta periodicidad y temática abordan las principales amenazas del momento.

La segunda línea promueve el **desarrollo, certificación y fomento de tecnologías seguras** sobre las que debe descansar cualquier producto o servicio. En este campo, el Centro Criptológico Nacional dirige y desarrolla diferentes productos de cifra y realiza numerosas auditorías de seguridad en páginas web de la Administración.

La tercera línea de trabajo se centra en la elaboración de un conjunto de **normas, procedimientos y directrices** técnicas que garantizan la seguridad y que se materializan en las Guías CCN-STIC de las que existen ya 273 (que contienen un total de 374 documentos). Unas guías que han alcanzado un gran prestigio y aceptación entre los profesionales del sector, y se han convertido en manuales de referencia en ciberseguridad.

Dear Reader,

Within the National Cryptologic Centre, an organisation that is part of the National Intelligence Centre, we are fully aware of our assignment and the need to put it across to Spanish society. The 2015-2016 Activity Report that I have the pleasure of presenting here is one of the most important tools to raise awareness on our work, our concerns and above all the service that we provide to Spain, its organisations and its citizens.

I would invite you to consult it and look over the main actions carried out over the last two years in the field of cyberspace security and protection of sensitive information for both the Spanish **public sector** and from **companies of strategic interest** for the country and the systems that process, store or transmit **classified information**.

Over this period of time, cyber-security has become one of the main concerns for Governments and institutions all over the world and the most important threats, explained in detail in this report, have escalated at a dizzying rate. This pace requires continuous work to constantly renew, investigate and adapt.

In this respect, the CCN maintains four major lines of work: the first consists of encouraging **training and awareness raising** and so the CCN already has a critical mass of 6,130 civil servants and state employees who have received classroom training on different aspects of security for Information and Communication Technologies (ICT). They are joined by over 20,200 students signed up to the nine online courses available from the CCN-CERT website plus security reports and newsletters sent out with varying frequency covering the main current threats.

A second line promotes development, certification and promotion of **secure technology** on which any product or service should be based. In this field, the National Cryptologic Centre runs and develops different encoding products and carries out many security audits on Administration websites.

The third line of work is focussed on drawing up a set of standards, procedures and technical guidelines that guarantee security and that take shape in the **CCN-STIC** guides of which there are already 273 (containing a total of 374 documents). These guides have achieved great prestige and

La cuarta la línea de actuación, en la que el CCN ha volcado una gran parte de sus esfuerzos, es la capacidad de **prevención, detección, respuesta y recuperación** ante ciberincidentes, materializada en el **CCN-CERT**. Una capacidad que gestionó en solo dos años un total de 39.172 ciberincidentes en organizaciones del sector público y de empresas de interés estratégico, de los que 1.050 fueron catalogados con un índice de peligrosidad "crítico" o "muy alto". Y lo hizo gracias a la mejora en los mecanismos de coordinación y los sistemas de alertas de amenazas, vulnerabilidades y agresiones o ataques, desarrollando herramientas propias de detección y propiciando un intercambio de información fructífero entre todos los agentes implicados. Afortunadamente, en esta tarea de conformación de un sistema de protección nacional no nos hemos encontrado solos. Por un lado, contamos con el **respaldo normativo**, tanto nacional como internacional, que en los últimos años ha ido adecuándose a las crecientes necesidades (Directiva NIS, Planes derivados del Plan Nacional de Ciberseguridad, la modificación del Código Penal incluyendo tipos de ciberterrorismo o la Ley 40/2015 de Régimen Jurídico del Sector Público). Por otro lado, es preciso destacar la **colaboración** creciente de organismos y entidades públicas, el trabajo de todo nuestro personal, la ayuda de las empresas proveedoras y la cooperación con nuestros colegas y aliados de otros países.

Estas han sido nuestras líneas de actuación en los dos últimos años y lo seguirán siendo en el futuro, conscientes de que la misión que el Gobierno nos tiene asignada no tiene límite en el tiempo y necesita cada día de mayor dedicación de personas y recursos. A ella nos seguiremos entregando, día a día, con el único objetivo de mantener seguro nuestro ciberespacio y proteger la información sensible de nuestro país.

Contamos con su ayuda.

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.06.23 11:23:10 +02'00'

Félix Sanz Roldán
Secretario de Estado director del CNI,
Director del CCN
Secretary of State-Director of CNI, Director of CCN

acceptance among sector professionals and have become cyber-security reference manuals.

The fourth line of action, into which the CCN has poured a lot of its hard work, is the capacity for prevention, detection, response and recovery, in the form of the **CCN-CERT**. Within just two years, it has managed a total of 39,172 cyber-incidents in public sector organisations and companies of strategic interest of which 1,050 were classified as having a "critical" or "very high" danger index. And this was possible thanks to improving coordination mechanisms and the warning systems for threats, vulnerabilities and attacks, developing own detection tools and providing fruitful information exchange among all agents involved. Fortunately, we were not alone in this task of shaping a national protection system. On the one hand, we are backed by both national and international standards that have been adapting to growing needs over the last few years (NIS Directive, Plans derived from the National Cyber-Security Plan, modification of the Criminal Code including types of cyber-terrorism or Law 40/2015 on the public sector Legal Regime). On the other hand, we should highlight growing collaboration from organisations and public entities, the work of all our staff, help from supplier companies and cooperation with our colleagues and allies in other countries.

This explains our lines of action over the last two years and we will continue them into the future, aware that our Government assignment does not have a time limit and every day requires greater dedication of persons and resources. We intend to continue working on this day by day with the sole aim of keeping our cyberspace secure and protecting our country's sensitive information.

We are counting on your help.

ÍNDICE
TABLE OF CONTENTS

2

CCN

Centro Criptológico Nacional

- Acreditación
- Normativa
- Evaluación
- Desarrollo
- Certificación
- Velar

El Centro Criptológico Nacional (CCN) es un organismo, adscrito al Centro Nacional de Inteligencia (CNI). Fue creado en el año 2002 con el fin de garantizar la seguridad TIC[1] en las diferentes entidades de la Administración Pública, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.

Su ámbito de competencia está definido por el siguiente marco normativo:

- Ley 11/2002, de 6 de mayo, reguladora del **Centro Nacional de Inteligencia (CNI)**.
- Real Decreto 421/2004, de 12 de marzo, que regula y define el ámbito y funciones del **Centro Criptológico Nacional (CCN)**.
- Orden Ministerio Presidencia PRE/2740/2007, de 19 de septiembre, que regula el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, y que confiere al CCN la capacidad de actuar como **Organismo de Certificación (OC)** de dicho Esquema.
- Real Decreto 03/2010, de 8 de enero, de desarrollo del **Esquema Nacional de Seguridad** (ENS), actualizado en el RD 951, de 23 de octubre, en el que se establecen los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
- Comisión Delegada del Gobierno para Asuntos de Inteligencia, que define anualmente los objetivos del CNI mediante la Directiva de Inteligencia, que marca la actividad del Centro.

The National Cryptologic Centre (CCN) is an Organisation, within the National Intelligence Centre (CNI), set up in 2002 to guarantee ICT security in different public administration entities and security for systems that process, store or send out classified information.

Its sphere of competence is defined by the following standard framework:

- Law 11/2002, dated 6th May, regulating the National Intelligence Centre (CNI)
- Royal Decree 421/2004, 12th March, regulating and defining the sphere and functions of the National Cryptologic Centre (CCN).
- Presidential Ministerial Order PRE/2740/2007, dated 19th September , that regulates the National Evaluation Frame work and Information Technology Security Certification giving the CCN the capacity to act as a Certification Body (OC) for this Framework.
- Royal Decree 03/2010, dated 8th January, developing the National Security Framework (update RD 951/2015, dated 23 October), establishing basic principles and mínimum requirements, as well as protection measures to be implanted in Administration systems.
- **Government Delegate Commission for Intelligence Matters**, that annually defines CNI objectives using the Intelligence Directive setting out the Centre's work.

[1] Tecnologías de la Información y la Comunicación

Además de la legislación anteriormente expuesta, varias normativas publicadas en los dos últimos años afectan muy directamente al sector de la ciberseguridad y, por ende, a la actividad del Centro Criptológico Nacional. Entre otras, podemos citar:

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, también conocida como **Directiva NIS**. Se trata de la primera directiva comunitaria en materia de ciberseguridad.Entró en vigor el 9 de agosto de 2016 y debe ser adoptada y publicada en cada uno de los Estados miembros antes del 9 de mayo de 2018.

- Estrategia de Ciberseguridad Nacional y los nueve Planes Derivados del Plan Nacional de Ciberseguridad, que fueron aprobados el 14 de julio de 2015 por el Consejo de Seguridad Nacional y que desarrollan la Estrategia y ordenan la actividad y el esfuerzo del Estado en este ámbito.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que amplía el ámbito de aplicación del ENS al sector público institucional y con ello la responsabilidad del CCN.

- Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad. Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas.

- Instrucción Técnica de Seguridad (ITS) de Informe del Estado de la Seguridad. Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal en materia de delitos de terrorismo incluyendo tipos penales de ciberterrorismo.

In addition to the aforementioned legislation, there have been several standards published over the last two years that directly affect the cyber-security sector and consequently the National Cryptologic Centre's work as well. Among others, we might mention:

- The (EU) Directive 2016/1148 from the European Parliament and Council dated 6th July 2016 relating to measures intended to guarantee a high common level of security in the Union's networks and information systems, also known as the NIS Directive. This is the first community directive in terms of cyber-security that came into force on 9th August 2016; it should be adopted and published in each of the Member States before 9th May 2018.

- National Cyber-Security Strategy and the nine **Plans Derived from the National Cyber-security Plan**, approved on 14th July 2015 by the National Security Council, that develop the Strategy and organise the State's work in this field.

- Law 39/2015, dated 1st October, on the Common Administrative Procedure for Public Administrations.

- Law 40/2015, dated 1st October, on the Public Sector Legal Regime

- Technical Security Instruction (ITS) in compliance with the National Security Framework. Resolution dated 13th October 2016 from the Secretary of State for Public Administrations.

- Technical Security Instructions (ITS) from the State Security Report. Resolution dated 7th October 2016, from the Secretary of State for Public Administrations to approve the Technical Security Instruction in the State Security Report.

- Organic Law 1/2015, dated 30th March, modifying Organic Law 10/1995, dated 23rd November, on Criminal Law regarding terrorism crimes including criminal cyberterrorism.

El Centro Nacional de Inteligencia (CNI), al que está adscrito el CCN y con quien comparte medios, procedimientos, normativa y recursos, 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. Esta misión se concreta en diversas funciones (art. 4 de la **Ley 11/2002, de 6 de mayo**) que definen sus cometidos y ámbitos de actuación y que, anualmente, se detallan y desarrollan en la Directiva de Inteligencia.

El CNI se adscribe orgánicamente al **Ministerio de la Presidencia y para las Administraciones Territoriales**.

The National Intelligence Centre (CNI), on which the CCN depends and with which it shares equipment, procedures, standards and resources, is the public Organisation responsible for providing the President of the Government and the Government of the Nation with the information, analysis, studies or proposals that help prevent or avoid any danger, threat or attack on the independence or territorial integrity and stability of the Rule of Law and its institutions. This assignment is specific for different functions (art.4 of Law 11/2002 dated 6th May), defining their tasks and fields of action, that are itemised and developed in the Intelligence Directive every year.

The CNI depends organically on the Ministry of the Presidency and for Territorial Administrations.

Funciones del secretario de Estado director del CNI
Functions of the Secretary of State-Director of the CNI

- Autoridad Nacional de Seguridad Delegada de la Información Clasificada OTAN/UE/ Acuerdos Internacionales
  - National Delegated Security Authority for classified NATO/ EU Information / International Agreements.
- Presidencia del Consejo Nacional de Ciberseguridad
  - President of the National Cyber-Security Council
- Director del Centro Criptológico Nacional
  - Director of the National Cryptologic Centre
- Miembro de la Comisión Delegada del Gobierno para Asuntos de Inteligencia
  - Member of the Delegate Government Intelligence Commission
- Miembro del Consejo de Seguridad Nacional
  - Member of the National Security Council
- Miembro de la Comisión Delegada del Gobierno para Situaciones de Crisis
  - Member of the Delegate Government Crisis Situations Commission

Es un órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, en el marco de la Ley 50/1997, de 27 de noviembre, del Gobierno. El Consejo Nacional de Ciberseguridad se crea por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013 y está presidido por el secretario de Estado director del CCN.

Entre sus funciones destacan las siguientes:

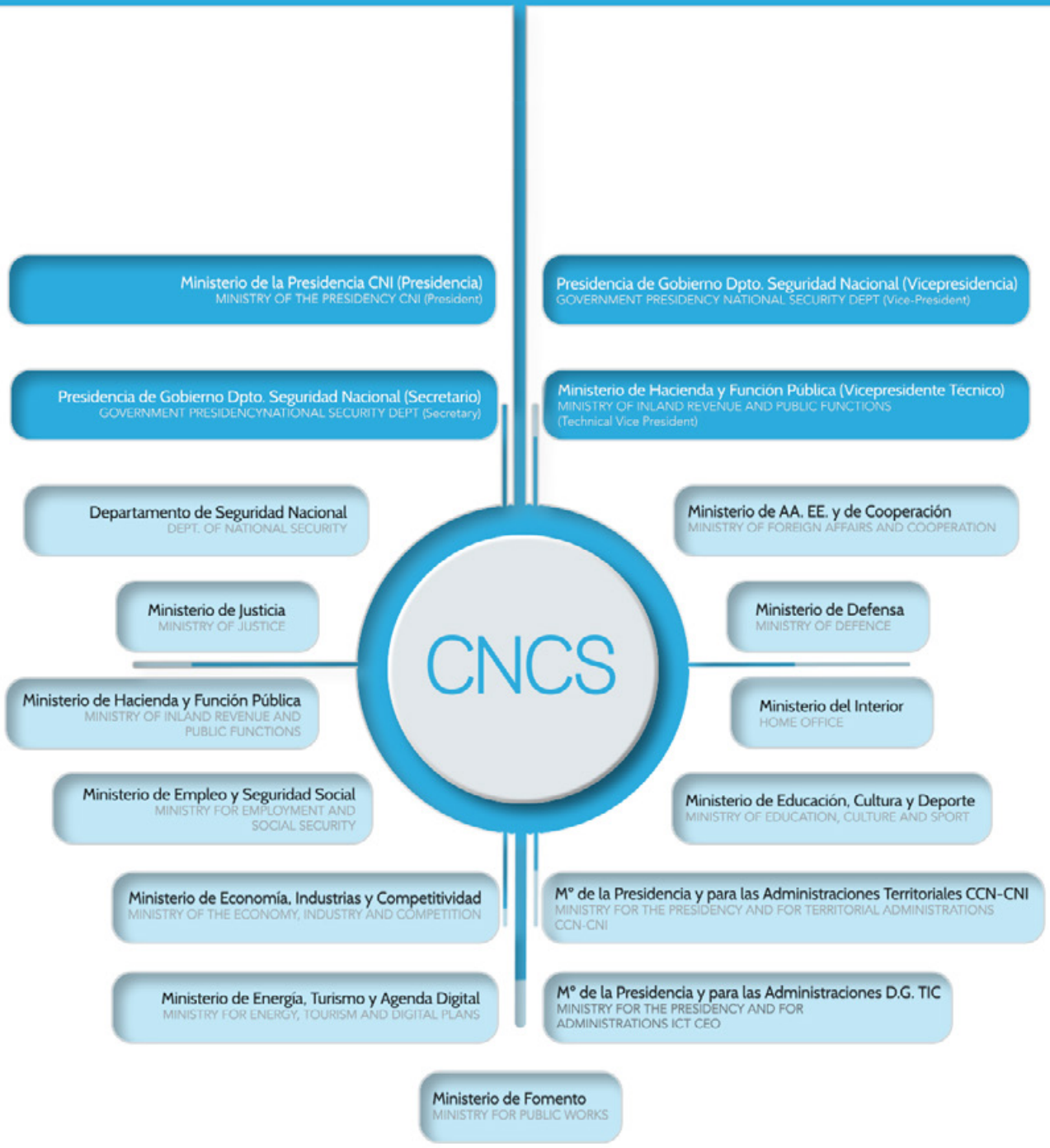
- Apoyar la toma de decisiones del **Consejo de Seguridad Nacional (CSN)** en materia de ciberseguridad mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional y contribuir a la elaboración de propuestas normativas.
- Reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas, así como entre los sectores público y privado.
- Verificar el grado de cumplimiento de la **Estrategia de Ciberseguridad Nacional e informar al CSN**.
- Valorar los **riesgos y amenazas**, analizar los posibles escenarios de crisis, estudiar su posible evolución, elaborar y mantener actualizados los planes de respuesta y formular directrices para la realización de ejercicios de gestión de crisis en coordinación con los órganos y autoridades directamente competentes.
- Contribuir a la disponibilidad de los **recursos existentes** y realizar los estudios y análisis sobre los medios y capacidades de las distintas Administraciones Públicas y Agencias.
- Facilitar la coordinación operativa entre los órganos y autoridades competentes cuando las situaciones que afecten a la ciberseguridad lo precisen y mientras no actúe el Comité Especializado de Situación.

This is a collegiate body supporting the National Security Council as Delegate Government National Security Commission within the framework of Law 50/1997, dated 27th November, from the Government. The National Cyber-Security Council was set up by Agreement from the National Security Council on 5th December 2013 and it is presided over by the Secretary of State, director of the CCN.

Its main functions include:

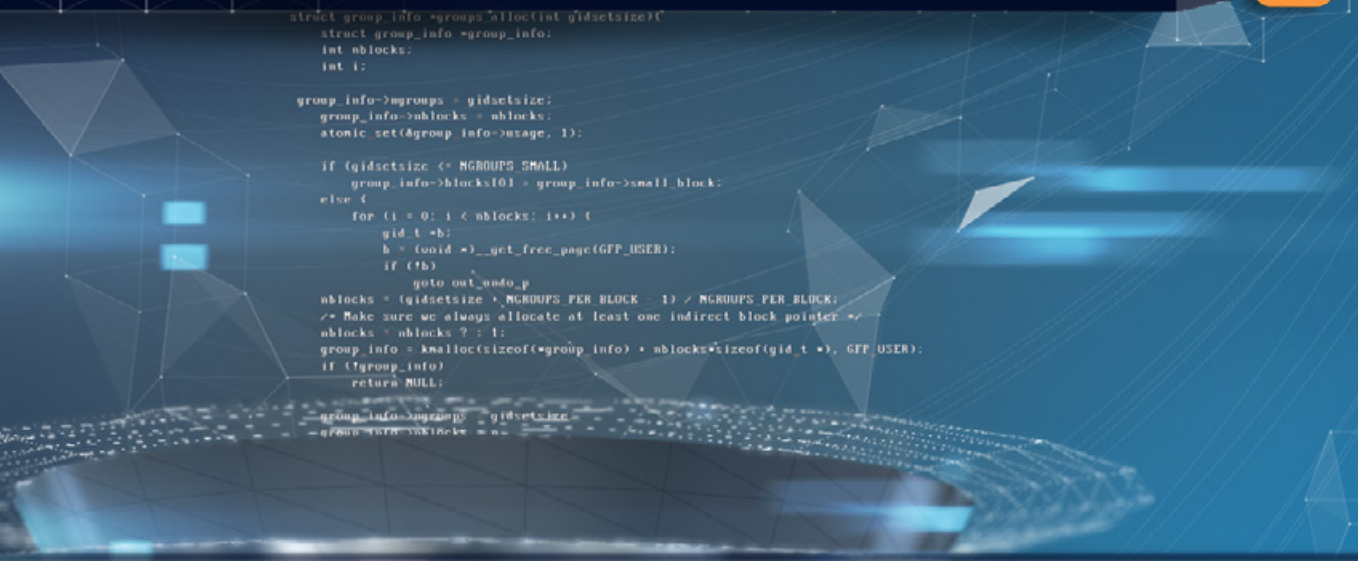
- **Supporting National Security Council (CSN)** decision-making in terms of cyber-security by means of analysis, study and proposal of initiatives in both national and international fields and helping to draft **proposals for standards**.
- Strengthening coordination, collaboration and cooperation between different Public Administrations, and between public and private sectors.
- Verifying the degree of compliance with the **National Cyber-Security Strategy** and reporting to the CSN.
- Evaluating **risks and threats**, analysing possible crisis scenarios, studying any possible changes, drafting response plans and keeping them updated and devising directives to run crisis management exercises, coordinating with directly competent bodies and authorities.
- Helping make **existing resources** available and carrying out studies and analysis on the resources and capabilities of the different Public Administrations and Agencies.
- Easing operative coordination between competent bodies and authorities when required by situations affecting cyber-security, unless the Specialised Situation Committee is involved.

CONSEJO NACIONAL DE CIBERSEGURIDAD
NATIONAL CYBERSECURITY COUNCIL



FUNCIONES DEL CCN
CCN FUNCTIONS

4



NORMATIVA
STANDARS

1

Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas TIC (Guías CCN-STIC).
Drawing up and disseminating standards, instructions, guides and recommendations to guarantee security for the Administration's information and communication technology systems.

FORMACIÓN
TRAINING

2

Formar al personal de la Administración especialista en el campo de la seguridad.
Administration staff specialising in the sphere of security for in-formation and communication technology systems.

VIGILAR
LOOK OUT

3

Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.
Making sure that standards are met relating to protecting classified information in its field of competence.

DESARROLLO
DEVELOPMENT

4

Coordinar la promoción, desarrollo, obtención, adquisición y puesta en explotación y uso de tecnologías de seguridad.
Setting up the Certification Body for the National Evaluation and Certification Scheme and certification of information technology security, to be applied to products and systems in its field.

EVALUACIÓN
EVALUATION

5

Valorar y acreditar la capacidad de los productos de cifra y de los sistemas para manejar información de forma segura.
Assessing and accrediting the capacity of encryption products and information technology systems that include encryption devices to process, store or send out information securely.

CERTIFICACIÓN
CERTIFICATION

6

Constituir el Organismo de Certificación del Esquema nacional de evaluación y certificación de la seguridad, de aplicación a productos y sistemas en su ámbito.
Coordinating promotion, development, obtaining, purchasing and operating plus the use of security technology for the aforementioned systems.

CIBERSEGURIDAD
CYBERSECURITY

7

Contribuir a la mejora de la ciberseguridad española, a través del CCN-CERT, afrontando de forma activa las amenazas que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para el país, en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y a cualquier sistema TIC que procese información clasificada.
Help improve Spanish cyber-security, through the CCN-CERT, actively addressing threats affecting public sector systems, companies and organisations of strategic interest for the country, in coordination with the National Centre for the Protection of Critical Infrastructures (CNIPIC) and any classified system.

RELACIONES
RELATIONS

8

Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.
Establishing the necessary relationships and signing relevant agreements with similar organisations from other countries to develop the aforemen-tioned functions.

Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas.

The CCN-STIC series is made up of regulations, guidelines, guides and recommendations developed by the National Cryptologic Centre in order to enhance cybersecurity within organizations. These guides are regularly updated and supplemented with new information, according to the threats and vulnerabilities detected.

Series CCN-STIC
CCN-STIC Series

A finales de 2016 había un total de 273 Guías (374 documentos), de las cuales 63 fueron nuevas o actualizadas entre 2015 (28) y 2016 (35). Estas guías están enmarcadas en alguna de las nueve series CCN-STIC. La serie 800 de acceso público se elaborada en colaboración con el Ministerio de Hacienda y Función Pública.

By the end of 2016 there were 273 guides (374 documents) within the CCN-STIC series (the CCN-STIC 800 series, drawn up in collaboration with the Ministry of the Finance and Civil Service). Of these, 63 have been draw up or updated over the last two years (28 first year and 35 the second).

Listado de Guías CCN-STIC 2017
List of CCN-STIC 2017 Guides

Cumple con el ENS / COMPLIES WITH ENS
Pendientes de publicar / PENDING PUBLICATION
* Difusión limitada / LIMITED DIFUSSION
Adaptables al ENS / ADAPTED TO ENS
Fuera de Soporte / OUT OF SUPPORT
** Confidencial / CONFIDENTIAL

Serie 000: Políticas
SERIE 000: POLICIES

001	Seguridad de las TIC que manejan información clasificada en la Administración ICT Security in the Public Administration	JUN-16
002	Coordinación Criptológica Cryptologic Coordination	MAR 11
003*	Uso cifradores certificados protección inf. clasificada Use of Certified Encryption Equipment	MAY 13

Serie 100: Procedimientos
SERIE 100: PROCEDURE

101	Acreditación sitemas que manejan Información Nacional Clasificada en la Administración National Accreditation Procedure in Public Administration	DIC 16
102	Procedimiento de evaluación de productos criptológicos Cryptologic products evaluation procedure	MAR 14
103*	Catálogo de productos con certificación criptológica Catalogue of products with cryptologic certificantion	JUL 16
104	Catálogo de Productos con clasificación Zoning Zoning products clasification catalogue	ENE 13
105	Catálogo de productos STIC (CPSTIC) Catalogue of products SICT	
106	Inclusión productos STIC cualificados en el Catálogo de Productos Inclusion of products SICT in the catalogue of products	
130*	Requisitos productos cifra para evaluación criptológica Encryption equip. requirements cryptologic evaluation	
140	Taxonomías de referencia para productos STIC Taxonomy of SICT products reference	
151*	Evaluación y Clasificación TEMPEST de Equipos TEMPEST Evaluation and Classification of Equipment	MAR 17
152*	Evaluación y Clasificación ZONING de Locales Facility ZONING, Evaluation and Classification	MAR 17
153*	Evaluación y Clasificación de Armarios Apantallados Evaluation and Classification of Shielded Cabinets	MAR 17
154*	Medidas de protección TEMPEST para instalaciones Protection TEMPEST Measures for Facilities	MAR 17

Serie 200: Norma
SERIE 200: STANDARDS

201	Organización y gestión para la seguridad Organization and management for security	ENE 09
202	Estructura y Contenido Declaración Requisitos Seg. DRS SSRS. Structure and Content	MAR 05
203	Estructura y Contenido Procedimientos Operativos POS SecOps. Structure and Content	MAR 05
204	Estructura y Contenido CO-DRES-PO estaciones aisladas y pequeñas redes. Formulario CO-DRES-POC Structure and Content Isolated station and smal networks. Form.	ENE 09
205	Actividades Seguridad Ciclo Vida CIS Security Life Cycle Activities (CIS)	DIC 07
207	Estructura y Contenido del Concepto de Operación Concept of Operation. Structure and Content	NOV 05
210*	Norma de Seguridad en las Emanaciones TEMPEST Safety Standard TEMPEST Emanations	MAR 17
211*	Gestión del material de cifra en las cuentas de cifra Encryption material managment	

Serie 300: Instrucciones Técnicas
SERIE 300: TECHNICAL INSTRUCTIONS

301*	Requisitos STIC SICT Security Requirements	DIC 07
302*	Interconexión sistemas que manejan inform. nacional clasificada en la Administración Interconnection of systems managment classified national information	JUL 12
303*	Inspección STIC SICT Security Inspection	ENE 09
304	Baja y destrucción de material criptológico Destructing and Taking Cryptologic material out of Circulation	MAR 11
305*	Destrucción y sanitización de soportes Media Sanitization and Destruction	JUL 13
307*	Seguridad en Sistemas Multifunción Security in Multifunction Systems	ENE 09

Serie 400: Guías Generales
SERIE 400: GENERAL GUIDES

400	Manual STIC SICT Security Manual	MAY 13
401	Glosario / Abreviaturas Glossary / Abbreviations	AGO 15
402	Organización y Gestión STIC SICT Security Organization and Management	DIC 06
403	Gestión de incidentes de seguridad Security incidents management	DIC 07
404	Control de Soportes Informáticos Computing Devices Control	DIC 06
405	Algoritmos y parámetros de firma electrónica Electronic signature: algorithms and parameters	FEB 12
406	Seguridad en redes inalámbricas estándar 802.11 Wireless Security	JUL 13
407	Seguridad en telefonía móvil Mobile Phone Security	DIC 06
408	Seguridad perimetral – Cortafuegos Perimeter Security – Firewalls	MAR 10
409A*	Colocación de Etiquetas de Seguridad Security Labels	MAY 13
409B**	Colocación de Etiquetas de Seguridad en Equipos de Cifra Security Labels in Encryption Equipments	MAY 13
410	Análisis riesgos en sistemas de la Administración Risk Analysis in the Administration	DIC 06
411*	Modelo de Plan de Verificación STIC Plan Model of ICT Security verification	ENE 09
412	Requisitos seguridad entornos y aplicaciones Web Security Requirements for Environments and Web Applications	ENE 09
413	Auditoría de entornos y aplicaciones Web Audit Environments and Web Applications	
414	Seguridad en Voz sobre IP VoIP Security	ENE 09
415	Identificación y Autenticación Electrónica Electronic Identification and Authentication	DIC 07
416	Seguridad en Redes Privadas Virtuales VPN Security	DIC 07
417	Seguridad en PABX PABX Security	MAY 10
418	Seguridad en Bluetooth Bluetooth Security	ENE 09
419	Configuración segura con IPtables Secure Configuration with IPtables	DIC 07
420	Test de penetración Pentest	
421	Copias de seguridad y recuperación ante desastres Backup and disaster recovery	
422	Desarrollo seguro de aplicaciones web Secure Development of web applications	JUL 13
423	Indicadores de Compromiso (IOC) Indicators of Commitment (IOC)	OCT 15
424	Intercambio de información de ciberamenazas. STIX-TAXII. Empleo en REYES	OCT 15
425	Seguridad en IP versión 6 IPv6 Security	OCT 15
426	REYES. Manual de usuario REYES. Handbook	ABR 16

430	Herramientas de Seguridad Security Tools	ENE 09
431	Herramientas de análisis de vulnerabilidades Tools for Vulnerabilities Evaluation	DIC 06
432	Seguridad Perimetral – IDS Perimeter Security – Intrusion Detection Systems	ENE 09
434	Herramientas para el análisis de ficheros de logs Tools for Log Files Analysis	JUN 09
435	Herramientas de monitorización de tráfico Tools for Data Flow Monitoring	DIC-12
436	Herramientas de análisis de contraseñas Password Analysis Tools	DIC 07
437	Herramientas de cifrado software Encryption Software Tools	DIC 07
438	Esteganografía Steganographia	SEP 11
440	Mensajería Instantánea Instant Messaging	DIC 07
441	Configuración Segura de entornos virtuales VMWare Secure Configuration of VMWare	ENE 10
442	Seguridad en VMWare ESXi VMWare ESXI security	
443	Tecnología de identificación por radiofrecuencia RFID RFID	ENE 09
444	Seguridad en redes inalámbricas IEEE 802.16 WiMAX WiMax Security	MAR 11
445A	Curso Especialidades Criptológicas. Probabilidad (correspondencia) Cryptologic Specialised Course (CEC) – Probability	JUL 10
445B	Curso de Especialidades Criptológicas. Principios digitales (correspondencia) Cryptology Specialist Course. Digital Principles	JUL 10
445C	Curso de Especialidades Criptológicas. Teoría de números (correspondencia) CEC – Numbers Theory	JUL 10
450	Seguridad en dispositivos móviles Security on Mobile Devices	MAY 13
451	Seguridad en Windows Mobile 6.1 Security on Windows Mobile 6.1	MAY 13
452	Seguridad en Windows Mobile 6.5 Security on Windows Mobile 6.5	MAY 13
453	Seguridad en Android 2.1 Security in Android	MAY 13
453B	Seguridad en dispositivos móviles: Android 4.x Security in Android 4.x	ABR 15
453C	Seguridad en dispositivos móviles: Android 5.x Security in Android 5.x	
453D	Seguridad en dispositivos móviles: Android 6.x Security in Android 6.x	
454	Seguridad en dispositivos móviles iPad (iOS 7.x) Security in iPad (iOS 7.x)	JUL 14
455	Seguridad en dispositivos móviles iPhone (iOS 7.x) Security in iPhone (iOS 7.x)	JUL 14
455B	Seguridad en dispositivos móviles: iPhone (iOS 10.x) Security in iPhone (iOS 10.x)	
456	Seguridad en entornos BES BES Security enviroments	
457	Herramientas de gestión de dispositivos móviles: MDM Mobile Device Management Tool	NOV 13
460	Seguridad en WordPress WordPress Security	JUL 15
461	Seguridad en Drupal Security in Drupal	JUN 16
462	Seguridad en Joomla Security in Joomla	AGO 16
470A	Manual de usuario PILAR 4.1 Risk Analysis Tool Manual PILAR 4.1	DIC 07
470B	Manual de usuario PILAR 4.3 Risk Analysis Tool Manual PILAR 4.3	DIC 08
470C	Manual de usuario PILAR 4.4 Risk Analysis Tool Manual PILAR 4.4	FEB 10
470D	Manual de usuario PILAR 5.1 Risk Analysis Tool Manual PILAR 5.1	MAY 11
470E1	Manual de usuario PILAR 5.2 Risk Analysis Tool Manual PILAR 5.2	JUL 12
470E2	Manual de usuario PILAR 5.2. Análisis del Impacto y Continuidad del Negocio. Risk Analysis Tool Manual PILAR 5.2 Impact Analysis and Business Continuity	JUL 12
470F1	Manual de usuario PILAR 5.3 Risk Analysis Tool Manual PILAR 5.3	NOV 13
470F2	Manual de usuario PILAR 5.3. Análisis del Impacto y Continuidad del Negocio. Manual PILAR 5.3 Impact Analysis and Business Continuity	NOV 13
470G1	Manual de usuario PILAR 5.4 Análisis y gestión riesgos Risk Analysis Tool Manual PILAR 5.3	AGO 14
470G2	Manual de usuario PILAR 5.4. Análisis del Impacto y Continuidad del Negocio. Manual PILAR 5.3 Impact Analysis and Business Continuity	AGO 14
470H1	Manual usuario PILAR. 6.2. Análisis y gestión de riesgos Risk Analysis Tool Manual PILAR 6.2	
470H2	Manual de usuario PILAR. Análisis del impacto y continuidad del negocio versión 6.2 Manual PILAR 6.2 Impact Analysis and Business Continuity	
471B	Manual de Usuario de RMAT 4.3 Handbook for RMAT 4.3	DIC 08
471C	Manual de Usuario de RMAT 5.1 Handbook for RMAT 5.1	AGO 11
471D	Manual de Usuario de RMAT 5.4 Handbook for RMAT 5.1	AGO 14
471E	Manual de Usuario de RMAT nueva versión Handbook for RMAT new version	
472A	Manual de usuario PILAR BASIC 4.3 Risk Analysis Tool Manual PILAR BASIC v.4.3	DIC 08
472B	Manual de usuario PILAR BASIC 4.4 Risk Analysis Tool Manual PILAR BASIC v.4.4	FEB 10
472C	Manual de usuario PILAR BASIC 5.2 Risk Analysis Tool Manual PILAR BASIC 5.2	JUL 12
472D	Manual de usuario PILAR BASIC 5.3 Risk Analysis Tool Manual PILAR BASIC 5.3	NOV 13
472E	Manual de usuario PILAR BASIC 5.4 Risk Analysis Tool Manual PILAR BASIC 5.4	AGO 14
472F	Manual de usuario PILAR BASIC nueva versión Handbook for PILAR BASIC new version	
473A	Manual de usuario µPILAR Risk Analysis Tool Manual (µPILAR)	MAR 11
473B	Manual de usuario µPILAR 5.2 Risk Analysis Tool Manual µPILAR 5.2	JUL 12
473C	Manual de usuario µPILAR 5.3 Risk Analysis Tool Manual µPILAR 5.3	NOV 13
473D	Manual de usuario µPILAR 5.4 Risk Analysis Tool Manual µPILAR 5.4	AGO 14
473E	Manual de usuario µPILAR nueva versión Handbook for µPILAR new version	
480	Seguridad en Sistemas SCADA Security on SCADA systems	MAR 10
480A	Seguridad en el control de procesos y SCADA. Guía de Buenas Prácticas SCADA- Best Practices	FEB 10
480B	Seguridad en el control procesos SCADA. Guía 1. Comprender el Riesgo del Negocio SCADA- Understanding Business Risks	MAR 10
480C	Seguridad en el control de procesos y SCADA. Guía 2. Implementar una Arquitectura Segura SCADA- Implementing Secure Architecture	MAR 10
480D	Seguridad en el control de procesos y SCADA. Guía 3. Establecer Capacidades de Respuesta SCADA- Establishing Response Capabilities	MAR 10
480E	Seguridad en el control de procesos SCADA. Guía 4. Mejorar la concienciación y las habilidades. Improving Awareness and Capabilities	ENE 10
480F	Seguridad en el control de procesos y SCADA. Guía 5. Gestionar el riesgo de terceros SCADA- Dealing with Risks Derived from Third Parties	MAR 09
480G	Seguridad en el control de procesos y SCADA. Guía 6. Afrontar Proyectos SCADA- Confront Projects	MAR 09
480H	Seguridad en el control de procesos y SCADA . Guía 7. Establecer una dirección permanente SCADA – Establishing a Permanent Address	MAR 10

490	Dispositivos biométricos de huella dactilar Biometric Fingerprints Devices	DIC 07
491	Dispositivos biométricos de iris Iris Biometric Devices	DIC 08
492	Evaluación Parámetros de Rendimiento en Dispositivos Biométricos Evaluation of Performance Parameters in Biometric Devices	FEB 11
495	Seguridad en IPv6 Security in IPv6	JUL 16

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)	DIC 07
501B	Seguridad Windows XP SP2 (cliente independiente) Windows XP SP2 Security (independent client)	DIC 07
502	Seguridad Aplicaciones Cliente. Navegador y Correo Electrónico Client Windows Security: Browser and E-mail	DIC 08
502B	Seguridad en Aplicaciones Cliente Windows Vista. Navegador y Correo Electrónico Client Windows Vista Security. Browser and E-mail	ENE 10
503A	Seguridad en Windows 2003 Server (controlador de dominio) Windows 2003 Server Security (domain controller)	NOV 05
503B	Seg. Windows 2003 Server (servidor independiente) Windows 2003 Server Security (independent server)	DIC 07
504	Seguridad en Internet Information Services 6.0 Internet Information Server Security	OCT 05
505	Seguridad Microsoft SQL server 2000 BD SQL Security	DIC 06
506	Seguridad en Microsoft Exchange Server 2003 MS EXCHANGE Server 2003 Security	JUN 07
507	Seguridad en ISA Server ISA Server Security	DIC 06
508	Seguridad en Clientes Windows 2000 Windows 2000 Clients Security	DIC 07
509	Seguridad Windows 2003 Server. Servidor de Ficheros Security on Windows 2003 Server. File Server	DIC 07
510	Seguridad Windows 2003 Server. Servidor de Impresión Security on Windows 2003 Server. Printing Server	ENE 09
512	Gestión Actualizaciones Seguridad en Sistemas Windows Security Updates Management	DIC 05
515	Servidor de Impresión en Windows 2008 Server R2 Print Server in Windows 2008 Server R2 Security	FEB 16
517A	Seguridad Windows Vista enterprise (miembro de dominio) Windows Vista Security (client within a domain)	ENE 10
517B	Seg. Windows Vista enterprise (cliente independiente) Windows Vista Security (independent client)	ENE 09
519A	Navegador y correo electronico en Windows XP Browser and email in Windows XP	ENE 10
520	Configuración Segura de Internet Explorer 11 Secure Configuration of Internet Explorer 11	ENE 15
521A	Seguridad en Windows Server 2008 R2 (controlador de dominio o miembro) Windows 2008 Server Security (domain controller)	ABR 14
521B	Seguridad en Windows Server 2008 R2 Instalación completa e independiete Windows 2008 Server Security (independent server)	AGO 10
521C	Seguridad en Windows Server 2008 Core (controlador de dominio o miembro) Windows 2008 Server Core Security (domain controller)	MAY 14
521D	Seguridad en Windows Server 2008 R2 Core (servidor independiente) Windows 2008 Server Core Security (independent server)	JUN 13
522A	Seguridad en Windows 7 Enterprise (cliente en dominio) Windows 7 Security (domain client)	JUN 11
522B	Seguridad Windows 7 Enterprise (cliente independiente) Windows 7 Security (independent client)	NOV 10
523	Seguridad en Windows Server 2008 R2. Servidor de Ficheros. Windows 2008 Server Security. File Server	FEB 12
524	Seguridad en Internet Information Server (IIS) 7.5 sobre Windows Server 2008 R2 Internet Information Server 7.5 Security	FEB 14
525	Microsoft Exchange Server 2007 sobre Windows Server 2003 Microsoft Exchange Server 2007 on Windows 2003 security	JUN 13
526	Seguridad en Microsoft Exchange Server 2007 sobre Windows Server 2008 Microsoft Exchange Server 2007 on Windows 2008 security	AGO 13

Cumple con el ENS
COMPLIES WITH ENS

Pendientes de publicar *
PENDING PUBLICATION

Difusión limitada
LIMITED DIFUSSION

Adaptables al ENS
ADAPTED TO ENS

Fuera de Soporte
OUT OF SUPPORT

** Confidencial
CONFIDENTIAL

527	Microsoft Windows 2008 R2 clúster de conmutación Failover Clustering para Windows 2008 Server R2	AGO 13
528	Implementación Hyper-V sobre Windows 2008 R2 Core Hyper-V Windows 2008 Sever R2 Core Security	DIC 13
529	Microsoft Office 2013	ENE 15
530	Microsoft Office 2010	JUL 13
531	Microsoft Office Sharepoint Server 2007 Sharepoint Server Security 2007	DIC 12
532	MS Office Sharepoint Server 2007 enterprise en MS Windows Server 2008 R2 Microsoft Sharepoint Server 2007 on Windows Server 2008 R2 Security	SEP 14
533	Microsoft Sharepoint Server 2010 en Windows Server 2008 R2 Microsoft Sharepoint Server 2010 on Windows Server 2008 R2 Security	NOV 14
534	SharePoint 2013 sobre Windows Server 2012 R2	
540	Implementación de MS SQL Server 2008 R2 en servidor individual y en cluster MS SQL Server 2008 R2	ABR 14
541	SQL Server 2014 sobre Windows Server 2012 R2	
550	Seguridad en Microsoft Exchange Server 2010 sobre Windows Server 2008 R2 Microsoft Exchange Server 2010 on Windows Server 2008 R2 Security	SEP 14
552	Microsoft Exchange Server 2013 en Windows Server 2012 R2	NOV 16
560A	Seguridad en Windows 2012 Server R2 (controlador de dominio) Windows 2012 Server R2 (domain controller) Security	MAR 15
560B	Seguridad en Windows 2012 Server R2 (servidor independiente) Windows 2012 Server R2 (independent server) Security	MAY 15
560C	Windows Server 2012 R2 instalación core, controlador de dominio o servidor miembro Windows Server 2012 R2 (domain controller)	DIC 16
561	Servidor de Impresión Windows Server 2012 R2 Print Server Windows Server 2012 R2	MAR 16
562	Servidor de Ficheros Windows Server 2012 R2 Data Server Windows Server 2012 R2	SEP 16
563	Internet Information Service 8.5 sobre Windows Server 2012 R2 en servidor miembro de dominio Internet Information Service 8.5 Windows Server 2012 R2 in domain controller	NOV 16
566	Servicios de escritorio remoto sobre Windows Server 2012 R2 Remote APP Windows Server 2012 R2	FEB 17
567	Implementación de Hiper V en MS Windows Server 2012 R2 core Hiper V MS Windows Server 2012 R2 core	DIC 16
568	Windows Server Update Service (WSUS)	NOV 16
569	Terminal Server sobre Windows Server 2008 R2	FEB 17
575	Configuración segura SCCM 2014 sobre Windows Server R2 2012 Secure configuration SCCM 2014 Windows Server R2 2012	
585	Configuración segura en MS Office 2016 en Windows 10 Secure configuration MS Office 2016 Windows 10	
590	Recolección y consolidación de eventos - Windows Server 2008 R2 Collecting and consolidating events Windows Server 2008 R2	SEP 14
595	Entidad de Certificación en Windows Server 2008 R2 Certification Entity in Windows Server 2008 R2	FEB 16
596	Protección de sistema con AppLocker AppLocker	FEB 16
597	Entidad de Certificación en Windows Server 2012 R2 Certification Entity Windows Server 2008 R2	DIC 16
598	Virtualización guía de buenas prácticas Good practice guide virtualization	
599A	Configuración segura de Windows 10 Enterprise LTSB (Cliente miembro de dominio) Secure configuration Windows 10 Enterprise LTSB	JUL 16
599B	Configuración segura de Windows 10 Enterprise LTSB (Cliente independiente) Secure configuration Windows 10 Enterprise LTSB	JUL 16
599C	Configuración segura en Windows 10 Anniversary Secure configuration Windows 10 Anniversary	

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	DIC 06
602	Seguridad en HP-UX 11i HP-UX 11i Security	OCT 04
603	Seguridad en AIX-5L AIX-5L Security	MAR 11
606	Configuración segura en Mac OS X 10.10.X Yosemite Secure configuration Mac OS X 10.10 X Yosemite	SEP 15
610	Seguridad en Red Hat Linux 7 Red Hat Linux 7 Security	DIC 06
612	Seguridad en sistemas basados en Debian Debian Security	AGO 14
614	Seguridad en Red Hat Linux (Fedora) Red Hat Linux (Fedora) Security	DIC 06
615	Seguridad en Entornos basados en Redhat Security on Redhat-based Environments	
621	Seguridad en Sun Solaris 8.0 Sun-Solaris 8.0 Security	JUL 04
622	Seguridad en Sun Solaris 9.0 para Oracle 8.1.7 Sun-Solaris 9.0 Security for Oracle 8.1.7	DIC 06
623	Seguridad en Sun Solaris 9.0 para Oracle 9.1 Sun-Solaris 9.0 Security for Oracle 9.i	DIC 06
624	Seguridad en Sun Solaris 9.0 para Oracle 9.2 Sun-Solaris 10 Security for Oracle 9.2	DIC 06
625	Seguridad en Sun Solaris 10g Oracle 10g | Sun-Solaris 10 Security for Oracle 10g	MAR 10
626	Guía de Securización de Sun Solaris 10 con NFS Security Guide for Sun Solaris 10 with NFS	DIC 07
627	Guía de Securización de Sun Solaris 9 con Workstation Security Guide for Sun Solaris 9 with Workstation	DIC 07
628	Guía de Securización de Sun Solaris 9 con NFS Security Guide for Sun Solaris 9 with NFS	DIC 07
629	Guía de Securización de Sun Solaris 10 con Workstation Security Guide for Sun Solaris 10 with Workstation	DIC 07
631	Seguridad en Base de Datos Oracle 8.1.7 sobre Solaris Security for DB Oracle 8.1.7 on Solaris	SEP 05
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	DIC 07
634	Seguridad en Base de Datos Oracle 9i sobre Solaris 9 y 10 Security for DB Oracle 9i on Solaris 9 y 10	DIC 07
635	Seguridad en Base de Datos Oracle 9i sobre HP-UX 11i Security for DB Oracle 9i on HP-UX 11i	DIC 07
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	DIC 07
637	Seguridad en Base de Datos Oracle 10gR2 sobre Solaris 9 y 10 Security for DB Oracle 10gR2 on Solaris 9 y 10	DIC 07
638	Seguridad en Base de Datos Oracle 10gR2 sobre HP-UX 11i Security for DB Oracle 10gR2 on HP-UX 11i	DIC 07
639	Seguridad en Base de Datos Oracle 10g sobre Windows 2003 Server Security for DB Oracle 10g on Windows 2003 Server	AGO 10
641	Seguridad en Router Cisco Router Cisco	NOV 13
642	Seguridad Switches Enterasys Security Switches Enterasys	DIC 06
643A	Seguridad en Equipos de Comunicaciones. Allied Telesis con sistema operativo AW Security for Communication Equipment. Allied Telesis	SEP 13
643B	Seguridad en Equipos de Comunicaciones. Allied Telesis AT-8100S/ AT-8100L y FS970M Security for Communication Equipment. Allied Telesis AT-8100S/AT-8100L and FS970M	MAY 15
644	Seguridad en Equipos de Comunicaciones. Switches Cisco Security for Communication Equipment. Switches Cisco	DIC 07
645	Sistemas de Gestión de Red (Cisco Works LMS) Network Management systems (Cisco Works LMS)	MAR 11
646	Seguridad en Equipos de Comunicaciones. Switches HP Security for Communication Equipment. Switches hp	SEP 14
646B	Seguridad router HUAWEI S7712	
647	Seguridad en switches HP COMWARE Switches HP COMWARE	ENE 16
650	Seguridad en cortafuegos Fortigate Firewall security Fortigate	ABR 15
651	Seguridad en cortafuegos Cisco ASA Firewall security Cisco ASA	JUL 15
655	Guía de Securización Sun Solaris 9 con Oracle 10 Security Guide for Sun Solaris 9 with Oracle 10	DIC 07
656	Guía Securización Sun Solaris 9 con Oracle 10 y VCS 4.1 Guide for Sun Solaris 9 with Oracle 10 and VCS 4.1	DIC 07
660	Seguridad en Proxies. Ejem. Listas negras Proxies Security. Blacklist	MAY 14
661	Seguridad en Firewalls de Aplicación Application Firewalls Security	MAR 11
662	Seguridad en Apache Traffic Server Security of Apache Traffic Server	NOV 12
663	Seguridad en DNS (BIND) Security of dns (BIND)	ABR 14
664*	Passive DNS PASSIVE DNS	MAR 14
665	Configuración segura de SSH SSH secure configuration SSH secure configuration	OCT 14
671	Seguridad en Servidores Web Apache Security of Web Apache Server	DIC 06
672	Seguridad en Servidores Web Tomcat Security of Web Tomcat Server	ENE 09
673	Seguridad en Servidores Web Tomcat7 Security of Tomcat 7 Server	
674	Seguridad en GlassFish 3.1 Security in GlassFish 3.1	ENE 13
681	Seguridad en Servidores de Correo Postfix Security of Postfix Email Server	DIC 06
682	Configuración Segura de Sendmail Secure Configuration for Sendmail	ENE 10
691	Oracle Application Server 10gR2 para Red Hat 3 y 4 Oracle Application Server 10gR2 for Red Hat 3 y 4	DIC 07
692	Oracle Application Server 10gR2 para Solaris 9 y 10 Oracle Application Server 10gR2 for Solaris 9 y 10	DIC 07
693	Oracle Application Server 10gR2 para HP-UX 11i Security in Oracle Application Server 10gR2 for HP-UX 11i	DIC 07

Serie 800: Esquema Nacional de Seguridad

SERIE 800: NATIONAL SECURITY FRAMEWORK

800	Glosario de Términos y Abreviaturas Glossary of Terms and Abbreviations	MAR 11
801	Responsabilidades en el ENS Responsibilities in the National Security Framework	FEB 11
802	Auditoría del Esquema Nacional de Seguridad Audit for the National Security Framework	JUN 10
803	Valoración de Sistemas en el ENS Systems Evaluation in the National Security Framework	ENE 11
804	Implementación en el ENS Implementation measures in National Security Framework	MAR 13
805	Política de Seguridad de la Información Information Security Policy	SEP 11
806	Plan de Adecuación del ENS Adaptation Plan in the National Security Framework	ENE 11
807	Criptología de Empleo en el ENS Encryption in the National Security Framework	ABR 15
808	Verificación del Cumplimiento de las Medidas en el ENS Verification of Compliance with measures	SEP 11
809	Declaración de conformidad del ENS ENS declaration of conformity	MAY 16
810	Guía de creación de un CERT/CSIRT CERT/CSIRT construction guide	SEP 11
811	Interconexión en el ENS ENS interconnection	NOV 12
812	Seguridad en entornos y aplicaciones Web Security in web applications and enviroments	OCT 11
813	Componentes Certificados en el ENS ENS components certificates	FEB 12
814	Seguridad en corro electrónico Security in email	AGO 11
815	Indicadores y Métricas en el ENS Indicators and Metrics ENS	ABR 12

816	Seguridad en Redes Inalámbricas en el ENS Wireless Network Security ENS	
817	Gestión de Ciberincidentes Cyberincident Management	JUL 16
818	Herramientas de seguridad en el ENS Safety Tools National Security Scheme	OCT 12
819	Medidas compensatorias en el ENS ENS compensatory measures	
820	Guía de protección contra Denegación de Servicio DDoS protection guide	JUN 13
821	ENS. Normas de seguridad Safety rules	ABR 13
	Apéndice I. NG 00 Utilización de recursos y sistemas Resources and systems	
	Apéndice II. NP 10 Acceso a Internet Internet access	
	Apéndice III. NP 20 Correo Electrónico E-mail	
	Apéndice IV. NP 30 Trabajar fuera de instalaciones del organismo Work outside the body´s facilities	
	Apéndice V. NP 40 Creación y uso de contraseñas Passwords	
	Apéndice VI. NP 50 Acuerdo confidencialidad terceros Confidetiality with third parties	
	Apéndice VII. NP 60 Modelo de buenas prácticas para terceros Good practices with third parties	
822	Esquema Nacional de Seguridad. Procedimientos de Seguridad	OCT 12
	Anexo I .PR 10 Procedimiento de gestión de usuarios User Management	
	Anexo II. PR 20 Procedimiento de clasificación y tratamiento de la información clasificada Classification and treatment of classified information	
	Anexo III. PR 30 Procedimiento de generación de copias de respaldo y recuperación de la información Backup and recovery information	
823	Utilización de servicios en la nube Safety requirements CLOUD environments	ABR 14
824	Informe del estado de seguridad Security Status Report	OCT 16
825	Certificaciones 27001 27001 certificates	NOV 13
826	Esquema de certificación de personas Person certification schemes	
827	Gestión y uso de dispositivos móviles Management and use of mobile devices	MAY 14
828	Seguridad de las TIC en entidades locales de menos de 2.000 habitantes ICT Security local entities with less than 2.000 inhabitants	
830	Seguridad en Bluetooth en el marco del ENS Bluetooth security in ENS	SEP 16
831	Registro de actividad de usuario User activity log	
835	Borrado de metadatos en el marco del ENS Deleting metadata	MAR 17
836	Seguridad en VPN en el marco del ENS VPN security	
837	Seguridad en Bluetooth en el marco del ENS Bluetooth security	
844	INES – Informe Nacional del Estado de Seguridad. Manual de usuario INES, Status report on security. User manual	SEP 16
	INES – Anexo – I. Preguntas más frecuentes (FAQ)	SEP 16
	INES – Anexo-II. Recopilación de datos Data collection	OCT 16
	INES – Anexo-III. Formato para la creación del XML de incidentes propios en caso de no disponer de instancia propia de LUCIA Format for the creation of XML of own incidents in case of non-dispense of own LUCIA´s instance	NOV 16
845A	LUCIA. Manual de usuario LUCIA. User manual	ABR16
845B	LUCIA. Manual de usuario Sistema de Alerta Temprana (SAT) LUCIA. User manual with SAT	FEB 16
845C	LUCIA. Manual de instalación. Organismo LUCIA. Installation manual	FEB 17
845D	LUCIA. Manual de administrador LUCIA. Administrator manual	NOV 16

Cumple con el ENS
COMPLIES WITH ENS

Pendientes de publicar *
PENDING PUBLICATION

Difusión limitada
LIMITED DIFUSSION

Adaptables al ENS
ADAPTED TO ENS

Fuera de Soporte
OUT OF SUPPORT

** Confidencial
CONFIDENTIAL

850A	Seguridad en Windows 7 en el ENS (cliente en dominio) Windows 7 security in ENS (client within a domain)	AGO 14
850B	Seguridad en Windows 7 (cliente independiente) Windows 7 security in ENS (independent client)	OCT 14
851A	Seguridad en Windows 2008 Server R2 (controlador de dominio) Windows 2008 Server R2 security in ENS (domain controller)	AGO 14
851B	Seguridad en Windows 2008 Server R2 (servidor independiente) Windows 2008 Server R2 security in ENS (independent server)	AGO 14
859	Recolección y consolidación de eventos con Windows Server 2008R2 Collections and consolidation of events in Windows Server 2008 R2	ENE 15
860	Seguridad en el servicio de Outlook Web App del Microsoft Exchange Server 2010 Outlook Web App of Microsoft Exchange Server 2010 security	AGO 15
869	AppLocker en el ENS ENS AppLocker	OCT 15
870A	Seguridad en Windows 2012 Server R2 en el ENS Windows 2012 Server R2 security in ENS	JUL 15
870B	Seguridad Windows 2012 Server R2 en el ENS (servidor independiente) Windows 2012 Server R2 security (independent server)	AGO 15
871	Windows Server 2012 R2 como servidor de impresión Windows Server 2012 R2 (print server)	FEB 17
872	MS Windows Server 2012 R2 como servidor de ficheros MS Windows Server 2012 R2 File servr	FEB 17
873	MS Windows Internet Informations Server 8,5	DIC 16
880	Exchange Server 2013 sobre Windows Server 2012 R2	NOV 16
899A	MS Windows 10 (cliente miembro de dominio) MS Windows 10 (client within a domain)	NOV 16
899B	MS Windows 10 (cliente independiente) MS Windows 10 (independent client)	NOV 16

Serie 900: Informes técnicos
SERIE 900: TECHNICAL REPORTS

903	Configuración Segura de HP-IPAQ HP-IPAQ Secure Configuration	DIC 05
911A*	Ciclo de una APT APT geberal recomendations	JUN 13
911B*	Recomendaciones generales ante un APT APT general recomendations	JUL 13
912	Procedimiento de investigación de código dañino malware investigation procedure	JUN 13
920	Análisis de malware con Cuckoo Sandbox Análisis de malware con Cuckoo Sandbox	MAR 14
951	Empleo de la Herramienta Ethereal/Wireshark Using Ethereal/ Wireshark Tool	DIC 06
952	Empleo de la Herramienta Nessus Usage Recommendations for Nessus Tool	AGO 11
953	Recomendaciones de Empleo de la Herramienta Snort Usage Recommendations for Snort Tool	JUN 09
954	Recomendaciones de Empleo de la Herramienta Nmap Usage Recommendations for Nmap Tool	AGO 12
955	Recomendaciones de Empleo de GnuPG v.1.4.7 Usage Recommendations for GnuPG Tool v.1.4.7	DIC 07
955B	Recomendaciones de Empleo de GPG Usage Recommendations for GPG	DIC 16
956	Seguridad de entornos de computación virtuales Virtual Environments	DIC 07
957	Recomendaciones de empleo de TrueCrypt TrueCrypt recomendations	ENE 13
958	Procedimiento de empleo Crypto Token USB Crypto Token USB Employment Procedure	ENE 13
970**	Uso de Cifradores IP en Redes Públicas Use of IP Encryption in Public Networks	SEP 13
980	Arquitecturas de seguridad Security architectures	

En el ámbito de las Administraciones Públicas, el Centro Criptológico Nacional ha continuado concienciando y formando a funcionarios y empleados públicos. Existe ya una masa crítica de **6.117 personas formadas**, de manera presencial, en los diferentes aspectos de la seguridad de las tecnologías de la información. Estos cursos se realizan en colaboración con el Instituto Nacional de Administración Pública (INAP).

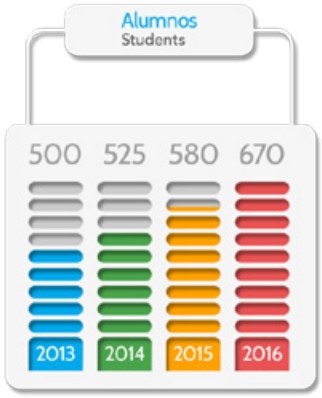
A ellas, se unen los **20.218 alumnos** inscritos en alguno de los nueve cursos *online* desarrollados por el CCN y disponibles en el portal del CCN-CERT. Cursos que están disponibles tanto en la parte pública como privada, incluyendo algunos *ad hoc* ofrecidos a diversos organismos, tanto nacionales como internacionales (Dirección General de la Policía, Ejército de Tierra, Armada, Oficina Nacional de Seguridad, México o Perú).

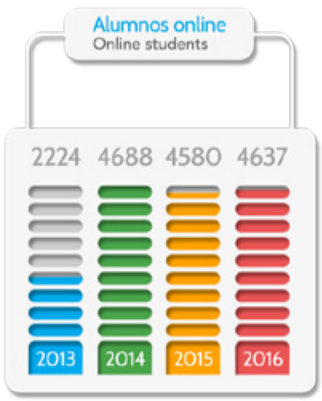
Como perspectiva para el 2017, se pretende incrementar la oferta de formación a distancia para entidades locales y comunidades autónomas, desarrollar cursos específicos para mejorar la eficiencia de los responsables de seguridad, firmar acuerdos con universidades para ofrecer formación *online* e implantar el I Curso Avanzado de Gestión de Incidentes de Ciberseguridad.

Within the Public Administration field, the National Cryptologic Centre has continued to raise awareness and train civil servants and state workers on different aspects of information technology security. A critical mass of 6,117 people have already been trained. These courses are run jointly with the National Public Administrations Institute (INAP).

This comes in addition to the 20,218 students registered on one of the nine online courses run by the CCN and available on the CCN-CERT portal. Courses are available both in the public and private sector including some "ad hoc" courses offered to different national and international organisations (Police, Army, Navy, National Security Office, Mexico and Peru).

With a view to 2017, the goal is to increase the distance learning offer for Local entities and Regions, develop specific courses to improve efficiency among security managers, sign agreements with Universities to offer online training and set up the Advanced Course on Cyber-Security Incident Management





Cursos 2015-2016

1. Cursos informativos y de concienciación en seguridad

- XII-XIII Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC). Fase *online*: 30 h./Fase Presencial: 50 h. TOTAL: 80h.

2. Cursos básicos de seguridad

- X y XI Curso Básico STIC- Infraestructura de Red. Fase *online*: 15 h./ Presencial: 25 h. TOTAL: 40 h.
- X y XI Curso Básico STIC- Base de Datos.25 h.

3. Cursos específicos de gestión de seguridad

- XII y XIII Curso de Gestión STIC y del ENS. Fase *online*: 30 h. / Presencial 50 h. TOTAL: 80 h.
- XXVI y XXVII Curso de Especialidades Criptológicas. **Fase** *online*: 125 h./ Presencial: 75. TOTAL: 200 h.

4. Cursos de especialización en seguridad

- X y XI Curso STIC - Seguridad Redes Inalámbricas. Presencial: 25 h.
- IV y V Curso STIC- Seguridad Dispositivos móviles. Presencial: 35 h.
- VII y VIII Curso STIC- Seguridad Aplicaciones Web. Presencial: 25 h.
- XI Curso STIC- Cortafuegos. Presencial: 25 h.
- XI y XII Curso STIC- Detección de Intrusos. Fase ***online***: 15 h./ Presencial: 25 h. Total: 40 h.
- XII y XIII Curso Acreditación STIC- Entornos Windows. Fase ***online***: 15 h./ Presencial: 25 h. Total: 40 h.
- VIII y IX Curso STIC- Búsqueda de Evidencias. Presencial: 25 h.
- X y XI Curso STIC- Inspecciones de Seguridad. Presencial: 25 h.
- VI y VII Curso STIC- Herramienta PILAR. ***Fase online***: 10 h. / Presencial 25h. Total: 35 h.
- I y II Curso STIC- Gestión Incidentes Ciberseguridad. Presencial: 25 h.

STIC Courses

1. Security Information and Awareness Courses

- XII-XIII Course about Security Information and Communication Technologies (SICT). Blended learning.

2. Basic Security Courses

- X-XI Basic SICT Course - Network Infrastructure. Blended learning.
- X-XI Basic SICT Course – Databases.

3. Specific Courses on Security Management

- XII-XIII SICT Management Course. Application to ENS. Blended learning.
- XXVI-XXVII Cryptologic Specialized Course. Blended Learning.

4. Courses Specializing on Security

- X-XI SICT Course - Wireless Networks
- IV-V SICT Course – Security in Mobile Devices
- VII-VIII SICT Course – Security in Web Applications
- XI SICT Course – Firewall
- XI-XII SICT Course - Intrusion Detection. Blended learning
- XII- XIII Accreditation SICT Course - Windows Environment. Blended Learning
- VIII-IX SICT Course – Search for Evidence and Integrity Control
- X-XI SICT Course – Security Inspections
- VI-VII SICT Course – PILAR Tool (online)
- I-II SICT Course – Incident Handling

4.2.2 Cursos exclusivos de Formación online
Exclusive on-line training courses

Durante 2015 y 2016, el Centro Criptológico Nacional ha ido ampliando su oferta formativa, adaptándose a las demandas de muchos usuarios y facilitando, a través de métodos de enseñanza a distancia y ***e-learning***, algunos de sus cursos más demandados. Los cursos disponibles en el portal del CCN-CERT (www.ccn-cert.cni.es) son los siguientes:

1. Cursos públicos

Los cursos disponibles en la parte pública son accesibles para todos los usuarios, pero son meramente informativos. Al no contar con registro de datos, no es posible generar ningún tipo de certificación.

- Esquema Nacional de Seguridad
- Análisis y Gestión de Riesgos de los Sistemas de Información

2. Cursos privados

En la parte privada existe una oferta de cursos más amplia. En caso de que se desee obtener un certificado de finalización, se accederá a los cursos de esta parte del portal (solo para usuarios registrados).

- Curso INES (Informe Nacional del Estado de la Seguridad)
- Curso básico STIC - Seguridad en entornos Windows
- Curso básico STIC - Seguridad en entornos Linux
- Curso de Análisis y Gestión de Riesgos de los Sistemas de Información
- Curso del Esquema Nacional de Seguridad
- Curso de Seguridad de las Tecnologías de la Información y las Comunicaciones

3. Cursos CCN-INAP (fase ***online***)

Estos cursos corresponden con la fase ***online*** de los cursos impartidos por el CCN en colaboración con el **Instituto Nacional de Administración Pública (INAP)**. El acceso está reservado a los alumnos que hayan resultado seleccionados tras el correspondiente proceso de inscripción en la plataforma del INAP. Además, en los cursos impartidos en colaboración con el INAP se han creado o adaptado las siguientes fases ***online*** durante 2015 y 2016:

- XII y XIII Curso de Gestión STIC y del ENS. Fase ***online***: 30 h./ Presencial 50 h. TOTAL: 80 h.
- XXVI y XXVII Curso Especialidades Criptológicas. Fase ***online***: 125 h./ Presencial: 75. TOTAL: 200 h.
- Curso de Infraestructura de Red. Fase ***online***: 15 h./Presencias 25 h.. Total 40h.

During 2015 and 2016, the National Cryptologic Centre has been widening its training offer, adapting to many users' demands and providing some of their most sought-after courses through distance learning and e-learning methods. The following courses are available on the CCN-CERT portal (www.ccn-cert.cni.es):

1. Public courses

Courses available in the public area are available for all users but merely provide information. As users are not registered, it is not possible to receive any type of certification.

- National Security Framework
- Risk Analysis and Management in Information Systems

2. Private Courses

The private area has a wider offer of courses. In the event that you wish to obtain a completion certificate, courses can be accessed from this section of the portal (registered users only).

- INES Course
- Basic Security Course. Windows environment
- Basic Security Course. Linux environment
- Information System Risk Analysis and Management Course
- National Security Framework Course
- SICT Information and Communication Technology Security Course

3. CCN-INAP courses (online phase)

These courses correspond to the online phase for courses given by the CCN in collaboration with the National Institute of Public Administration (INAP). Access is limited to students who have been selected through the corresponding registration process on the INAP platform. In addition, for joint courses with INAP, the following online phases have been created or adapted during 2015 and 2016:

- Intrusion Detection Course (online phase).
- Cryptologic Specialized Course (online phase).
- Network Infrastructure Course (online phase).

Una de las funciones del Centro Criptológico Nacional es la de coordinar la promoción, desarrollo, obtención, adquisición, puesta en explotación y utilización de la tecnología de la seguridad de los sistemas TIC que incluyan cifra, para procesar, almacenar o transmitir información de forma segura. Este capítulo de I+D es fundamental para garantizar la seguridad de los sistemas TIC y representa un apoyo al desarrollo de empresas españolas que apuestan por la innovación.

One of the functions of the National Cryptologic Centre is to coordinate the promotion, development, obtaining, acquisition, start-up and use of security technology for CIS systems, including encryption, to process, store or transmit information securely. This R+D chapter is fundamental to guarantee CIS system security and it represents support for developing Spanish companies that back innovation.

Durante los años 2015 y 2016, el CCN ha participado y/o llevado la dirección técnica en los siguientes proyectos:

During 2015 and 2016, the CCN has participated and/or run technical management of the following projects:

Cifrador IP europeo EP430GU
EP430GU European IP Crypto

Sistema de cifrado que protege las comunicaciones multimedia (voz IP, vídeo, datos, etc.) y permite el despliegue de redes privadas virtuales (VPN) de un modo seguro. Está financiado en parte con fondos I+D del **Programa Galileo**, desarrollado por Epicom, bajo la dirección técnica del CCN.

Con esta versión europea se espera conseguir la certificación de España como nación **AQUA** (***Appropriated Qualified Authority***) lo que permitirá ingresar a nuestro país en el selecto grupo de naciones europeas con esta capacidad.

Una vez finalizado su desarrollo en 2015, comenzó su evaluación funcional en 2016 y se le ha otorgado una aprobación interina para procesar **información nacional clasificada**.

Encryption system that protects multimedia communications (voice IP, video, data, etc.) and allows virtual private networks (VPN) to run in safe mode. It is partly financed with **Galileo Programme** R&D funding, **technically managed** by the CCN and developed by Epicom. With this European version, it is hoped that Spain will acheive **AQUA** (Appropriated Qualified Authority) certification, making our country one of the select European nations with this capability.

Once completely developed in 2015, its **functional certification** began in 2016 and it was given an interim approval to process **classified national information**.

Prototipo de Cifrador Personal para el Combatiente (CIFPECOM-2)
Crypto device prototype for dismounted soldier (CIFPECOM-2)

En su versión hardware, desarrollado por Tecnobit, el CIFPECOM permite proteger la información clasificada, tanto la voz como los datos, para su transmisión a través de la Red Radio de Combate (RRC). Asimismo, en su versión software (librería cripto) cifra los datos generados por un sistema de mando y control (TALOS) para su envío vía RRC. Este proyecto ha contado con financiación de I+D de la Dirección General de Armamento y Material del Ministerio de Defensa (DGAM) durante los años 2015 y 2016.

CIFPECOM hardware can protect classified information, both voice and data, for transmission over the Combat Radio Net (CRN). In addition, its software (crypto library) encodes the data generated by a command and control system (TALOS) to be sent via the CRN.

This project received R&D financing from the Ministry of Defence (DGAM) during 2015 and 2016.

Evolución de COMSec Admin
Evolution of COMSec Admin

Sistema de comunicaciones móviles seguras creado por la empresa española Indra SCS para su uso en la Administración española, con el objetivo de asegurar la confidencialidad de las comunicaciones de voz y mensajería. Durante 2016, el CCN ha trabajado en la evaluación funcional y criptológica de la nueva versión de esta solución (COMSec Admin+).

Secure mobile communications system created by Spanish company INDRA SCS for use in the Spanish Administration, with the aim of ensuring confidentiality for voice and message service communications. During 2016, the CCN worked on the **functional and cryptological evaluation** of the new version of this solution (COMSec Admin+).

Evolución SecVoice
SecVoice evolution

Durante 2016 ha comenzado la evolución de SecVoice (solución de comunicaciones móviles seguras basada en SCIP) para adaptarse a los nuevos sistemas operativos. Igualmente, se ha iniciado la evaluación funcional de dicha solución.

The evolution of SecVoice began in 2016 (secure mobile communications solution in SCIP) to adapt to new operating systems. In the same way, **functional evaluation** of this solution has begun.

Prototipo de Pasarela militar para entornos tácticos
Military Gateway prototype for tactical environments

Iniciado el desarrollo de esta pasarela que permitirá el intercambio de información a través de servicios web entre nodos CSD (***Coalition Share Database***), pertenecientes a la comunidad MAJIIC de las Fuerzas Armadas, que podrán estar ubicados en la misma o en distintas redes (OTAN, países aliados, redes públicas, etc.) o dominios de seguridad.

Este proyecto, desarrollado por Autek, ha contado con la financiación de I+D de la DGAM durante los años 2015 y 2016 y con la dirección técnica del CCN.

Having started to develop this gateway that will allow information exchange through web services between **CSD** (Coalition Share Database) nodes, belonging to the MAJIIC Armed Forces community, that might be located in the same or in different networks (NATO, allied countries, public networks, etc.) or security domains.

This project, developed by Autek, received R&D financing from the DGAM during 2015 and 2016 and worked with the **CCN technical board**.

Prototipo de pasarela para la herramienta de compartición de información, MISP
Gateway prototype for the MISP information sharing tool

Permite el intercambio seguro y controlado de información sobre código dañino entre dos instancias que se encuentran en redes diferentes interconectadas.

El prototipo se concibió para permitir la interconexión de dos instancias de la herramienta REYES (véase capítulo correspondiente) situadas en redes con distinta clasificación de seguridad. En su primera versión, financiada íntegramente por el CCN y desarrollada por la empresa Autek, solamente implementa el control de flujo de entrada desde la red interna a la externa.

Allow secure and controlled information exchange on malware between two interconnecting authorities in different networks.

The prototype was designed to allow interconnection of two REYES tool authorities, (see corresponding chapter), located in networks with a different security classification. In its first version, **financed entirely by the CCN** and developed by AUTEK, it only implements control of the incoming flow from the internal to the external network.

Diodo de datos
Data diode

Dispositivo de protección de perímetro cuya función principal es interconectar redes rompiendo la continuidad del protocolo de comunicaciones y obligando a que el flujo de información sea en un solo sentido. Se utiliza en interconexiones de redes o sistemas de distinta clasificación, distinto nivel de confianza o dominios de seguridad, cuando no sea admisible que exista flujo de información desde el sistema de mayor nivel de seguridad al de menor nivel.

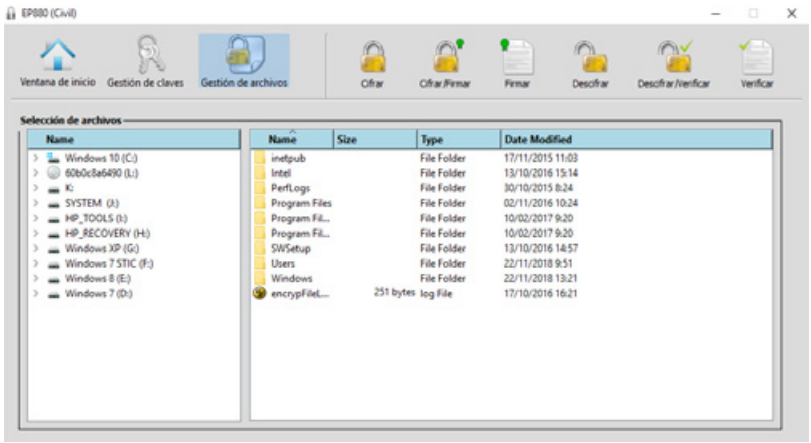
El producto final, desarrollado por la empresa Autek con fondos propios del CCN, permitirá conectar una red clasificada con otra red externa.

Perimeter protection device whose main function is to interconnect networks by breaking continuity of the communications protocol and making the information flow in just one direction. It is used in interconnections of networks or systems with different classifications, different trust levels or security domains, when it is not admissible for this information to flow from the System with the highest to the lowest level of security.

The final product, developed by AUTEK using **CCN own funds**, will allow a classified network to be connected up with another external network.

Software de Cifrado Offline – EP880
Offline Encrypted Software – EP880

Mediante el uso de certificados permite cifrar y firmar archivos para su posterior envío de forma segura por redes abiertas. El sistema posibilita el cifrado simultáneo para múltiples usuarios, protegiendo la confidencialidad y la autenticidad de los archivos cifrados y firmados con este método, mediante un software controlado.



Durante 2017 se realizará el desarrollo para su integración con Outlook y dará comienzo el proceso de evaluación, permitiendo de esta manera tener un producto nacional para el cifrado de ficheros offline.

Using certificates, it can encrypt and sign files to be subsequently sent securely through open networks. The system makes it possible to encrypt simultaneously for multiple users, protecting confidentiality and authenticity for files that are coded and signed with this method, using controlled software.

Development will be carried out during 2017 to integrate with Outlook and start the evaluation process, thereby giving a national product for encoding offline files.

Sistema Gestión del Crypto Token – EP585
Crypto Token Management System – EP585

Facilita la gestión de los equipos EP851v1, EP851v2 y EP852 simplificando la configuración, grabado y contabilidad de los dispositivos, la creación, exportación y control de las claves; así como las funcionalidades de cifrado y descifrado de los token, permitiendo la creación de circuitos de cifrado/descifrado entre carpetas.

It eases the management of EP851v1, EP851v2 and EP852 equipment by simplifying device configuration, recording and accounting, key creation, export and control; as well as the token functional features for encryption and decryption, allowing encryption/decryption circuits to be created between folders.

Otras colaboraciones del CCN, en la investigación y desarrollo de productos durante 2015 y 2016, fueron los siguientes proyectos:

Plataforma Färist Mobile
Färist Mobile Platform

Se ha colaborado con el CCEA (Ministerio de Defensa) en el despliegue e implantación del sistema TMSDEF, compuesto por la aplicación **Secvoice** de la empresa española Tecnobit, instalada en la plataforma segura Färist Mobile de la empresa sueca TUTUS Data AB. Esta solución proporciona comunicaciones móviles seguras de voz y datos.

Joint project with the CCEA (Ministry of Defence) on deployment and establishment of the TMSDEF system, comprising the **Secvoice** application by the Spanish company Tecnobit, installed on the Färist Mobile secure platform run by the Swedish company TUTUS Data AB. This solution provides secure mobile communications for voice and data.

Pruebas de interoperabilidad NINE (NISWG)
NINE inter-operability tests (NISWG)

El CCN organizó la 15° reunión del grupo de trabajo de OTAN para la especificación de interoperabilidad NINE. Entre los fabricantes presentes se encontraban las empresas españolas Epicom y Tecnobit que realizaron las pruebas de interoperabilidad con sus productos EP430T9 y el CIFPECOM respectivamente. La primera de ellas, Epicom, con el fabricante estadounidense VIASAT (IPS-250X) y con el italiano Leonardo (emulador).

Asímismo, Tecnobit también consiguió establecer comunicaciones con el fabricante polaco TRANSBIT (RP-101-NINE).

The CCN organised the 15th meeting of the NATO working group for the NINE interoperability specification. Attending manufacturers included Spanish companies Epicom and Tecnobit who performed interoperability tests with their EP430T9 products and CIFPECOM respectively. The former, Epicom, worked with the American manufacturer VIASAT (IPS-250X) and the Italian Leonardo (emulator).

In addition, Tecnobit also managed to set up a contact with Polish manufacturer TRANSBIT (RP-101-NINE).

Pruebas de interoperabilidad, durante el 15° NISWG, entre España (EPICOM) y EEUU (Viasat), así como entre España (EPICOM) y Polonia (TRANSBIT).
Interoperability tests during the 15th NISWG between Spain (EPICOM) and USA (Viasat), and between Spain (EPICOM) and Poland (TRANSBIT).

Catálogo de Productos Cualificados
Qualified Product Catalogue

4.3.1

La finalidad de este catálogo es ofrecer un listado de productos STIC supervisado por el CCN que proporcione un nivel mínimo de confianza al usuario final en los productos adquiridos (con mejoras de seguridad derivadas del proceso de evaluación y certificación) y en su empleo seguro (garantizado por un Procedimiento de Empleo) en las redes de la Administración.

A lo largo del 2016 se ha avanzado en el desarrollo del apartado de "Productos Cualificados de seguridad TIC", dentro del **Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicaciones (CPSTIC)** que estará recogido en la guía CCN-STIC 105. El trabajo se ha concretado en las siguientes actividades:

- Desarrollo de la guía **CCN-STIC-106** de procedimiento de inclusión de un producto de seguridad TIC cualificado en el CPSTIC (próxima publicación).
- Desarrollo de una taxonomía de productos de seguridad TIC y definición de unos Requisitos Fundamentales de Seguridad (RFS) para cada familia de productos. Estos documentos estarán incluidos dentro de la guía **CCN-STIC-140** de próxima publicación.

The purpose of this catalogue is to offer a list of STIC products supervised by the CCN that provides a minimum trust level for the end user when purchasing products (with security improvements derived from the evaluation and certification process) and for its secure use (guaranteed by an operational doctrine) in the Administration networks.

Over 2016, progress has been made in developing the CIS Qualified Security Products section within the Information and Communication Technologies Security Product Catalogue (CPSTIC) compiled in the CCN-STIC-105 guide. The work has been specified in the following activities:

- Development of the **CCN-STIC-106** guide (next publication). Procedure to include an qualified CIS security procedure in the CPSTIC.
- Development of a taxonomy for CIS security products and definition of Fundamental Security Requirements (RFS) for each product family. Documents included in the **CCN-STIC-140** guide (next publication).

Apoyos técnicos más significativos
Most significant technical supports

4.3.2

Durante el período 2015 y 2016, el CCN realizó una intensa actividad de apoyo técnico a distintos desarrollos, entre los que destacan:

- Asesoramiento a diferentes organismos de la Administración sobre las características técnicas, configuración y uso de productos de cifra y de sistemas de intercambio seguro de información, así como para la adquisición o desarrollo de **sistemas de protección TEMPEST**.
- Gestión y programación de los algoritmos de cifrado en todos los equipos producidos por Epicom para la Administración del Estado.
- Asesoramiento en el empleo de la **criptología en el ENS**.
- Apoyo a las Oficinas de Programa del Ministerio de Defensa, en grupos de trabajo internacionales sobre aspectos de seguridad de las comunicaciones (COMSEC), de la información (INFOSEC) y contra emanaciones no deseadas (TEMPEST) del avión militar de transporte A400M, del Eurofighter EF2000, así como sobre cuestiones de cifra en el Programa MIDS .
- Apoyo a la Comisión Permanente del Consejo Superior de la Administración Electrónica (CP CSAE), en la correcta definición de los Códigos Seguros de Verificación (CSV) de los distintos organismos de la Administración.

During 2015 and 2016, the CCN ran an intense technical support activity for different developments including:

- Consultancy advising different Administration Organisations on the technical features, configuration and use of crypto products and systems for exchanging information securely as well as acquiring or developing TEMPEST protection systems.
- Management and programming of encryption algorithms in all equipment produced by Epicom for the State Administration.
- Consultancy on the use of Cryptologic in the ENS.
- Support for the Ministry of Defence Programme Offices in international working groups on aspects of security for communications (COMSEC), information (INFOSEC) and against undesired emissions (TEMPEST) from the A400M military transport plane, the EF2000 Eurofighter, as well as regarding encoding in the MIDS Programme.
- Support for the Senior Electronic Administration Council Permanent Commission (CP CSAE) when correctly defining Secure Verification Codes (CSV) for the different Administration organisations.

El CCN ha participado en los paneles de seguridad de los proyectos internacionales clasificados, desarrollados por la industria española y patrocinados por los ministerios de Defensa, Fomento e Industria. Entre otros:

The CCN has taken part in security panels for classified international projects, developed by Spanish industry and sponsored by the Ministries of the Defence, Development and Industry. Among others:

Programa GALILEO
GALILEO Programme

Programa europeo de geoposicionamiento (GPS) en el que el CCN ha continuado participando en los distintos paneles y grupos de trabajo, como el de acreditación del sistema y los de labores de certificación y de seguridad de las comunicaciones (dirige el grupo de seguridad).

European Geopositioning Programme (GPS) where the CCN has continued to take part in the different panels and working groups, such as the system accreditation group and participating in communications security and certification tasks (it runs the security group).

Programa A-400M (avión militar de transporte)
A-400M programme (military transport plane)

El CCN ha continuado ejerciendo la dirección de la actividad COMSEC, representando los intereses españoles en el panel conjunto de acreditación y coordinando las actividades de certificación y radiación de emisiones radioeléctricas.

It has continued to run the programme's COMSEC activity board representing Spanish interests on the joint accreditation panel, coordinating activities concerning certification and radiation from radio-electric emissions.

Programa PAZ
PAZ programme

Asesoramiento en la topología de la red de este sistema espacial de observación de la Tierra en el espectro radar.

Consultancy regarding network topology for this spatial system observing the Earth in the radar spectrum.

Programa ARS ACCS
ACCS programme (Air Command and Control System)

Estudio de las condiciones de la arquitectura de red y asesoramiento en normativa y productos de seguridad para el intercambio seguro de información. Como resultado de este programa ha surgido el desarrollo de un diodo.

Study on the network architecture conditions and consultancy on standards and security products for secure information exchange. As a result of this programme, a diode has been developed.

Programa INGENIO
INGENIO programme

Se ha asesorado en la topología de la red del sistema.

Consultancy has been provided on the system network topology.

Programa EF2000 (avión militar de combate)
EF2000 programme (military fighter plane)

Se ha asesorado sobre las condiciones de seguridad del programa, modificando la estructura de algunos elementos de la red, especialmente en lo que se refiere a sus cifradores.

Consultancy has been provided on the programme's security conditions, modifying the structure of some network elements, particularly referring to its crypto systems.

Programa COALWNW (COALition Wideband Networking Waveform)
COALWNW programme (COALition Wideband Networking Waveform)

Pretende establecer un protocolo de radiocomunicaciones militares de banda ancha para interoperabilidad en despliegues de coalición entre las naciones participantes (Alemania, Australia, Canadá, España, Estados Unidos, Finlandia, Francia, Italia, Polonia, Reino Unido y Suecia).

El CCN representa a nuestro país en el "***Information Assurance Working Group***" (IAWG) de este programa, cuyo principal cometido es abordar todas las cuestiones relacionadas con seguridad criptográfica dentro del programa (COMSEC, TRANSEC, gestión de claves, etc.).

This programme to set a protocol for broadband military radio-communications for interoperability in coalition deployments between participating nationals (Germany, Australia, Canada, Spain, United States, Finland, France, Italy, Poland, United Kingdom and Sweden).

The CCN represents our country in the "Information Assurance Working Group" (IAWG) for this programme, whose main task is to tackle all questions related to cryptographic security for the programme (COMSEC,

Grupo de trabajo MICWG
MICWG working group

El principal cometido del MICWG (***MIDS international COMSEC working group***) dentro del programa internacional MIDS es tratar todos los temas COMSEC y, en particular, los relacionados con los nuevos desarrollos cripto correspondientes al BU2 (***Block Update 2***).

El CCN representa a España en este grupo de trabajo, el cual es gestionado y dirigido nacionalmente por la DGAM (Dirección General de Armamento y Material). A nivel internacional también se ha realizado la promoción de la industria nacional de cifra y seguridad realizando la visita a empresas nacionales y presentación de productos de cifra y seguridad a representantes de otras naciones, tales como Colombia, Perú, Finlandia o Francia .

The main task of the MICWG (MIDS International COMSEC Working Group) within the international MIDS programme is to tackle all COMSEC topics, particularly related to new crypto developments corresponding to BU2 ("Block Update 2").

The CCN represents Spain in this working group which is managed and run nationally by the DGAM. Internationally, the national encryption and security industry has been promoted by visiting national companies, presenting encryption and security products to representatives from other nations such as Colombia, Peru, Finland or France.

Se entiende por acreditación, la autorización otorgada a un sistema de información por la autoridad responsable de ellos 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 TIC que manejen información clasificada OTAN/UE o de otros Estados con los que España tiene suscritos acuerdos bilaterales es responsabilidad de la **Autoridad Nacional de Seguridad Delegada de la Información Clasificada** (definida en la persona del secretario de Estado director del CNI), que ejerce a través de la **Oficina Nacional de Seguridad (ONS)**, mientras que los aspectos técnicos de la acreditación son responsabilidad del CCN.

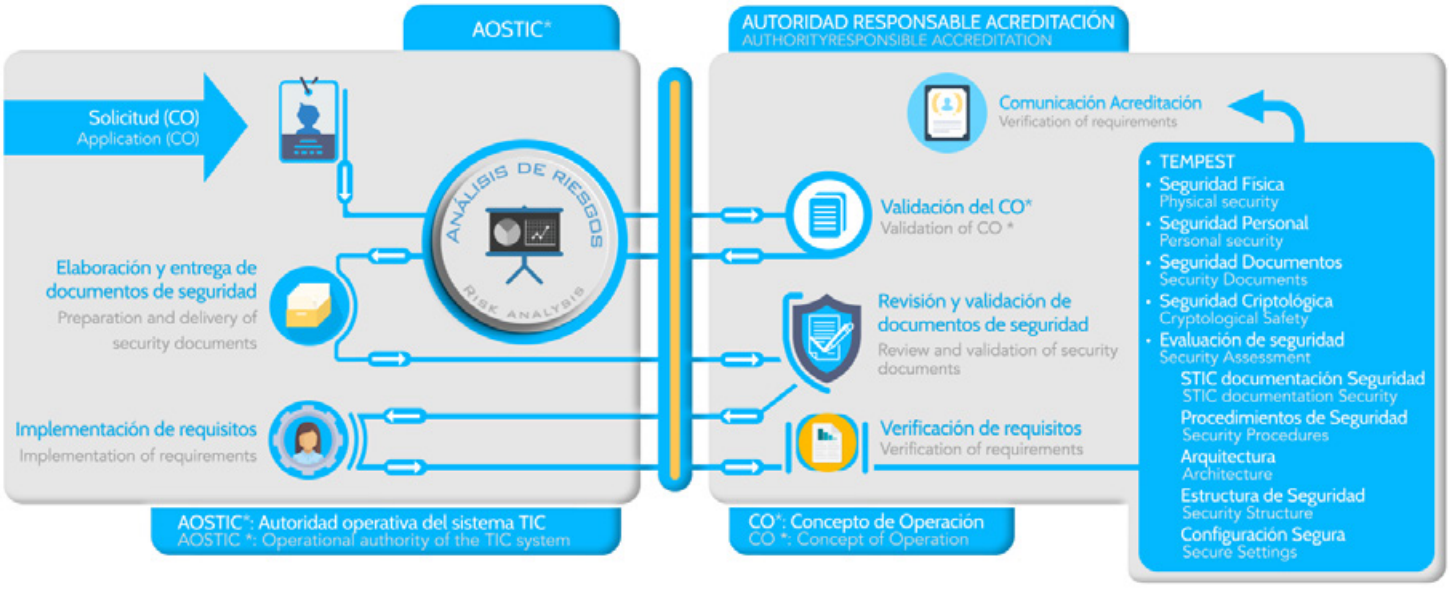
Antes de la acreditación de un sistema, es preciso implantar un conjunto de medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro para la información, las aplicaciones y los sistemas que sustentan a todos ellos.

Las inspecciones permiten verificar la seguridad implementada en un sistema y que los servicios y recursos utilizados cumplen con lo mínimo especificado y requerido.

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 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.

It is necessary to implant a set of measures, both procedural and technical/ organisational, giving a secure environment for the information, the applications and the Systems sustaining them. Security inspections can verify the security implemented in a System and that the services and resources used meet the specified and required minimum.

Procedimiento de Acreditación
Accreditation procedure



Dentro de las responsabilidades del CCN en este aspecto y, en concreto, de su grupo de Acreditación e Inspecciones de Seguridad, se han desarrollado, entre 2015 y 2016, 72 inspecciones STIC (frente a las 60 del período 2013-2014), previas a la acreditación de un sistema, cuyo resultado fue:

Within the CCN responsibilities in this aspect and specifically for its Security Accreditation and Inspections group, the following actions were run between 2015 and 2016:

- Acreditación completa de 14 ordenadores aislados y 18 sistemas completos. Entre otros:
  72 SICT inspections (60 in the period 2013-2014), prior to accrediting a system, whose result was:

NATO SECRET del Mando de Combate del Ejército del (MACOM).
NATO SECRET Combat Command of Spanish Air Force.

NATO SECRET WAN del Cuartel General del Ejército de Tierra
NATO SECRET WAN of Army Land Forces Headquarters.

NATO SECRET WAN de la Base de Retamares
NATO SECRET WAN Retamares Base

Fragatas F-100 de la Armada, 14 de ellas han completado el proceso
Frigate F-100 of Spanish Navy

- Autorización temporal de 32 sistemas para manejar información NATO SECRET. Entre otros:
  Temporary authorisations of 32 systems to handle NATO SECRET information for:

Buques de la Armada (para la realización de ejercicios)
Ships of Spanish Navy (for the accomplishment of exercises).

Extensiones de la Organización de la OTAN, BICES (***Battlefield Information Collection and Exploitation System***), en algunos ejercicios como el CSD B (***Coalition Share Database***)
Extensions of the NATO Organization, BICES (Battlefield Information Collection and Exploitation System), in some exercises such as CSD B (Coalition Share Database).

NRDC ESP (***Nato Rapid Deployment Corp de Bétera***)
NRDC ESP (NATO Rapid Deployment Corp de Bétera)

NATO SECRET del Mando Conjunto de Ciberdefensa
NATO SECRET of the Joint Cyber Defense Command (MCCD)

NATO SECRET WAN de la Brigada "Galicia" VII mientras se resolvían las deficiencias encontradas
NATO SECRET WAN of the Brigade "Galicia" VII while the deficiencies were solved.

Primer sistema de la Guardia Civil dentro del marco EUROSUR para Agencia Europea de Control de Fronteras Exteriores (FRONTEX)
First Civil Guard system within the EUROSUR framework for the European External Border Control Agency (FRONTEX).

- Colaboración con el Ejército del Aire en el diseño de la seguridad del ACCS (***Air Command & Control System***).
  Collaboration Air Force in designing security for the ACCS (Air Command & Control System).

Este mismo grupo de Acreditación e Inspecciones de Seguridad del CCN, como representante en diversos foros internacionales, entre ellos la agencia BICES de la OTAN, organizó en noviembre de 2016, el **74º Encuentro BSWG/BSAB& BTWG**. La conferencia, que tuvo lugar entre los días 14 y 18 de noviembre, reunió en Madrid a 105 representantes del Grupo de Seguridad de BICES (BSWG) y del Grupo de Acreditación (BSAB).

Security Accreditation and Inspections group, as representative in various international forums, including the BICES Agency of NATO, organized in November 2016 the 74th BSWG / BSAB & BTWG Meeting. The conference, which took place from 14 to 18 November, brought together 105 representatives of the BICES Security Group (BSWG) and the Accreditation Group (BSAB) in Madrid.

Esquema Nacional de Seguridad
National Security Framework

5

Adecuación y cumplimiento

En la disposición transitoria del Real Decreto 3/2010 se articula un mecanismo escalonado para la adecuación a lo previsto en el Esquema Nacional de Seguridad de manera que los sistemas de las administraciones deberán estar adecuados a este Esquema en unos plazos en ningún caso superiores a 48 meses desde la entrada en vigor del mismo. El plazo de adecuación ha vencido el 30 de enero de 2014.

Intrumentos adecuación

Su Serie 800 establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS y muy especialmente los siguientes documentos:

CCN-STIC 802 Guía de Auditoría
CCN-STIC 804 Guía de Implantación
CCN-STIC 808 Verificación cumplimiento medidas del ENS
CCN-STIC 815 Métricas e Indicadores
CCN-STIC 809 Declaración y Certificación Conformidad ENS. Distintivos Cumplimiento.
CCN-STIC 824 Informe Estado Seguridad
CCN-STIC 844 INES
CCN-STIC 47X Manual de uso PILAR

Conformidad

Consciente de la necesidad de dar publicidad a las garantías adoptadas en el desenvolvimiento de las Administraciones Públicas y el desarrollo del procedimiento administrativo prestado por medios electrónicos, el artículo 41 del ENS señala:

Artículo 41. Publicación de conformidad.

Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.

INES

El Esquema Nacional de Seguridad (ENS) establece la obligación de evaluar regularmente el estado de la seguridad de los sistemas por parte de las Administraciones Públicas. Así, su artículo 35 señala: "El Comité Sectorial de Administración Electrónica articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas". Asimismo, el ENS dispone la necesidad de establecer un sistema de medición de la seguridad del sistema estableciendo un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad, en los siguientes aspectos:

a) Grado de implantación de las medidas de seguridad.

b) Eficacia y eficiencia de las medidas de seguridad.

c) Impacto de los incidentes de seguridad.

Para cumplir con este mandato, el CCN ha desarrollado el proyecto INES (Informe Nacional del Estado de Seguridad) con el fin de facilitar la labor de todos los organismos. Este proyecto cuenta con una nueva plataforma telemática, a la que puede acceder desde este portal, que proporciona a las distintas Administraciones Públicas un conocimiento más rápido e intuitivo de su nivel de adecuación al ENS y del estado de seguridad de sus sistemas.

CLARA

Herramienta para analizar las características de seguridad técnicas definidas a través del Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. El análisis del cumplimiento está basado en las normas de seguridad que han sido proporcionadas a través de la aplicación de plantillas de seguridad, según las guías CCN-STIC de la serie 800: 850A, 850B, 851A, 851B, 870A y 870B.

Entidades de Certificación

La Entidad Nacional de Acreditación (ENAC) pone a disposición de los interesados el esquema de acreditación de entidades que quieran certificar el cumplimiento con el Esquema Nacional de Seguridad (ENS).

El esquema de acreditación ha sido desarrollado por ENAC en estrecha colaboración con el Ministerio de Hacienda y Función Pública (MINHAFP) y el Centro Criptológico Nacional (CCN).

En el caso de sistemas clasificados con el grado de DIFUSIÓN LIMITADA (DL) o equivalente, una entidad debe estar acreditada por ENAC en el ámbito de aplicación del Esquema Nacional de Seguridad conforme a la norma UNE-EN ISO/IEC 17065:2012 para poder certificar el cumplimiento de requisitos STIC. Además, las entidades auditoras de seguridad deben disponer de Habilitación de Seguridad de Empresa (HSEM) en vigor.

Como es sabido, el CCN, en colaboración con el entonces denominado Ministerio de Hacienda y Administraciones Públicas (MINHAP), participó activamente en el desarrollo e implantación del **Esquema Nacional de Seguridad (ENS)**, regulado por el **Real Decreto 3/2010, de 8 de marzo** y cuyo ámbito de aplicación es el sector público[2].

Cinco años después, en 2015, ambos organismos volvieron a tener un papel fundamental en la actualización del Esquema a través del **Real Decreto 951/2015, de 23 de octubre**, en respuesta a la evolución del entorno regulatorio (en especial de la Unión Europea), de la tecnología y de la experiencia de su implantación en los años precedentes.

Principales novedades del nuevo Real Decreto:

- Artículo 15. Las Administraciones públicas exigirán que las organizaciones que les presten servicios de seguridad cuenten con **profesionales cualificados**.
- Artículo 18. En la adquisición de productos de seguridad las AAPP utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan **certificada la funcionalidad** de seguridad relacionada con el objeto de su adquisición.
- Artículo 24. Despliegue de procedimientos de **gestión de incidentes** de seguridad, y de debilidades detectadas en los elementos del sistema de información.
- Artículo 27. Las medidas de seguridad se formalizarán en un documento denominado "**declaración de aplicabilidad**".
- Artículo 29. **Instrucciones técnicas de seguridad y Guías de seguridad** que se desarrollarán por iniciativa del Centro Criptológico Nacional y serán de obligado cumplimiento. De hecho, ya han sido publicadas dos Instrucciones Técnicas en el BOE de 2 de noviembre de 2016:
  - ITS de conformidad con el ENS
  - ITS de Informe del Estado de la Seguridad
- Artículo 35. Elaboración de un perfil general del **estado de la seguridad** en las AAPP. El CCN será el encargado de recoger y consolidar la información.
- Artículo 36. Las AAPP notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados.
- Artículo 37. El CCN-CERT (véase capítulo correspondiente) dará soporte y coordinación para el tratamiento de vulnerabilidades y resolución de incidentes.

It is common knowledge that the CCN, working with the then Ministry of Inland Revenue and Public Administrations (MINHAP), took an active part in developing the **National Security Framework (ENS)**, regulated by **Royal Decree 3/2010**, dated 8th March whose field of application is the Public Sector[2].

Five years later, in 2015, both organisations once again played a fundamental role in updating the Framework through **Royal Decree 951/2015, dated 23rd October** in response to changes in the regulatory environment (particularly the European Union), technology and experience in implanting it over the previous years.

Main new aspects of the new Royal Decree:

- Article 15 Public Administrations will require that the organisations providing them with security services employ **qualified professionals**.
- Article 18. Article 18 When purchasing security products, depending on the determined category of the system and security level, public administrations will use products with **certified functional security features** related to the subject of its purchase.
- Article 24. Article 24 Deployment of procedures for security **incident management** and weaknesses detected in information system elements.
- Article 27. The security measures will be formalized in a document called "**declaration of applicability**".
- Article 29. **Technical safety instructions and safety guides** that will be developed on the initiative of the National Cryptological Center and will be obligation to comply. In fact, two Technical Instructions have already been published (BOE November 2, 2016):
  - ITS in compliance with the National Security Framework.
  - ITS for the Security Status Report
- Article 35. Drafting a **general security status profile** in Public Administrations. The CCN will be in charge of compiling and consolidating the information.
- Article 36. The Public Administrations **will notify** the CCN about any **incidents** that have a significant impact on the security of information being handled and services being provided.
- Article 37. The CCN-CERT (see the corresponding chapter) will provide support and coordination to handle vulnerabilities and resolve incidents.

[2] Véase Guía CCN-STIC 830. Ámbito de Aplicación del ENS: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html
[2] See CCN-SICT 830 guide. ENS Field of Application: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

ESQUEMA NACIONAL DE SEGURIDAD

6 Principios básicos-Guía
6 Principles Basic-Guide

- a Seguridad integral/Full security
- b Gestión de riesgos/Risk management
- c Prevención, reacción y recuperación/Prevencion, reaction and recovery
- d Líneas de defensa/Lines of defense
- e Reevaluación periódica/Periodic reassessment
- f La seguridad como función diferenciada/Security as a differentiated function

15 Requisitos mínimos (obligado cumplimento)
15 Minimum requirements (obligation to comply)

75 Medidas de seguridad
75 Measures of security

- A Organización e implantación del proceso de seguridad.
  Organisation and implantation of the security process
- B Análisis y gestión de los riesgos
  Risk analysis and management
- C Gestión de personal
  Staff management
- D Profesionalidad
  Professionalism
- E Autorización y control de los accesos
  Authorization and access control
- F Protección de las instalaciones
  Protection of facilities
- G Adquisición de productos
  Purchase of products
- H Seguridad por defecto
  Default security
- I Integridad y actualización del sistema
  System integrity and update
- J Protección de la información almacenada y en tránsito
  Protection of information when stored and in transit
- K Prevención ante otros sistemas de información interconectados
  Prevention against other interconnected information systems
- L Registro de actividad
  Activity Register
- M Incidentes de seguridad
  Security Incidents
- N Continuidad de la actividad
  Work continuity
- O Mejora continua del proceso de seguridad
  Continuous improvement of the security process

Marco orgarnizativo
ORGANISATIONAL FRAMEWORK

El marco organizativo está constituído por un conjunto de medidas relacionadas con la organización global de la seguridad.

The organisational framework is made up of a set of measures related to overall organisation of security.

4

- Política de seguridad/SECURITY POLICY
- Normativa de seguridad/SECURITY STANDARD
- Procedimiento de seguridad/SECURITY PROCEDURE
- Proceso de autorización/AUTHORISATION PROCESS

Marco operacional
OPERATIONAL FRAMEWORK

El marco operacional está constituído por un conjunto de medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

The operational framework is made up of measures to be taken to protect how the system operates as a full set of components for a particular purpose

31

- Planificación/ACCESS CONTROL
- Control de acceso/AUTHORISATION PROCESS
- Explotación/EXPLOITATION
- Servicios externos/EXTERNAL SERVICES
- Continuidad del servicio/SERVICE CONTINUITY
- Monitorización del sistema/SYSTEM MONITORING

Medidas de protección
PROTECTION FRAMEWORK

Las medidas de protección se centrarán en activos correctos, según su naturaleza, con el nivel requerido en cada dimención de seguridad

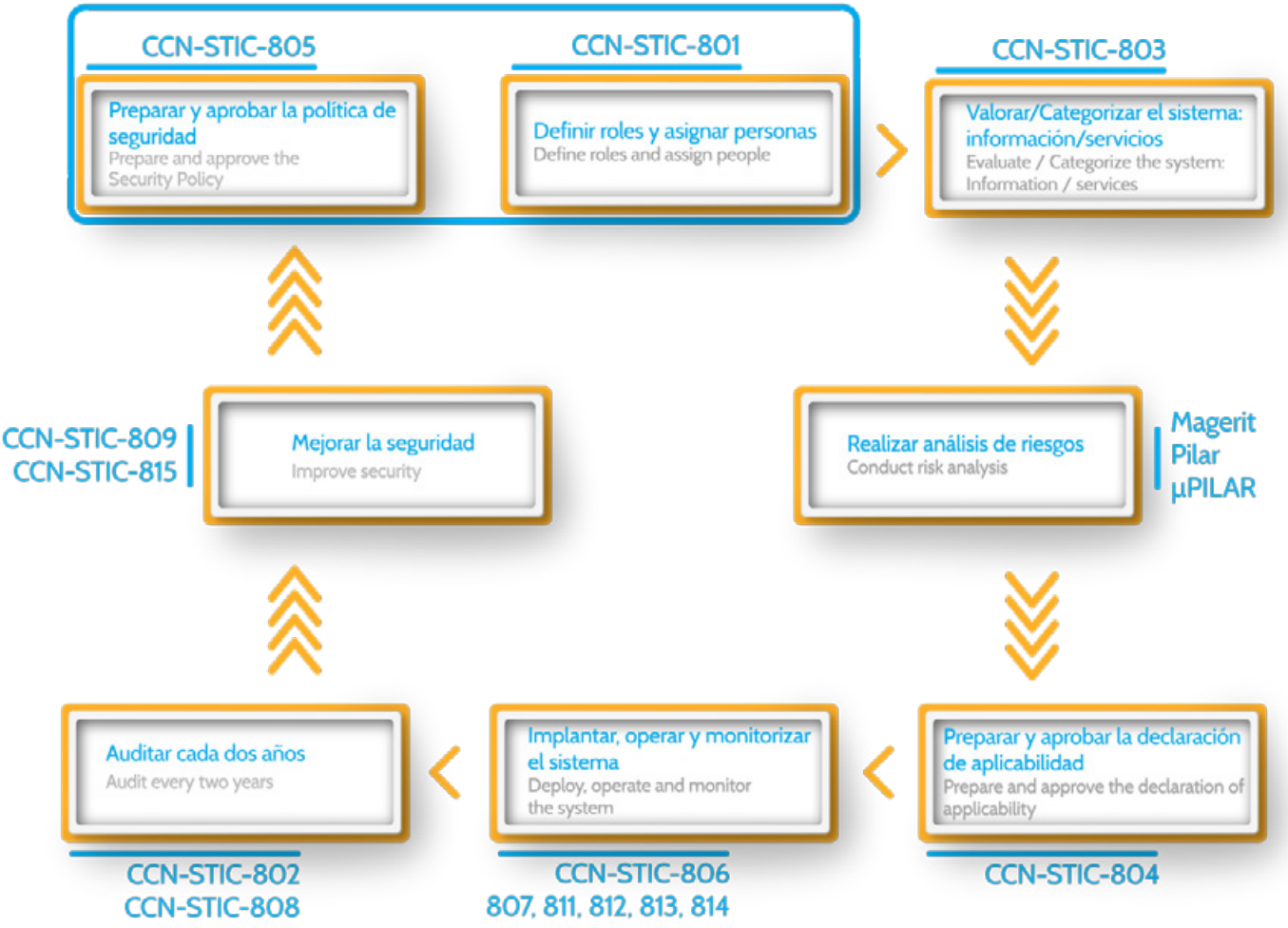
The protection measures focus on specific assets, depending on their nature, with the level required in each segurity dimension

40

- Instalaciones e infraestructuras/FACILITIES AND INFRASTRUCTURES
- Gestión del personal/STAFF MANAGEMENT
- Protección de los equipos/EQUIPMENT PROTECTION
- Protección de las comunicaciones/COMMUNICATION PROTECTION
- Protección soportes de información/INFORMATION SUPPORT PROTECTION
- Protección aplicaciones informáticas/COMPUTER APPLICATIONS PROTECTION
- Protección de la información/INFORMATION PROTECTION
- Protección de los servicios/SERVICE PROTECTION

Tal y como se ha señalado, todos los sistemas del ámbito de aplicación del ENS deberán adecuarse a él antes del 4 de noviembre de 2017. Las Guías CCN-STIC, las auditorías de servicios Web y las herramientas PILAR y CLARA (véase apartado correspondiente) pueden facilitar esta labor.

As previously mentioned, all systems in the ENS application field should adapt to it before 4th November 2017. The CCN-STIC Guides, the Web Services Audits and the PILAR and CLARA tools (see corresponding section) can make this work easier.



El RD del ENS establece, en su artículo 41, que los órganos y entidades de derecho público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.

Según la categoría del sistema se distingue entre:

a) **Declaración de conformidad:** de aplicación a sistemas de información de **categoría Básica**. Podrá representarse mediante sello o distintivo de declaración de conformidad generado por la entidad bajo cuya responsabilidad esté el sistema.

b) **Certificación de conformidad**: de aplicación **obligatoria** a sistemas de información de **categoría Media (lo son casi el 50% de los sistemas de la Administración) o Alta** y voluntaria en el caso de sistemas de información de categoría Básica.

The ENS RD establishes, in article 41, that the bodies and the Public Law Entities will publicise declarations of compliance in the corresponding electronic headquarters, plus any security emblems they have been awarded, obtained for compliance with the National Security Framework.

The system category distinguishes between:

a) **Conformity Declaration:** to be applied to **Basic category** information systems. This could be represented by means of a Compliance Declaration Seal or Emblem generated by the entity responsible for the system.

b) **Compliance Certificate:** must be applied to **Medium** (almost 50% of the Administration's systems) **or High category** information systems and voluntary in the case of Basic category information systems.

Las entidades que pueden certificar el grado de cumplimiento con el ENS de un organismo deben estar acreditadas por la **Entidad Nacional de acreditación (ENAC)** conforme a la norma UNE-EN ISO/IEC 17065:2012 Evaluación de la conformidad, con la excepción de los organismos de la Administración entre cuyas competencias se incluye el desarrollo de auditoría de sistemas de información y así conste en su normativa.

Por este motivo, la citada entidad ha desarrollado, junto con el CCN y el Ministerio de Hacienda y Función Pública, un Esquema de Acreditación para aquellas organizaciones que deseen certificar el cumplimiento con el ENS. De momento, son cuatro las empresas en vías de acreditación.

Regarding entities that can certify their degree of compliance with the ENS for an Organisation, they should be accredited by the **National Accreditation Entity (ENAC)** in compliance with the UNE-EN ISO/IEC 17065:2012 standard. Compliance evaluation.

For this reason, working with the CCN and the Ministry of Inland Revenue and Public Administration, the aforementioned entity has developed an Accreditation Framework for organisations that wish to certify compliance with the ENS. For the time being, there are four companies currently applying for credentials and once the process has begun they will be authorised to carry out ENS certifications in organisations for a year.

Las Administraciones Públicas deben adecuarse a las medidas de seguridad previstas en el Esquema Nacional de Seguridad (ENS) e informar regularmente del estado de sus sistemas de forma que se pueda elaborar un perfil general de toda la Administración. Es precisamente el Centro Criptológico Nacional el organismo encargado de articular los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación.

Public Administrations should adapt to the security measures envisaged in the National Security Framework (ENS) and provide regular **information** on the state of their systems so that a **general profile** can be drawn up for the entire Administration. The National Cryptologic Centre is the very Organisation in charge of articulating procedures required to collect and consolidate the information, as well as the methodological aspects for its processing and exploitation.

Para cumplir con este mandato, el CCN ha desarrollado el proyecto **INES (Informe Nacional del Estado de Seguridad)** que cuenta con una plataforma telemática, a través de la cual, los organismos pueden tener un conocimiento más rápido e intuitivo de su nivel de adecuación al ENS y del estado de seguridad de sus sistemas.

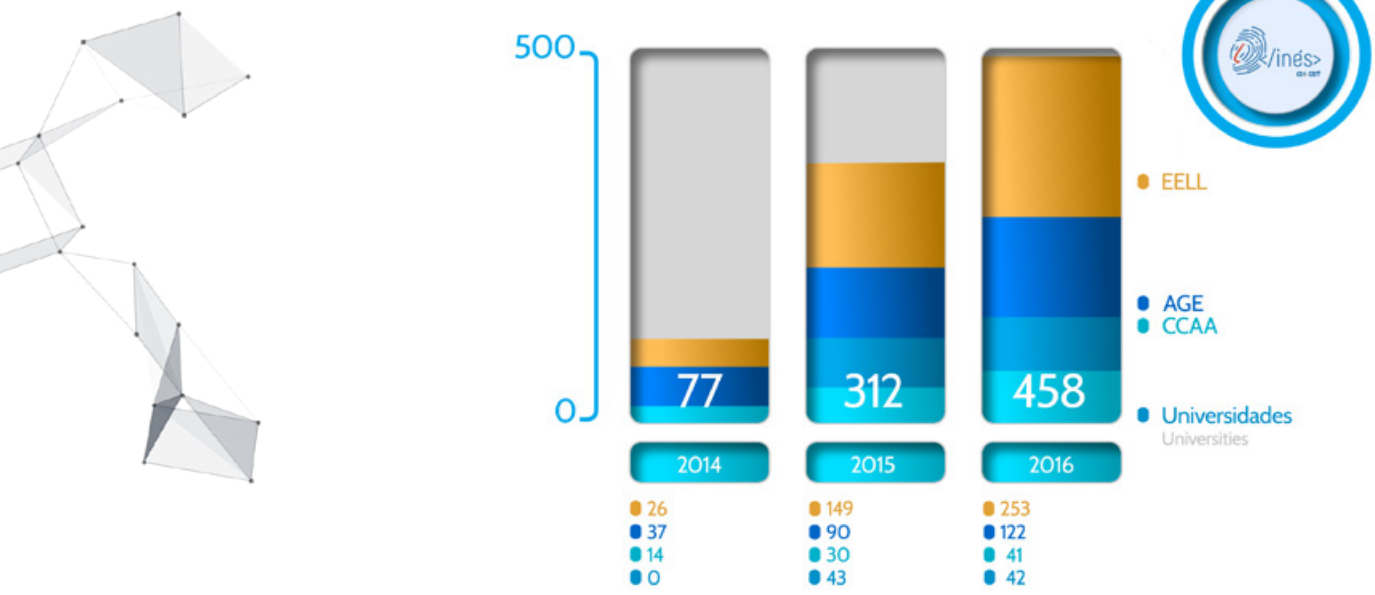
In order to comply with this mandate, the CCN has developed the **INES (National Security State Report)** project that has a data transmission platform through which the organisations can get faster and intuitive knowledge of their level of adaptation to the ENS and the state of security in its systems.

De este modo, desde el año 2014 se viene recopilando la información anualmente de forma que pueda verse la evolución del país y que cada organismo pueda cotejar su posición particular respecto de la media nacional.

In this way, information has been compiled annually since 2014 so that after a few years it will be possible to see how the country is evolving and each organisation will be able to simultaneously check its position against the national average.

Hasta la fecha, el CCN ha elaborado **tres Informes Nacionales del Estado de Seguridad** en función de los datos recogidos en INES. Se ha alcanzado una participación de 458 organismos en 2016 (frente a los 77 de 2014 con un aumento del 495%), procedentes de la Administración General del Estado, comunidades autónomas, entidades locales y universidades (invitadas a través de la Conferencia de Rectores de Universidades Españolas –CRUE-).

To date, the CCN has drawn up three national Security Status Reports according to data compiled in INES, with participation from 458 organisations in 2016 (77 in 2014), from the General State Administration, Regions, Local Entities and Universities (invited through the Spanish University Deans' conference - CRUE).



CCN-CERT, DEFENSA FRENTE A LAS CIBERAMENAZAS
CCN-CERT, DEFENSE AGAINST CYBERTHREATS

6

En el año 2006, y con el fin de incrementar las capacidades de prevención, detección, análisis, respuesta y coordinación antes las amenazas provenientes del cibersespacio, se creó en el seno del Centro Criptológico Nacional, el CCN-CERT[3]. Nace como CERT Gubernamental/Nacional español y sus funciones quedan recogidas en la Ley 11/2002 del Centro Nacional de Inteligencia, el RD 421/2004 del CCN y en el RD 3/2010, de 8 de enero, del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre y por la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del sector público.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a sistemas del sector público, a empresas y organizaciones de interés estratégico para el país, en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), y a cualquier sistema clasificado.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques y afrontar de forma activa las ciberamenazas.

Es competencia del CCN-CERT la gestión de ciberincidentes que afecten a sistemas del sector público, a empresas de interés estratégico, en coordinación con el CNPIC, y a cualquier sistema clasificado

In 2006, in order to increase prevention, detection, analysis, response and coordination capabilities in the light of threats from cyberspace, the CCN-CERT[3] was set up in the heart of the National Cryptologic Centre. It was created as a Spanish **Governmental/National CERT** and its functions are compiled in Law 11/2002 on the National Intelligence Centre, RD 421/2004 on the CCN and in RD 3/2010, dated 8th January on the National Security Framework (ENS), modified by RD 951/2015 dated 23rd October by Law 40/2015, dated 1st October on the Public Sector Legal Regime.

In accordance, the CCN-CERT is authorised to manage cyber incidents that affect **public sector** systems, **companies and organisations of strategic interest** for the country, in coordination with the National Centre for the Protection of Critical Infrastructures (CNPIC) and any **classified system**.

Its assignment is therefore to help improve **Spanish cyber-security** as the alarm and national response centre that cooperates and helps provide a fast and effective response to cyber-attacks and actively tackle cyber-threats.

Esta misión se desarrolla a través de numerosos servicios, en constante actualización en función de los nuevos riesgos y amenazas. Entre los principales se encuentran:

This assignment encompasses several services, constantly being updated depending on new risks and threats. Main services include:

- Gestión de incidentes. SAT/LUCIA
  Handling incidents. SAT/LUCIA
- Formación y sensibilización
  Training and awareness raising
- Guías de seguridad
  Security Guides
- Herramientas
  Tools
- Informes, avisos y vulnerabilidades
  Reports, warnings and vulnerabilities
- Auditorías de seguridad y páginas web
  Security Audits and Web Pages
- Capacidad forense y de ingeniería inversa
  Forensic and Reverse Engineering

[3] CERT, acrónimo de ***Computer Emergency Response Team***, es un término empleado en la comunidad internacional para definir a un equipo de expertos en ciberseguridad responsable de las capacidades de detección, contención y respuesta a un incidente. Marca registrada propiedad de la universidad estadounidense de Carnegie Mellon que autorizó al CCN-CERT a utilizar la citada denominación.
[3] CERT, acronym for Computer Emergency Response Team, is a term used in the international community to define a Team of Cyber-Security Experts in charge of detecting, containing and responding to an incident. The trademark is owned by Carnegie Mellon University in the USA that authorised the CCN-CERT to use this brand.

El principal servicio que proporciona el CCN-CERT a todo el sector público y a las empresas de interés estratégico es el de la gestión de incidentes. El CCN ofrece apoyo técnico y operativo en las distintas etapas del proceso: detección, análisis, notificación, respuesta, tratamiento y erradicación. De hecho, el CERT Gubernamental Nacional recibe diariamente más de dos millones y medio de eventos susceptibles de ser ciberincidentes y solo una ínfima parte (alrededor de 57 al día), se convierten en tales.

El CCN-CERT gestionó en el año 2016 un total de 20.940 ciberincidentes detectados en el sector público y en empresas de interés estratégico. Esta cifra representa un incremento del 14,5% con respecto al año 2015 en el que se gestionaron 18.232 incidentes. De ellos, el 3,6% fueron considerados como "muy alto" o "crítico", en función del grado de peligrosidad (tipo de amenaza, origen, perfil de usuario afectado, número o tipología de los sistemas afectados, impacto, etc.). Este tipo de ataques ("críticos", "muy alto" y "altos") son, tal y como señala el Esquema Nacional de Seguridad en su artículo 36, de obligada notificación al CCN por parte de todo el sector público (véase Guía CCN-STIC 817 de Gestión de Ciberincidentes y Guía CCN-STIC 830 del Ámbito de aplicación del ENS).

En este sentido, se está trabajando con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) para la coordinación de la notificación de incidentes en el caso de infraestructuras críticas que pertenezcan a operadores del sector público.

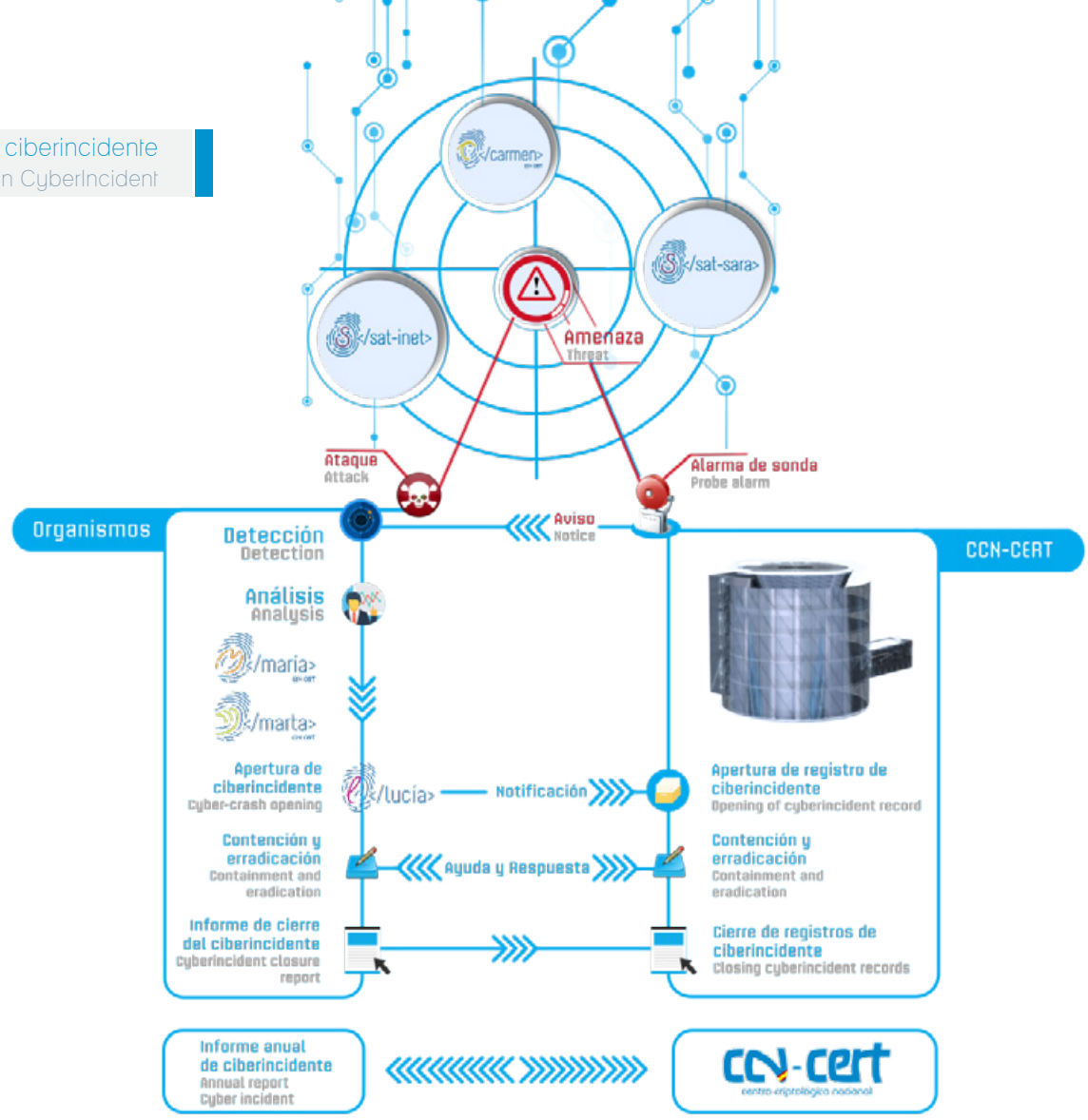
Se está trabajando con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) para la coordinación de la notificación de incidentes en el caso de infraestructuras críticas que pertenezcan a operadores del sector público

The main service offered by the CCN-CERT to the Public Sector and companies of strategic interest is incident management. It provides them with technical and operative support in the different process stages: **detection, analysis, notification, response, treatment and eradication**. In fact, the National Governmental CERT is notified about over two and a half million events every day that are likely to be a cyber incident and only a tiny part (around 75 a day) are actually such.

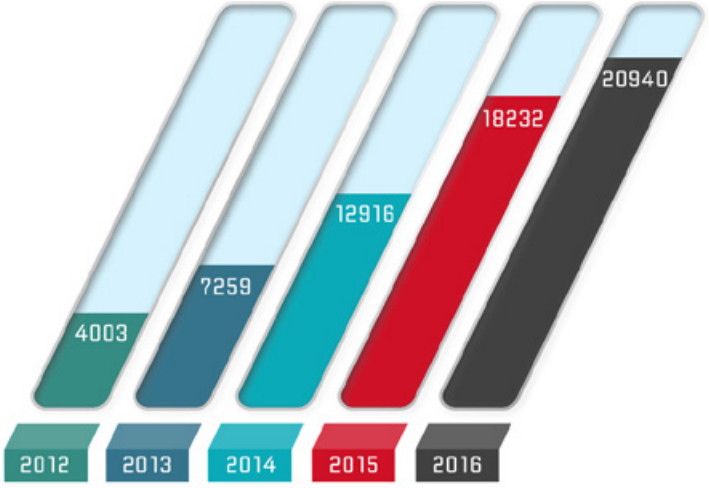
Consequently, in 2016 CCN-CERT managed a total of **20,940 cyber incidents** detected in the Public Sector and in companies of strategic interest. This figure represents a 14.5% increase on 2015 when 18,232 incidents were managed. Of them, 3.6% were considered as very high or critical, depending on their danger level (type of threat, origin, affected user profile, number or type of systems affected, impact, etc.). This type of attack (critical, very high and high), as mentioned in the National Security Framework, in article 36, must be reported to the CCN by the Public Sector (see CCN-STIC 817 Guide on Handling Cyber Incidents and CCN-STIC 830 Guide: ENS field of application).

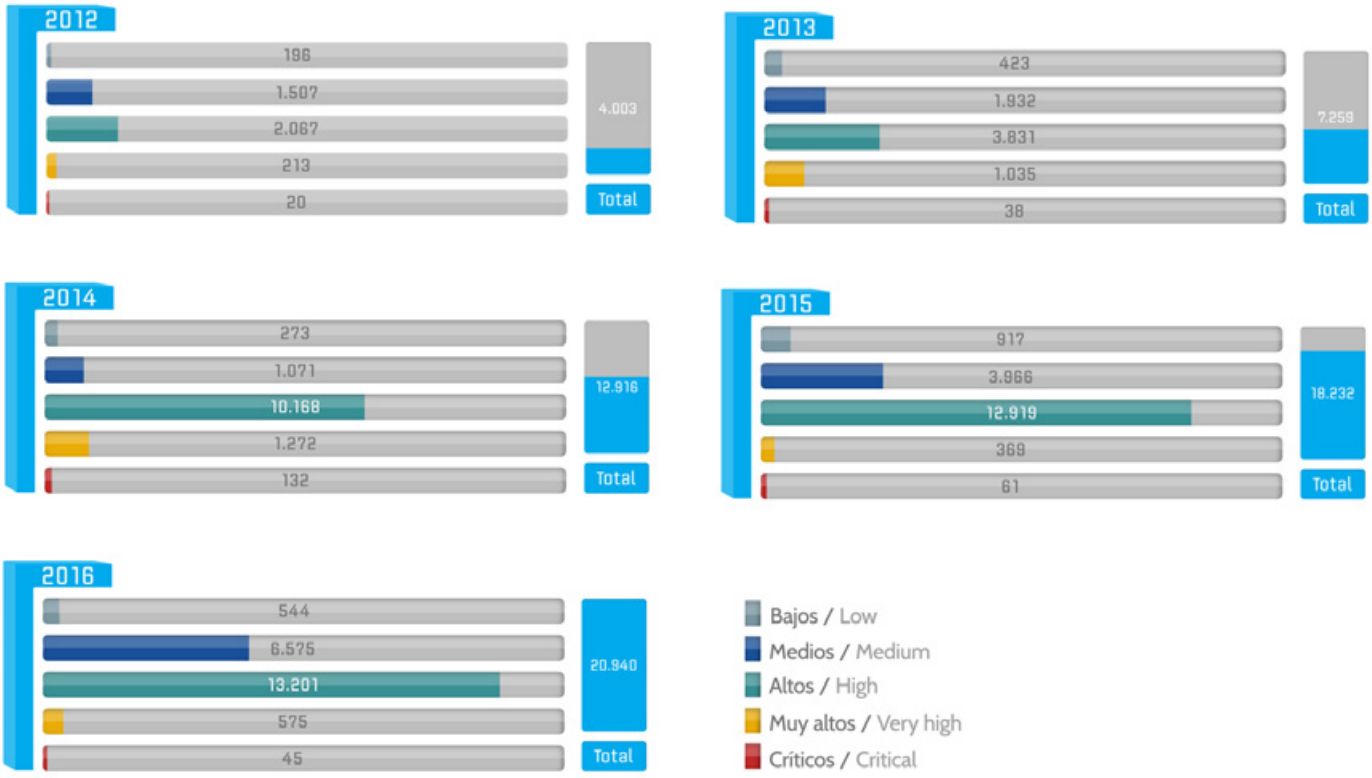
In this respect, work is being performed with the **National Centre for the Protection of Critical Infrastructures (CNPIC)** to coordinate notifications of incidents in the case of critical infrastructures that belong to Public Sector Operators.

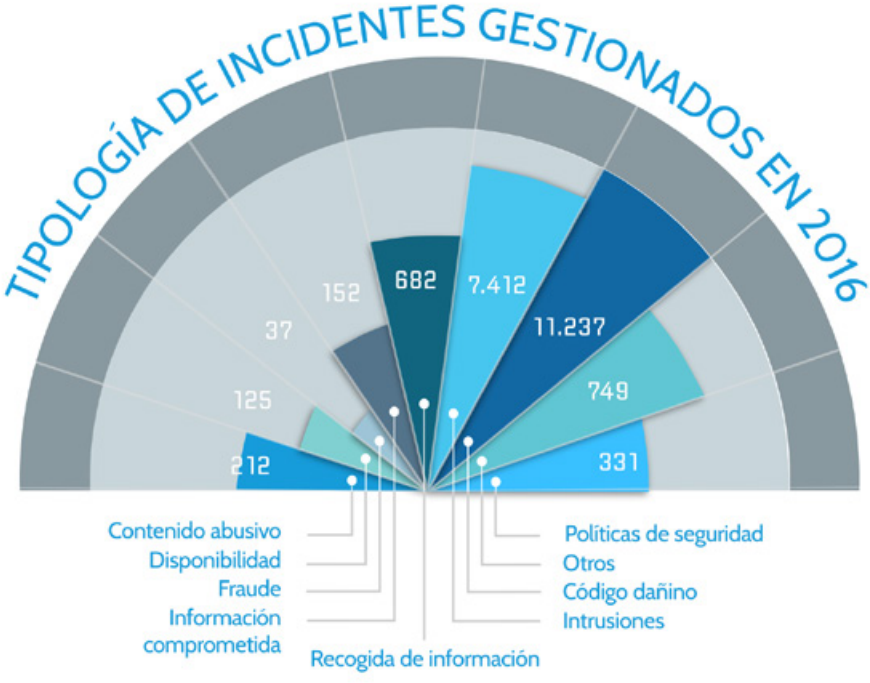
Procesos de gestión de un ciberincidente
Management Process of an CyberIncident



Ciberincidentes gestionados por CCN-CERT
Cyber incidents managed by the CCN-CERT




2012
196
1.507
2.067
213
20
4.003
Total
2013
423
1.932
3.831
1.035
38
7.259
Total
2014
273
1.071
10.168
1.272
132
12.916
Total
2015
917
3.966
12.919
369
61
18.232
Total
2016
544
6.575
13.201
575
45
20.940
Total
Bajos / Low
Medios / Medium
Altos / High
Muy altos / Very high
Críticos / Critical


TIPOLOGÍA DE INCIDENTES GESTIONADOS EN 2016
212
125
37
152
682
7.412
11.237
749
331
Contenido abusivo
Disponibilidad
Fraude
Información comprometida
Recogida de información
Políticas de seguridad
Otros
Código dañino
Intrusiones

6.1.1 Detección y análisis. Sistema de Alerta Temprana, SAT
Detection and Analysis. Early Warning System, SAT

Durante 2015 y 2016 se ha continuado desarrollando el **Sistema de Alerta Temprana (SAT)** en sus dos vertientes, en la intranet de la Administración **(SAT SARA)** y en la conexión a Internet de los organismos **(SAT INET)**.

En la primera de ellas, **SAT-SARA** existen ya **50 sondas desplegadas** (ministerios, organismos autónomos y comunidades autónomas). En los dos últimos años se ha producido una importante mejora en la detección, se ha desarrollado un nuevo portal de informes y un servicio de detección de vulnerabilidades de los servicios de la red SARA.

En cuanto al **SAT-INET** se ha continuado ampliando el despliegue de sondas, alcanzando las 130 en 109 organimos. Se ha mejorado el rendimiento de las mismas y se han desplegado dos sondas en la salida a Internet de la Administración General del Estado.

Además, en noviembre de 2016, se ha iniciado el despliege del SAT para la seguridad de sistemas industriales **(SAT-ICS)**, pensado para monitorizar la actividad en los sistemas de control industrial y SCADA[4] de los organismos, integrándolos en el servicio de gestión de alertas de ciberseguridad. La primera experiencia piloto se realizó en una confederación hidrográfica.

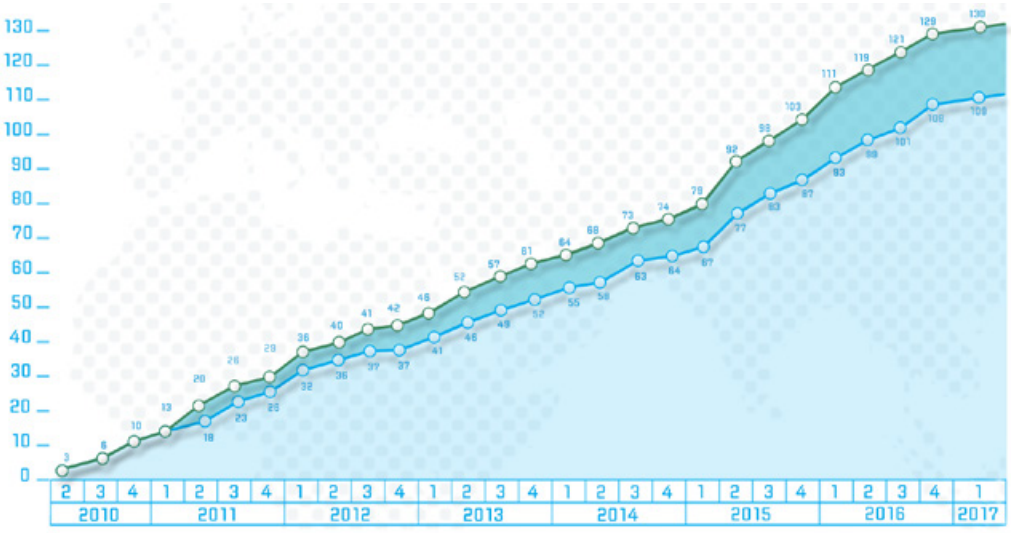
In this detection phase, during 2015 and 2016 both aspects of the **Early Warning System (SAT)** continued to be developed, on the Administration intranet **(SAT SARA)**, and on organisations' internet connections **(SAT INET)**.

In the former, **SAT-SARA** there are already **50 probes working** (Ministries, Autonomous Organisations and Autonomous Communities) and over the last two years there has been a significant improvement in detection, a new portal for reports has been developed plus vulnerability detection for services in the SARA network.

As far as **SAT-INET** is concerned, it has continued to broaden the deployment of probes, reaching 130 in 109 organisations, their performance has been improved and two probes have been deployed in AGE internet outlets.

In addition, in November 2016, SAT deployment began for industrial system security **(SAT-ICS)**, devised to monitor activity in industrial control systems and SCADA[4] for the Organisations, integrating them into the cyber-security warning management service. The first pilot experience was performed in a Hydrographic Confederation.

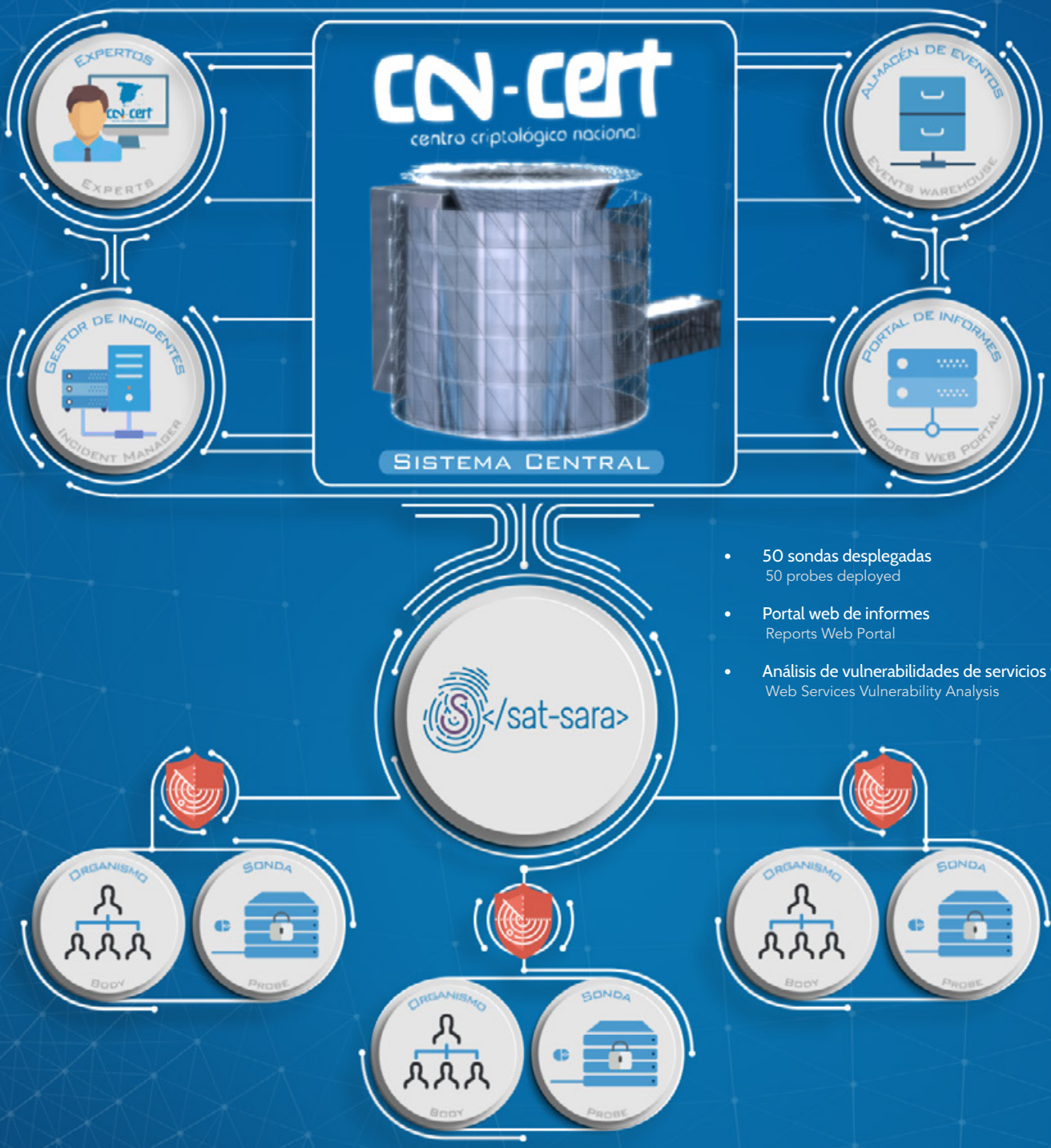
Se ha iniciado el despliege del SAT para la seguridad de sistemas industriales (SAT-ICS), pensado para monitorizar la actividad en los sistemas de control industrial y SCADA



Despliegue de sondas
Deployment of probes

[4] Supervisory Control and Data Acquisition

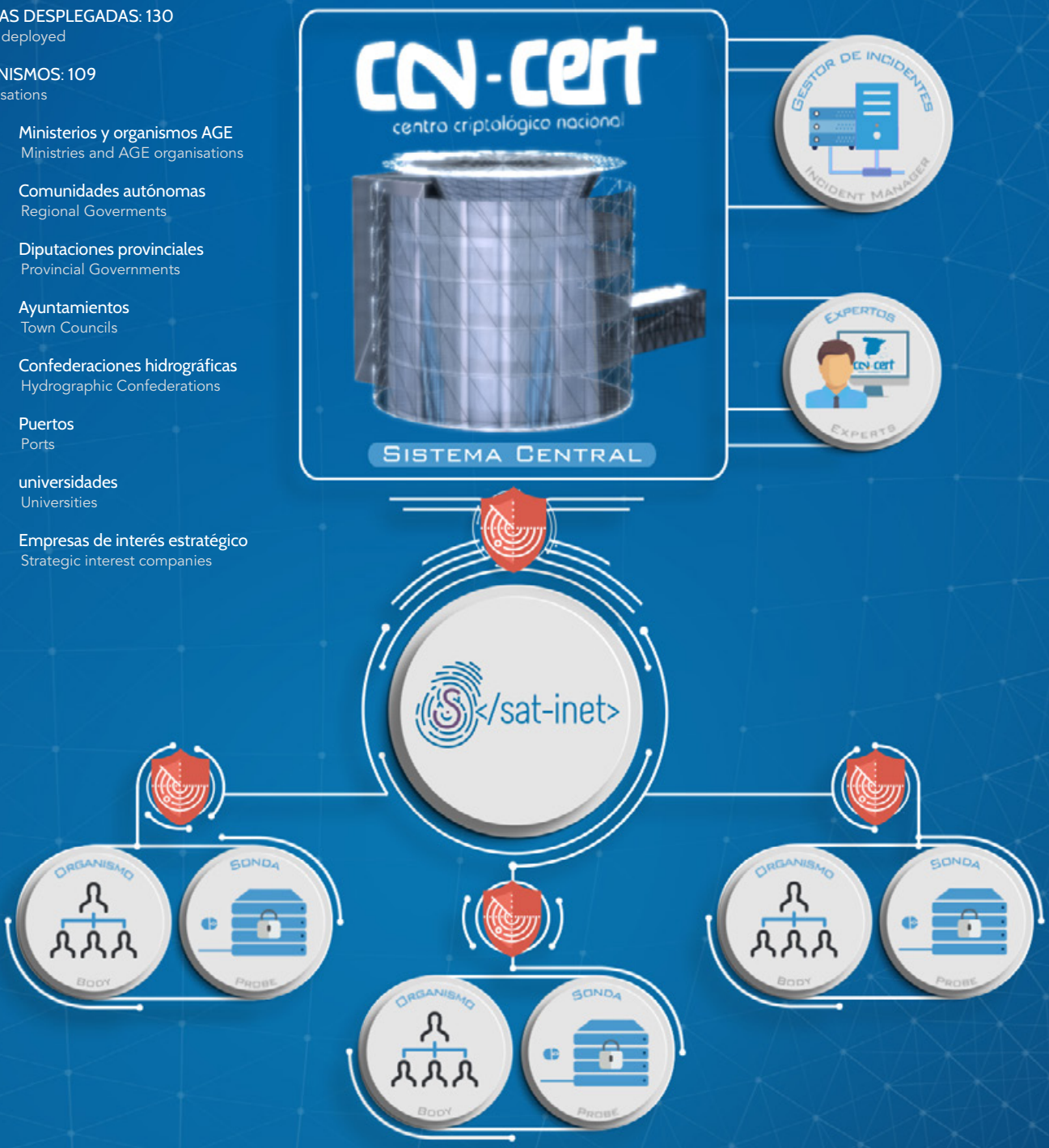
SAT - SARA



- 50 sondas desplegadas
  50 probes deployed
- Portal web de informes
  Reports Web Portal
- Análisis de vulnerabilidades de servicios web
  Web Services Vulnerability Analysis

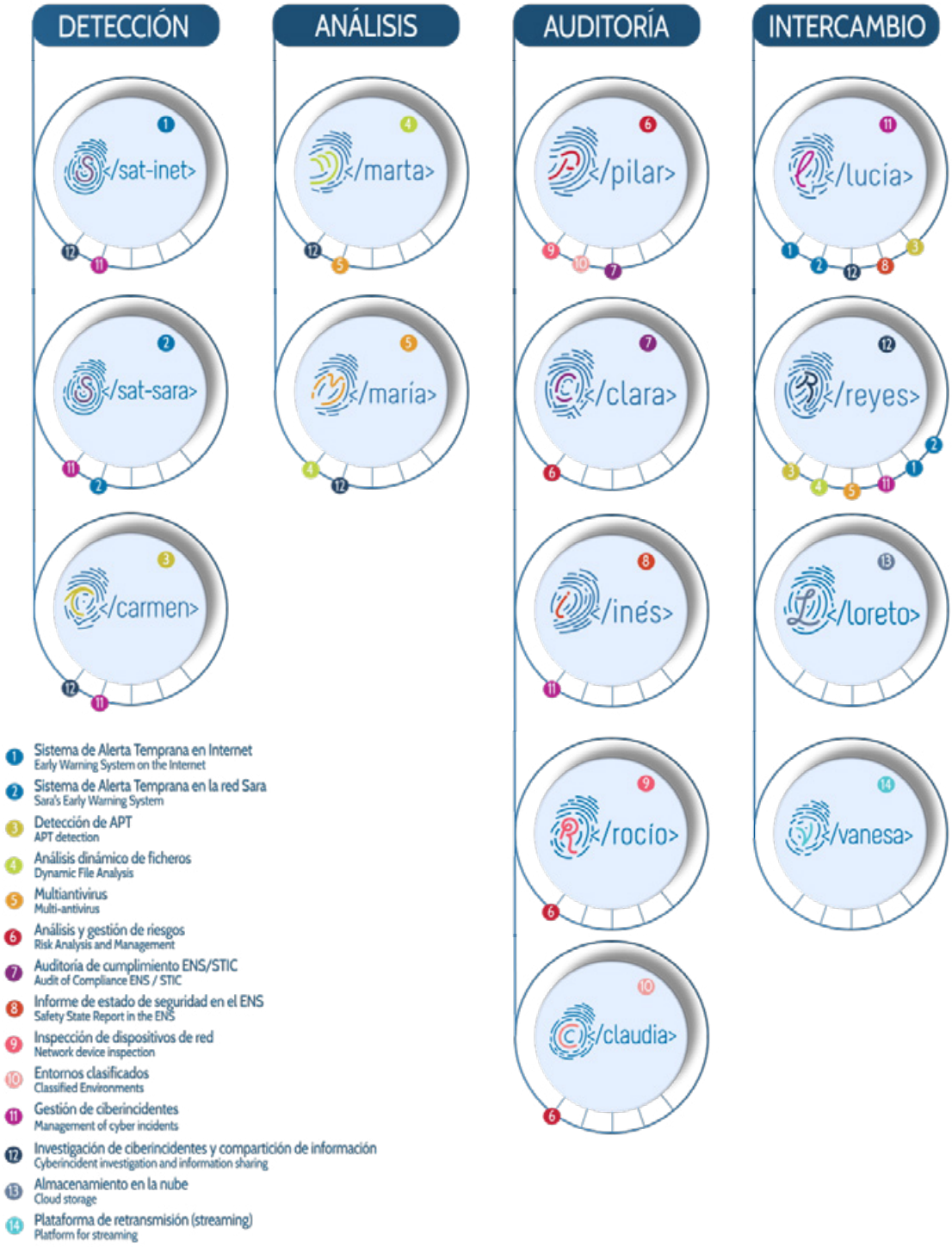
SAT - INET

- SONDAS DESPLEGADAS: 130
  Probes deployed
- ORGANISMOS: 109
  Organisations
  - Ministerios y organismos AGE
    Ministries and AGE organisations
  - Comunidades autónomas
    Regional Goverments
  - Diputaciones provinciales
    Provincial Governments
  - Ayuntamientos
    Town Councils
  - Confederaciones hidrográficas
    Hydrographic Confederations
  - Puertos
    Ports
  - universidades
    Universities
  - Empresas de interés estratégico
    Strategic interest companies



El CCN-CERT ha realizado un importante esfuerzo en el desarrollo e integración de herramientas propias con las que facilitar la labor de toda su comunidad en la mejor gestión de la ciberseguridad.

The CCN-CERT has made a significant effort in development and integration of own tools to facilitate the work of their entire Community in terms of better cyber-security management.



ACCESOS/DESCARGAS DESDE EL PORTAL DEL CCN-CERT
ACCESS / DOWNLOADS FROM THE CCN-CERT PORTAL

Herramientas Tools	Acumulado 2015 Accumulated 2015	Acumulado 2016 Accumulated 2016
REYES	-	25.381
INES	7.828	6.180
PILAR	1.149	3.402
CLARA	1.042	2.148
PILAR BASIC	611	1.677
µPILAR	385	1.520
LUCIA	444	939
CARMEN	701	578
RMAT	125	381
CCN-DROID WIPER	69	146
CCN-DROID CRYPTER	52	128

6.2.1 CARMEN, DETECCIÓN DE APT
CARMEN, APT DETECTION

carmen@ccn-cert.cni.es

Desarrollada en el año 2013 junto con la empresa S2Grupo, esta herramienta permite la captura y detección de tráfico anómalo que circula por una red.

A finales de 2016 estaba desplegada en más de 25 organismos públicos y empresas y había detectado 45 incidentes de una peligrosidad entre muy alta y crítica.

Interacción con otras herramientas del CCN-CERT como LUCIA y REYES.

Developed in 2013 working with the company S2Grupo, this tool allows problematic traffic to be captured and detected working from the corresponding traffic for a network. At the end of 2016 it was deployed in over 25 public organisations and companies and 45 incidents were detected with a danger level classified between Very High and Critical.

6.2.2 CLARA, AUDITORÍA DE CUMPLIMIENTO ENS/STIC
CLARA, AUDIT TO COMPLY WITH THE ENS/STIC

clara@ccn-cert.cni.es

Herramienta de auditoría, desarrollada en 2014 junto con la empresa Sidertia, que permite valorar de forma continua el nivel de seguridad de los sistemas, incluyendo redes clasificadas. Analiza las características de seguridad técnicas definidas a través del ENS y de las guías CCN-STIC.

La herramienta funciona exclusivamente en sistemas Windows, tanto en sus versiones cliente como servidor, miembros de un dominio o independientes al mismo.

Auditing tool, developed in 2014, along with the company Sidertia, allowing continuous evaluation of a system's security level, including classified networks. It analyses technical security features defined through the ENS and the CCN-STIC guides.

The tool works exclusively in Windows systems, both in customer and server versions, members of a domain or independently from it.

6.2.3 CLAUDIA, ENTORNOS CLASIFICADOS
CLAUDIA, CLASSIFIED ENVIRONMENTS

claudia@ccn-cert.cni.es

Desarrollada por el propio equipo de Acreditación de Sistemas del CCN, esta herramienta de auditoría se encuentra en su fase piloto y está especialmente dirigida a mejorar los procedimientos de seguridad de los entornos clasificados.

Basada en entornos abiertos (ELK[5]), CLAUDIA está orientada a la recopilación y explotación de registros de auditoría, sin perjuicio de su utilización como almacenamiento de cualquier tipo de información.

Developed by the actual CCN System Accreditation team, this auditing tool is in its pilot phase and it is particularly intended to improve security procedures for classified environments.

Based on open environments (ELK[5]), CLAUDIA is focussed on compilation and exploitation of audit records, without damaging their use to store any type of information.

6.2.4 INES, INFORME DEL ESTADO DE SEGURIDAD EN EL ENS
INES, SECURITY STATUS REPORT IN THE ENS

Desarrollada por el CCN-CERT y la empresa Nethaphora con el fin de facilitar la labor de todos los organismos a la hora de evaluar regularmente el estado de la seguridad de sus sistemas, tal y como recoge el ENS (véase apartado correspondiente).

Developed by the CCN-CERT and Nethaphora in order to make life easier for all organisations when regularly assessing their systems' security status, as complied in the ENS.

ines@ccn-cert.cni.es

6.2.5 LORETO, ALMACENAMIENTO EN LA NUBE
LORETO, STORAGE IN THE CLOUD

loreto@ccn-cert.cni.es

Herramienta de compartición desarrollada por el CCN-CERT para el almacenamiento virtual de archivos, datos, aplicaciones y el intercambio de los mismos con colaboradores.

Sharing tool developed by the CCN-CERT for virtual storage of files, data, applications and exchange with collaborators.

6.2.6 LUCIA, GESTIÓN DE CIBERINCIDENTES
LUCIA, CYBER INCIDENT MANAGEMENT

lucia@ccn-cert.cni.es

Herramienta desarrollada en 2015 por el CCN-CERT y la empresa CSA para la gestión de ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad.

Tool developed in 2015 by the CCN-CERT and CSA to Manage Cyber-Incidents in organisations within the field of applying the National Security Framework.

[5] *Elasticsearch , Logstash y Kibana*

Basada en un sistema de gestión de tickets, ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo, de acuerdo a la guía **CCN-STIC 817 de gestión de incidentes**. Permite cumplir con dos requisitos del ENS: la obligatoriedad de notificar los incidentes y la carga de datos en INES.

En 2016 se ha puesto en marcha la versión 2.5 que permite comunicar y sincronizar los incidentes provenientes de una organización con LUCIA Central (la instancia del CCN-CERT desde la que se gestionan los ciberincidentes). Hasta el momento son 20 los organismos federados (AGE, comunidades autónomas, universidades y ayuntamientos) y 13 en los que había instancias sincronizadas con LUCIA central y 11 en vías de instalación.

Based on a ticket management system, it offers a common language for danger levels and classification of incidents and maintains its traceability and monitoring in accordance with the **CCN-STIC 817 Incident Management** guide. It helps meet two ENS requirements: obligation to report incidents and loading the data in INES

In 2016, the 2.5 version was implemented that helps to communicate and synchronise incidents coming from an organisation with Central LUCIA (the CCN-CERT authority from which cyber incidents are managed). To date, there are 20 federated organisations (AGE, Autonomous Communities, Universities and Town Councils) and 13 where authorities had been installed, synchronised with central LUCIA and 11 currently being installed.

LUCIA permite cumplir con dos requisitos del ENS: la obligatoriedad de notificar los incidentes y la carga de datos en INES

MARIA, MULTIANTIVIRUS
MARIA, MULTIANTIVIRUS

6.2.7

Herramienta de detección desarrollada por el CCN-CERT y la empresa CSA para el análisis estático de código dañino, en proceso de instalación.

Permite analizar todo tipo de *malware*, utilizando las versiones de líneas de comando de múltiples motores antivirus y *antimalware* (están en proceso de incorporación más de 30), actualizados en tiempo real. Es, de hecho, una evolución de la plataforma MultiAntiVirus con la que ya contaba el CCN-CERT.

maria@ccn-cert.cni.es

Detection tool, currently being installed, developed by the CCN-CERT for static malware analysis.
It helps to analyse all types of malware, using command line versions of multiple antivirus and antimalware engines (they are in the process of including more than 30), updated in real time. It is, in fact, a development of the Multi-Antivirus platform already used by CCN-CERT.

Esta previsto que durante 2017 cuente con una aplicación para integrarse con otros servicios del CCN-CERT, como MARTA o REYES.
It has been envisaged that an application will be added during 2017 to be integrated with other CCN-CERT services such as MARTA or REYES.

MARTA, ANÁLISIS DINÁMICO DE FICHEROS
MARTA, DYNAMIC FILE ANALYSIS

6.2.8

Herramienta de análisis, desarrollada en 2016 por el CCN-CERT y la empresa InnoTec. Cuenta con una plataforma avanzada de ***sandboxing***[6] dedicada al análisis automatizado de múltiples tipos de ficheros que podrían tener algún comportamiento dañino (tanto ejecutables, como de Office o PDF).

marta@ccn-cert.cni.es

Analysis tool, developed in 2016 by the CCN-CERT and the company InnoTec; it has an advanced sandboxing[6] platform dedicated to automated analysis of multiple file types that might demonstrate some malware behaviour (both executable and using Office and PDF).

[6] Foso de pruebas

Entre sus ventajas se encuentran:

- Detección precoz de amenazas provenientes de código dañino que analiza las características de un fichero más allá de la información facilitada por un antivirus.
- Utilización de un sitio centralizado y seguro en el que albergar las muestras de ***malware*** de un modo organizado y con una herramienta de búsqueda avanzada.
- Organización, a través de un sistema de etiquetas, de toda la información de un modo visual y ágil de ficheros, análisis y reglas.

En una primera fase, esta herramienta está destinada a todas las organizaciones que se encuentren adheridas al Sistema de Alerta Temprana, SAT.

Its advantages include:

- Early detection of threats from malware, analysing the characteristics of a file beyond the information provided by an anti-virus.
- Use of a centralised and safe site to host samples of malware in an organised way using an advanced search tool.
- Organisation, using a label system, of all information by means of a visual and agile mode for files, analysis and rules.

In an initial phase, this tool is intended for all organisations that have been signed up to the Early Warning System, SAT.

6.2.9 PILAR, ANÁLISIS Y GESTIÓN DE RIESGOS
PILAR, RISK ANALYSIS AND MANAGEMENT

pilar@ccn-cert.cni.es

Herramienta de análisis y gestión de riesgos desarrollada y financiada en 2006 por el CCN y la empresa A.L.H.J.Mañas.

Se actualiza periódicamente y existen diversas variedades, todas ellas con su correspondiente guía CCN-STIC (470G/1, 470G/2, 471/D, 472E y 473D):

- PILAR: versión íntegra de la herramienta
- PILAR Basic: versión sencilla para pymes y Administración local
- µPILAR: versión de PILAR reducida, destinada a la realización de análisis de riesgos muy rápidos
- RMAT (***Risk Management Additional Tools***): personalización de herramientas

En su última versión (7), pendiente de publicar, PILAR ha incluido diversos apartados sobre los riesgos asociados a la protección de información de carácter personal y a la protección de bienes materiales, personas y medio ambiente en infraestructuras críticas.

Risk analysis and management tools developed and financed in 2006 by the CCN and the company A.L.H.J.Mañas.

It is updated periodically and there are several varieties, all with their corresponding CCN-STIC guide (470G/1, 470G/2, 471/D, 472E and 473D):

PILAR: full version of the tool

PILAR Basic: simple version for SMEs and Local Administration

µPILAR: reduced PILAR version, intended to perform very fast risk analyses

RMAT (Risk Management Additional Tools): Tool personalisation

In its latest version (7) pending publication, PILAR has included different sections on risks associated with protecting personal information and protecting material goods, persons and the environment in critical infrastructures.

reyes@ccn-cert.cni.es

Herramienta desarrollada por el CCN-CERT y la empresa InnoTec en 2016 para agilizar la labor de análisis e investigación de ciberincidentes y compartir información de ciberamenazas.

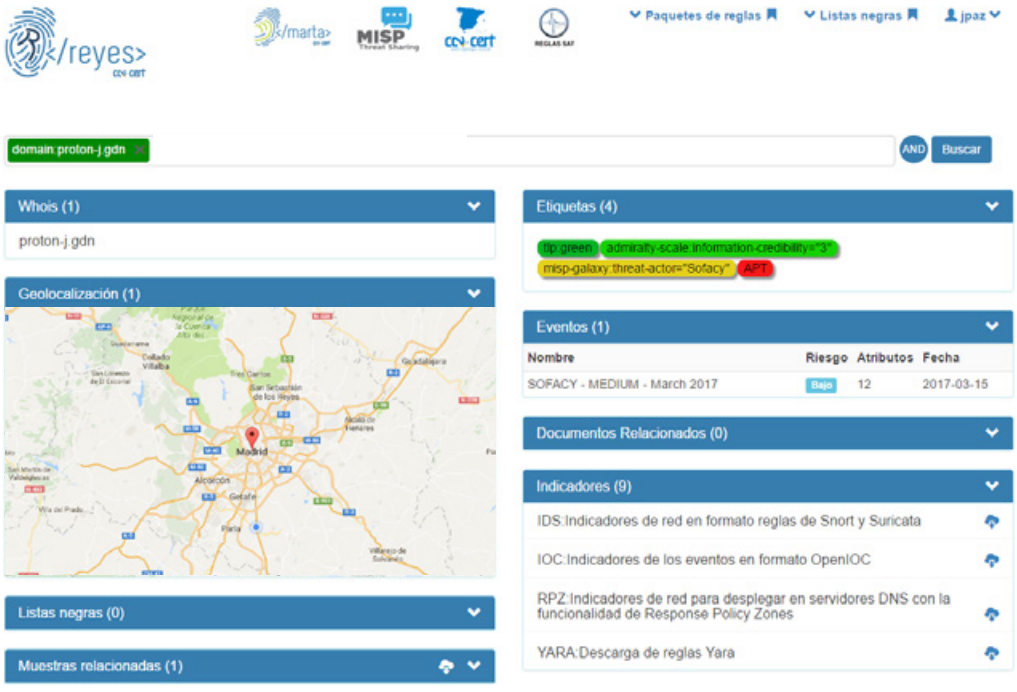
Permite acceder a todo tipo de listas negras relacionadas con incidentes (APT, botnet, malware, ransomware, spam o TOR); entrar en otras herramientas como MISP (***Malware Information Sharing Platform***, a su vez federada con otras organizaciones como OTAN, FIRST, EGC y otros CERT), MARTA o el propio SAT y su gestor de reglas o conocer el Whois y la geolocalización de una IP son algunas de las posibilidades que ofrece esta nueva plataforma.

A través de REYES se ha incrementado de forma notable el intercambio de información con los organismos del sector público, empresas de interés estratégico y con sistemas similares de otros países u organizacines internacionales. Al término de 2016 eran 33 las organizaciones incluidas en REYES.

Tool developed by the CCN-CERT and the company InnoTec in 2016 to streamline analysis and research into cyber incidents and share information on cyber threats.

Accessing all types of blacklists relating to incidents (APT, botnet, malware, ransomware, spam or TOR); entering other tools such as MISP (Malware Information Sharing Platform, in turn federated with other organisations such as NATO, FIRST, EGC and other CERTS), MARTA or the actual SAT and its rule administrator or finding out the Whois and the geolocation of an IP are just some of the possibilities offered by this new platform.

Using REYES, there has been a considerable increase in information exchange with Public Sector organisations, companies of strategic interest with similar systems from other countries or international organisations. By the end of 2016, 33 organisations had been included in REYES.



6.2.11 ROCIO, INSPECCIÓN DE DISPOSITIVOS DE RED
ROCIO, INSPECTION OF NETWORK DEVICES

Herramienta web desarrollada por el equipo de acreditación del CCN y la Universidad Politécnica de Madrid para analizar las configuraciones de los dispositivos de red, enrutadores (routers) y conmutadores Cisco. Es una herramienta utilizada durante los procedimientos de inspección. Su análisis se basa en la comprobación de una serie de reglas, desarrolladas por el CCN, sobre la configuración y los resultados de ejecutar ciertos comandos en las consolas de los equipos.

ROCIO proporciona una interfaz web en la que se permite almacenar configuraciones, seleccionar distintos paquetes de reglas y generar informes de cumplimiento.

rocio@ccn-cert.cni.es

Web tool developed by the CCN Accreditation team to analyse configurations of the network, routers and Cisco commutator. This is a tool used during inspection procedures; its analysis is based on checking a series of rules, developed by the CCN, regarding configuration and the results of running certain commands on the equipment consoles.

ROCIO provides a web interface where it is possible to store configurations, select different rule packages and generate compliance reports.

6.2.12 VANESA, GRABACIONES Y EMISIONES ONLINE
VANESA, RECORDINGS AND ONLINE BROADCASTS

Herramienta del CCN-CERT basada en tecnología Policom, para facilitar la tarea de formación y sensibilización con toda su comunidad de referencia. A través de esta plataforma de retransmisión de vídeo en directo, se pretende reducir los desplazamientos, tanto en los cursos de formación, como en las reuniones de seguimiento de cualquier proyecto.

vanesa@ccn-cert.cni.es

Tool developed by the CCN-CERT to make training and awareness-raising easier throughout its reference community. This live video broadcasting platform aims to reduce journeys for training courses and meetings to monitor any project.

El grupo de expertos del CCN-CERT elabora **informes y boletines de seguridad** de muy diversa temática y con diferente nivel de complejidad para ofrecer una visión actualizada del estado de la ciberseguridad. Los citados documentos incluyen características de la amenaza o vulnerabilidad, procedimientos de infección, formas de detección y, sobre todo, medidas preventivas y correctivas para hacerles frente.

Entre ellos destacan los informes de código dañino con Indicadores de Compromiso (IoC[7]), de acuerdo a estándares reconocidos por la comunidad internacional y el Informe Anual de Ciberamenazas 2016 y Tendencias 2017, en el que se analizan todos los años, el panorama nacional e internacional de la ciberseguridad. Los Informes referidos son publicados en el portal del CCN-CERT, www.ccn-cert.cni.es (en la parte pública o privada, en función de la amenaza) y remitidos a los organismos relacionados con el contenido del documento.

The CCN-CERT group of experts draws up **reports and security newsletters** on a wide variety of topics with different levels of complexity to offer an up-to-date view of cyber-security status. The aforementioned documents include threat or vulnerability features, infection procedures, means of detection and, above all, preventive and corrective measures to tackle it.

They include malware reports with Indicators of Compromise (IoC[7]), following standards recognised by the international community and the Annual Report on Cyber-Threats 2016 and Trends 2017, that takes an in-depth look at the national and international panorama for cyber-security every year. The aforementioned reports are published on the CCN-CERT website www.ccn-cert.cni.es (in the public or private section depending on the threat) and/or sent to organisations related to the document content.

Informes de Amenazas 2015: 33
Threat Reports 2015: 33

Publicados en el Portal 2015
Published on the 2015 Portal

- CCN-CERT IA-08/15 Amenaza en BIOS
  CCN-CERT IA-08/15 Threat in BIOS
- CCN-CERT IA-09/15 Ciberamenazas 2014 Tendencias 2015
  CCN-CERT IA-09/15 Cyber threats 2014 Trends 2015
- CCN-CERTIA-09/15 Ciberamenazas 2014 Tendencias 2015-Resumen ejecutivo
  CCN-CERT IA-09/15 Cyber-threats 2014 Trends 2015-Executive Summary
- CCN-CERT IA-22/15 Medidas de seguridad contra Ransomware
  CCN-CERT IA-22/15 Security measures against Ransomware
- CCN-CERT IA-28/15 Medidas de Seguridad en Telefonía Móvil
  CCN-CERT IA-28/15 Security Measures in Mobile Telephony

[7] Indicator of compromise

Informes de Amenazas 2016: 30
Threat Reports 2016: 30

Publicados en el Portal 2016
Published on the 2016 Portal

- CCN-CERT IA-01/16 Medidas de Seguridad contra Ransomware
  CCN-CERT IA-01/16 Security Measures Against Ransomware
- CCN-CERT IA-04/16 Amenazas y análisis de riesgos en Sistemas de Control Industrial (ICS)
  CCN-CERT IA-04/16 Threats and Risk Analysis in Industrial Control Systems (ICS)
- CCN-CERT IA-05/16 Comunicación de campo cercano (Near Field Communication - NFC). Vulnerabilidades
  CCN-CERT IA-05/16 Near Field Communication (NFC). Vulnerabilities
- CCN-CERT IA-06/16 Privacidad en Microsoft Windows 10 (Puestos de Trabajo en las Administraciones Públicas)
  CCN-CERT IA-06/16 Privacy in Microsoft Windows 10 (Jobs in Public Administrations
- CCN-CERT IA-08/16 Privacidad en Microsoft Windows 10 (Equipos Críticos Aislados y Redes Clasificadas)
  CCN-CERT IA-08/16 Privacy in Microsoft Windows 10 (Isolated Critical Equipment and Classified Networks)
- CCN-CERT IA-09/16 Ciberamenazas 2015 Tendencias 2016
  CCN-CERT IA-09/16 Cyber threats 2015 Trends 2016
- CCN-CERT IA-09/16 Ciberamenazas 2015 Tendencias 2016 - Resumen Ejecutivo
  CCN-CERT IA-09/16 Cyber threats 2015 Trends 2016 - Executive Summary
- CCN-CERT IA-21/16 Riesgos de uso de WhatsApp
  CCN-CERT IA-21/16 Risks of using WhatsApp

Informes de Código Dañino 2015: 26
Malware Code Reports published on the 2015 Portal: 26

- CCN-CERT ID-04/15 Fanny (Equation Group)
- CCN-CERT ID-06/15 Agent.BTZ
- CCN-CERT ID-10/15 Upatre
- CCN-CERT ID-11/15 H-Worm – Houdini
- CCN CERT ID-13/15 TorrentLocker
- CCN-CERT ID-15/15 Spybot
- CCN-CERT ID-16/15 "Trojan:Win32/Ramnit"
- CCN-CERT ID-17/15 Double Fantasy
- CCN-CERT ID-19/15 Ransom_Cryptear.A
- CCN-CERT ID-20/15 Worm.Hybris
- CCN-CERT ID-21/15 Win32.Kins
- CCN-CERT ID-22/15 Win32/Papras.EH
- CCN-CERT ID-24/15 "Trojan:Win32/Dridex"
- CCN-CERT ID-25/15 "Expiro"
- CCN-CERT ID-26/15 "Pushdo"

- CCN-CERT ID-01/16 "Elex"
- CCN-CERT ID-02/16 "Gozi"
- CCN-CERT ID-03/16 "Ponmocup"
- CCN-CERT ID-05/16 "Gamarue"
- CCN-CERT ID-06/16 Win32/Mudrop
- CCN-CERT ID-07/16 Ransom.TeslaCrypt
- CCN-CERT ID-09/16 Ransom.Locky
- CCN-CERT ID-11/16 Ransom.Petya
- CCN-CERT ID-13/16 Toopu
- CCN-CERT ID-15/16 Ransom.CryptoWall
- CCN-CERT ID-16/16 "Volgmer"
- CCN-CERT ID-18/16 Ransom.Mischa
- CCN-CERT ID-19/16 Ransom.DMALocker
- CCN-CERT ID-21/16 Ransom.Cerber
- CCN-CERT ID-23/16 Win32/Filecoder.Alfa
- CCN-CERT ID-24/16 Ransom.CryptXXX

Vulnerabilidades CCN
CCN Vulnerabilities

Diariamente el CCN-CERT publica (con hilo RSS[7]) las vulnerabilidades de los siguientes fabricantes: Microsoft, Red Hat, Cisco, Oracle, Adobe, Suse, Debian, IBM, Apple y Symantec.

Entre 2015 y 2016 se publicaron un total de 8.872 vulnerabilidades

- Total publicadas 2015: 5.099
- Total publicadas 2016: 3.773

Every day the CCN-CERT uses the RSS[7] news feed to publish vulnerabilities for the following manufacturers: Microsoft, Red Hat, Cisco, Oracle, Adobe, Suse, Debian, IBM, Apple and Symantec.
A total of 8.872 vulnerabilities were published between 2015 and 2016

Informes de Buenas Prácticas 2016
Best Practices Reports 2016

- CCN-CERT BP-06/16 Navegadores web
  CCN-CERT BP-06/16 Web browsers
- CCN-CERT BP-03/16 Dispositivos móviles
  CCN-CERT BP-03/16 Mobile Devices
- CCN-CERT BP-02/16 Correo electrónico
  CCN-CERT BP-02/16 E-mail

[7] Really Simple Syndication

Avisos y alertas a usuarios registrados del portal
Warnings and alerts for users registered on the site

Todos los usuarios registrados del portal del CCN-CERT (más de 7.500) reciben directamente los avisos y alertas de ciberseguridad en los que se informa de las nuevas amenazas detectadas:

- Avisos 2015-2016: 15
- Alertas 2015-2016: 12

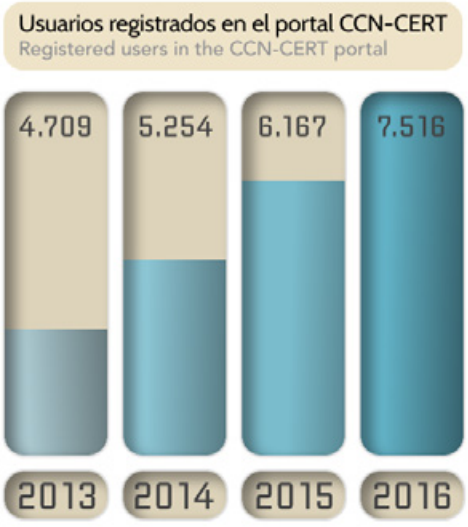
Del mismo modo, el equipo CCN-CERT lleva a cabo **auditorías a páginas web** de distintos organismos del sector público en busca de posibles vulnerabilidades críticas, con el fin de establecer las pautas adecuadas para reducirlas o eliminarlas. Durante 2015 y 2016 se han realizado 27 auditorías a páginas web.

All users registered on the CCN-CERT website (over 7,500) receive cyber-security notifications and warnings directly, informing them of newly detected threats.

- Notifications 2015-2016: 15
- Warnings 2015-2016: 12

In the same way, the CCN-CERT team carries out **audits on websites** for different organisations in the public sector in search of possible critical vulnerabilities in order to set the right guidelines to reduce or eradicate them. During 2015 and 2016, 27 website audits were carried out.

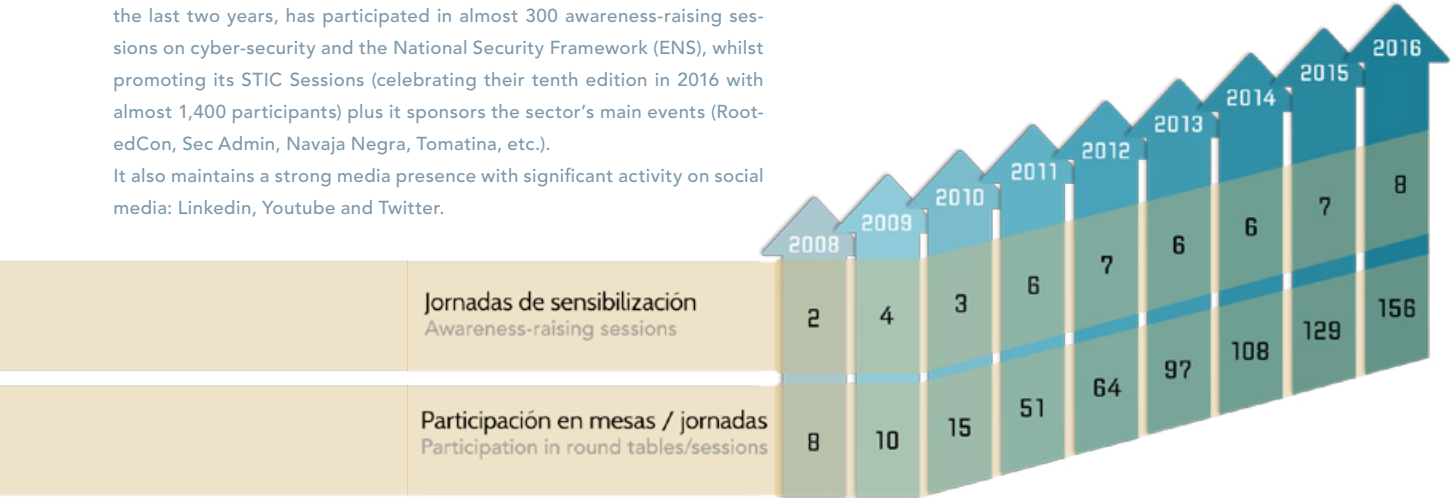
El CCN-CERT ha llevado a cabo 27 auditorías a páginas web de distintos organismos públicos

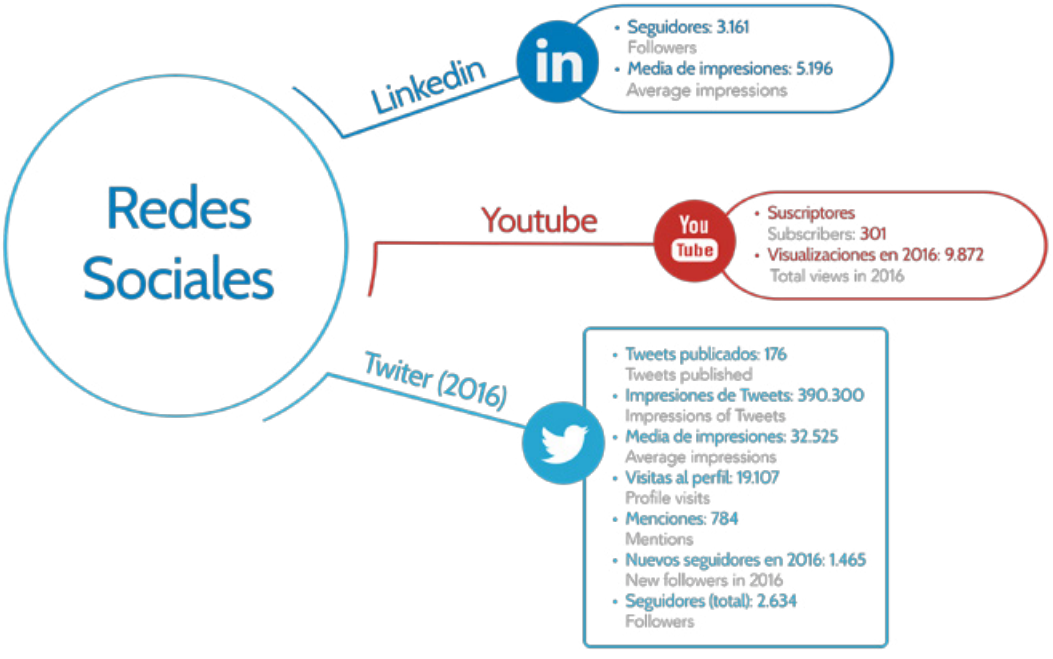


Dentro del capítulo de promoción en nuestro país de la cultura de la ciberseguridad, a través de iniciativas de intercambio de conocimientos entre todos los actores implicados, el CCN-CERT acomete un gran número de acciones de información y sensibilización. De este modo, el CERT Gubernamental Nacional, en los dos últimos años, ha participado en cerca de 300 jornadas de sensibilización y concienciación sobre ciberseguridad y el Esquema Nacional de Seguridad (ENS), al tiempo que ha promovido sus Jornadas STIC (que en 2016 alcanzaron la décima edición con cerca de 1.400 asistentes) y patrocinó los principales eventos del sector (RootedCon, Sec Admin, Navaja Negra, Tomatina, etc.).

Asimismo mantiene una fuerte presencia en los medios de comunicación y una actividad importante en las distintas redes sociales: Linkedin, Youtube y Twitter

Within the chapter on promoting cyber-security culture nationwide, through initiatives involving knowledge exchange among all stakeholders, the CCN-CERT performs a large number of information and awareness-raising actions. In this way, the National Governmental CERT, over the last two years, has participated in almost 300 awareness-raising sessions on cyber-security and the National Security Framework (ENS), whilst promoting its STIC Sessions (celebrating their tenth edition in 2016 with almost 1,400 participants) plus it sponsors the sector's main events (RootedCon, Sec Admin, Navaja Negra, Tomatina, etc.).
It also maintains a strong media presence with significant activity on social media: Linkedin, Youtube and Twitter.





El CCN ha participado en más de doscientas ochenta y cinco sesiones y mesas redondas entre las que destacan sus Jornadas STIC. Este evento, celebrado anualmente desde el año 2007 se ha convertido en el principal encuentro de expertos en ciberseguridad en España, no solo por el gran éxito de convocatoria (con cerca de 1.400 asistentes), sino también por la calidad de los temas abordados y por la experiencia y conocimiento de los ponentes.

Inauguradas por el secretario de Estado director del CNI, Félix Sanz Roldán, el evento está abierto a la participación de expertos del sector público y de empresas de interés estratégico para el país y ha alcanzado un gran prestigio gracias al esfuerzo de patrocinadores, ponentes y asistentes.

Among the more than two hundred and eighty-five actions and participation in round tables and conferences organized by the CCN-CERT stands out its STIC Conferences. This event, celebrated annually since 2007, has become the main meeting of experts in cybersecurity in Spain, not only for the great success of the call (with about 1,400 attendees), but also for the quality of the topics covered and for The experience and knowledge of the speakers.

Inaugurated by the Secretary of State-Director of the CNI, Félix Sanz Roldán, the event is open to participation from experts from the Public Sector and companies of strategic interest for the country and has achieved great prestige thanks to all-round hard work from sponsors, speakers and participants.

Jornadas STIC CCN-CERT
CCN-CERT STIC Conference

X Jornadas STIC CCN-CERT 2016
X CCN-CERT 2016 STIC Conference

España

1. Ministerio de la Presidencia y para las Administraciones Territoriales
   Ministerio de Hacienda y Función Pública

   - Subdirección General del Comité Ejecutivo de la Comisión de Estrategia TIC, encargada de impulsar la transformación digital de la Administración de acuerdo a una Estrategia común en el ámbito de las TIC.
   - Acuerdo y colaboración con el Instituto Nacional de Administración Pública (INAP) y la Secretaría de Estado para la Función Pública para impulsar la seguridad en el ámbito de la Administración Electrónica. En dicho acuerdo se contempla el desarrollo del Esquema Nacional de Seguridad.
   - 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.
   - Grupo de Trabajo del Esquema Nacional Seguridad.
   - Grupo de Trabajo de Seguridad del Comité Sectorial de la Administración Electrónica (CSAE)

2. Ministerio de Defensa

   - Grupo de Trabajo de cifra con el Estado Mayor Conjunto de la Defensa
   - Colaboración con el Mando Conjunto de Ciberdefensa

3. Ministerio de Energía, Turismo y Agenda Digital

   - Grupos de trabajo de los proyectos Rescata, Seguridad y Confianza, usabilidad del DNIe (e-ID)

4. Ministerio del Interior

   - Grupo de Trabajo sobre DNI electrónico con la Dirección General de la Policía
   - Grupo de Trabajo de Infraestructuras Críticas con la Secretaría de Estado de Seguridad

Spain

1. Ministry of the Presidency and for Territorial Administrations
   Ministry of Inland Revenue and Pubic Function

   - General Sub-Board of the ICT Strategy Commission Executive Commission, in charge of boosting the Administration's digital transformation in accordance with a common ICT Strategy.
   - Agreement and joint work with the National Public Administration Institute (INAP) and the Secretary of State for Public Functions to boost security in the field of Electronic Administration. This agreement considers development of the National Security Framework.
   - Working groups on secure electronic communications; transposition of the European directive on payment methods (SEPA), identification and authentication and WEB services from the Administration.
   - National Security Framework working group.
   - Security working group for the Electronic Administration Sector Committee (Regions)

2. Ministry of Defense

   - Encrypting working group with the Joint Chief of Staff for Defence
   - Working with the Joint Cyber-defence Command

3. Ministry of Energy, Tourism and Digital Agenda

   - Working groups for the Rescue, Security and Trust projects, usability of the DNIe (e-ID)

4. Ministry of the Interior

   - Working group on electronic ID with the General Police Board
   - Working group on Critical Infrastructures with the Secretary of State for Security

5. Federación Española de Municipios y Provincias

- Acuerdo de colaboración en materia de seguridad de la información en las entidades locales.

6. Junta de Castilla y León

- Apoyo a su Centro de Operaciones de Seguridad.

7. Generalitat Valenciana

- Apoyo y colaboración con el CSIRT-CV.

8. Generalitat de Catalunya

- Colaboración y apoyo al Centro de Seguridad. CESICAT.

9. Junta de Andalucía

- Colaboración para el Impulso de la Sociedad de la Información y apoyo al AndalucíaCERT.

10. Confederación Hidrográfica del Júcar

- Prueba piloto del Sistema de Alerta Temprana en Sistemas de Control Industrial. SAT-ICS

11. Otras comunidades autónomas y ayuntamientos

- Adhesión al Servicio de Alerta Temprana, SAT, del CCN-CERT.

12. Universidad

- Colaboración con el Consejo de Rectores de universidades Españolas (CRUE).
- Convenio de colaboración en materia de ciberseguridad.

13. Miembro de CSIRTes

- Grupo de trabajo CERT nacionales

14. AENOR

- Subcomités de seguridad TIC e identificación biométrica.

15. Foro ABUSES

- Grupo de trabajo con Proveedores de Servicio de Internet (ISP)

5. Spanish Federation of Towns and Provinces

- Collaboration agreement in terms of information security in local organisations.

6. Junta de Castilla y León

- Support for its Security Operations Centre.

7. Generalitat Valenciana

- Support and joint work with the CSIRT-CV.

8. Generalitat de Catalunya

- Joint work and support for the Security Centre. CESICAT.

9. Junta de Andalucía

- Joint work to boost the Information Society and support the Andalucia-CERT.

10. Júcar Hydrographic Confederation

- Pilot test of the Early Warning System in Industrial Control Systems. SAT-ICS

11. Other Regions and City Councils

- Members of the Early Warning System, SAT, from the CCN- CERT.

12. University

- Joint work with the Conference of Rectors of Spanish Universities (CRUE). Joint work agreement in terms of cyber-security
- Collaboration agreement on cybersecurity.

13. Member of CSIRTes

- National CERT Working Group

14. AENOR

- Subcommittees on CIS security and biometric identification.

15. ABUSES Forum

- Working group with Internet Service Providers (ISP)

Ámbito internacional

1. NCIRC de la OTAN (NATO Computer Incident Response Capability)

   - Los distintos CERT de los países miembros analizan y comparten información.

2. Agencia Europea de la Seguridad de las Redes y la Información (ENISA[8]) de la Unión Europea.

3. APWG (***AntiPhishing Working Group***)

   - Programa del Consejo de Europa enfocado a eliminar todo tipo fraude y robo de identidad a través de ciberataques como el envio de correos fantasma).

4. FIRST (***Forum of Incident Response and Security Teams***)

   - La primera y más importante de las organizaciones internacionales de Equipos de Respuesta a Incidentes, con miembros de Europa, América, Asia y Oceanía, procedentes del entorno gubernamental, económico, educativo, empresarial y financiero.

5. ***Trusted Introducer***

   - Principal foro europeo de CERT en el que colaboran, innovan y comparten información los CERT más destacados del continente, y que forma parte de TERENA, la Asociación Transeuropea de Investigación y Educación de Redes.

6. EGC (***European Government CERT Group***)

   - Organización que reúne a los principales CERT gubernamentales en Europa.

At international level

1. NATO NCIRC (NATO Computer Incident Response Capability)

   - The different CERT of member countries analyze and share information.

2. ENISA[8] - European Network & Information Security Agency

3. APWG (AntiPhishing Working Group)

   - European Council Programme aiming to wipe out all types of fraud and identity theft through phishing, pharming or ghost mails.

4. FIRST (Forum of Incident Response and Security Teams)

   - The first and most important of the existing international organisations with members in Europe, America, Asia and Oceania, coming from the governmental, economic, educational, business and financial environment.

5. Trusted Introducer

   - Main European forum for CERT where the most out- standing CERT on the continent work together, innovate and share infor- mation; they also form part of TERENA, the Pan-European Association of Network Research and Education.

6. EGC (European Government CERT Group)

   - Organisation that brings together the main governmental CERT in Europe.

[8] *European Network & Information Security Agency*

Organismo de Certificación OC
Certification Body

7

ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN

Certificación
Certification

- Funcional
  Functional
- Criptológica
  Cryptologic
- TEMPEST
  TEMPEST

Entre las funciones del Centro Criptológico Nacional está la de "constituir el Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, de aplicación a productos y sistemas en su ámbito". En este sentido, el OC realiza tres tipos de certificación en función de los aspectos de seguridad que se evalúen, pero siempre referidos a productos y sistemas STIC:

- Certificación funcional
- Certificación criptológica
- Certificación TEMPEST.

Anualmente se realiza una auditoría interna y una auditoría externa al OC. La auditoría interna la realiza personal del CNI (no perteneciente al CCN), para comprobar que la actividad de certificación se efectúa de acuerdo a las normas y procedimientos establecidos en cada caso.

La auditoría externa la realiza la Entidad Nacional de Acreditación (ENAC), según la correspondiente norma ISO, y es necesaria para que el OC mantenga la acreditación como entidad de certificación de producto. En 2014 se realizó la primera auditoría siguiendo la nueva normativa ISO 17065.

The National Cryptologic Centre's functions include "setting up the Certifcation Body for the National Evaluation Scheme and certifcation of information technology security, to be applied to products and systems in its feld." In this respect, the OC carries out three types of Certifcation depending on the security aspects being evaluated, although always referring to STIC products and systems:

- Functional certifcation
- Cryptological certifcation
- TEMPEST certifcation

The OC undergoes through an internal audit and an external audit every year. The internal audit is firstly carried out by CNI personnel (not belonging to the CCN) to check that the certification activity is following the rules and procedures set in each case.

The external audit is run by the National Accreditation Entity (ENAC), according to the ISO 17065, and it is necessary so that the OC maintains the accreditation as a product certification entity.

En el marco del reconocimiento internacional, el OC sigue participando activamente en dos importantes grupos de trabajo (técnicos y de gestión):

1. CCRA (***Common Criteria Recognition Arrangement***).

    - Ratificado en septiembre de 2014 por los 26 países integrantes.

2. SOGIS-MRA (***Senior Officers Group on Information Security – Mutual Recognition Agreement***).

    - Los participantes de este acuerdo son organizaciones o agencias gubernamentales de países de la Unión Europea o de AELC (Acuerdo Europeo de Libre Comercio), que representan a sus países. Cubre los siguientes dominios:

        - ***Smartcards and Similar Devices*** - Este dominio técnico está relacionado con las tarjetas inteligentes y dispositivos similares.

        - ***Hardware Devices with Security Boxes*** - Este dominio técnico está relacionado con productos compuestos por una o más placas de circuito impreso donde gran parte de la funcionalidad de seguridad requerida depende de su envoltura física (la llamada Caja de Seguridad).

Within the framework of international recognition, the OC continues to participate actively in two important working groups (technical and management):

1. CCRA (Common Criteria Recognition Arrangement).

    - Ratified in September 2014 by the 26 member countries.

2. SOGIS-MRA (Senior Officers Group on Information Security – Mutual Recognition Agreement).

    - Participants in this Agreement are organisations or government agencies from countries of the European Union or EFTA (European Free Trade Association), representing their country or countries. It covers the following domains:

        - Smartcards and Similar Devices - This IT-Technical Domain is related to smart cards and similar devices.

        - Hardware Devices with Security Boxes - This Technical Domain is related to products that comprises one or more printed circuit boards where its security functionality relies mostly on the physical casing of the product(a so-called Security Box").

Este tipo de certificación se articula mediante el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por Orden PRE/2740/2007, de 19 de septiembre, completado con sus procedimientos internos y haciendo uso de los documentos de soporte que se generan en los grupos internacionales CCRA y SOGIS-MRA.

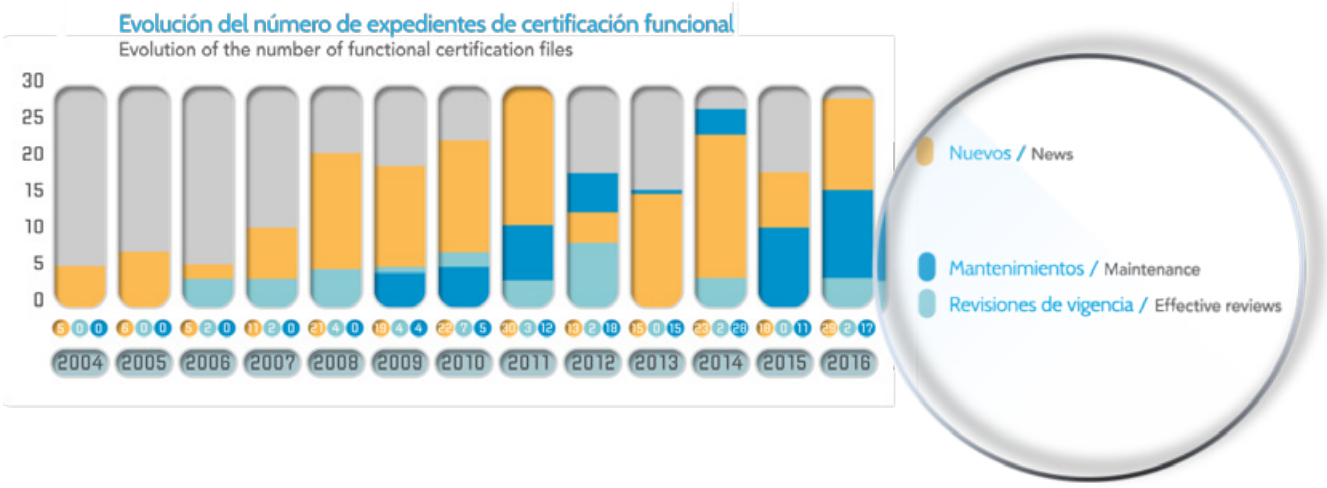
This type of certification is articulated by means of the Information Technology Security Evaluation and Certification Ruling, approved by Order PRE/2740/2007, dated 19th September, completed by its own internal procedures, and making use of the suppoting documents generated by the international groups CCRA and SOGIS-MRA.

Actuaciones destacadas en 2015 y 2016:

- Inicio de **84 expedientes de certificación**, entre nuevas solicitudes y mantenimiento o revisión de vigencia de los certificados ya existentes.
  - Cerca de dos tercios del total de los expedientes provienen del exterior, lo que ratifica la proyección internacional del OC.
- 25 resoluciones de certificación de productos o sistemas publicados en el BOE, tras pasar el proceso de evaluación, y 2 perfiles de protección.

Outstanding actions in 2015 and 2016:

- Start of **84 certification dossiers** among new applications, maintenance and review of existing certificates.
  - Nearly two-thirds of the certification dossiers come from overseasapplicants,which ratifies the Spanish Certification Body international renown.
- 25 certification resolutions of products or systems published in The BOE, after passing the evaluation process, and 2 protection profiles.



RESOLUCIONES BOE AÑO 2015
OFFICIAL STATE GAZETTE RESOLUTIONS 2015

Objeto a evaluar Object to evaluate	Solicitante de la certificación Certification Applicant	Nº de resolución en el BOE BOE resolution number
MRTT MPS-Secret OGM 6.1	EADS-CASA	8909, de 13 de marzo
CGP V100R005C00	HUAWEI	2419, de 30 de enero de 2015
DEVELOPMENT SITE GYD IBÉRICA	GYD IBÉRICA S.A.	2418, de 23 de enero de 2015
G&D INDIA SITE	G&D INDIA PVT. LTD.	4239, de 23 de febrero de 2015
ENIGMEDIA APP 1.0	ENIGMEDIA	9311, de 2 de julio de 2015
CYBEROAM FIRMWARE v10.5.4	CYBEROAM TECHNOLOGIES	484, de 10 de diciembre de 2014
HUAWEI LTE V100R008C01SPC820	HUAWEI	2417, 15 de enero de 2015

RESOLUCIONES BOE AÑO 2016
OFFICIAL STATE GAZETTE RESOLUTIONS 2016

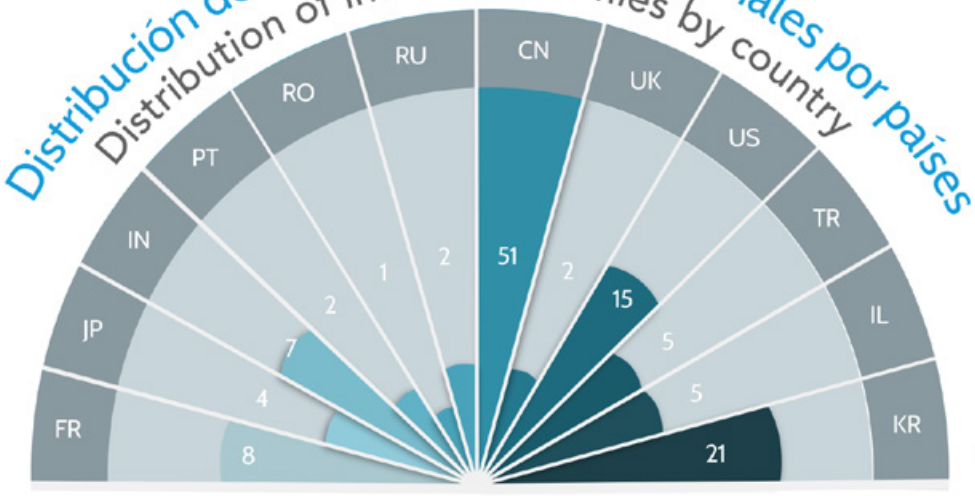
Objeto a evaluar Object to evaluate	Solicitante de la certificación Certification Applicant	Nº de resolución en el BOE BOE resolution number
ARIKARA 2	SAMSUNG	5038, de 1 de febrero de 2016
G&D DEVELOPMENT CENTER CHINA	G&D	4603, de 13 de mayo de 2016
G&D DEVELOPMENT CENTER CHINA	G&D	4603, de 13 de mayo de 2016
HUAWEI OCEANSTOR SOFTWARE	HUAWEI	5043, de 13 de abril de 2016
EUDEMON200E-N (USG6300&6500) SERIES FIREWALL	HUAWEI	5044, de 22 de abril de 2016
ASSET MANAGER WITH CONNECT-IT	HEWLETT PACKARD	5041, de 16 de marzo de 2016
SOLIDFIRE	SOLIDFIRE	5040, de 11 de marzo de 2016
EUDEMON1000E-N (USG6600) Series Firewall	HUAWEI	5109, de 25 de abril de 2016
EUDEMON8000E-X.USG9500	HUAWEI	5110, de 25 de abril de 2016
CERTUS	NERA COMPUTERS S.R.L.	BOE-A-2016-5886
GLU-X	EADS-CASA	BOE-A-2016-6402
A400M MPRS STD B1	EADS-CASA	BOE-A-2016-6403
KONA EPASSPORT BAC	KONA@I CO., LTD.	6960, de 20 de julio de 2016
KONA ePassport EAC	KONA@I Co., Ltd.	6961, de 20 de julio de 2016
CCN-PP-TP	CCN	BOE-A-2016-8305
PERFIL DE PROTECCIÓN CCN-PP-TP EAL2	CCN	BOE-A-2016-8305
MANTENIMIENTO ASSET MANAGER	HEWLETT PACKARD DEVELOPMENT	BOE-A-2016-8824
SOLARWINDS ORION	SOLARWINDS.	BOE-A-2016-11335
G&D Development Center Spain	GyD Ibérica S.A.U.	BOE-A-2016-11334
MANTENIMIENTO MPRS Std. B2.	AIRBUS DEFENSE AND SPACE	BOE-A-2016-11333

Distribución de expedientes (nacionales e internacionales)

Distribution of files (national and international)

Distribución de expedientes internacionales por países

Distribution of international files by country



7.3 Certificación Criptológica
Cryptologic Certification

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**. Tiene la consideración de cifrador nacional, con certificación criptológica, aquel equipo de cifra que ha sido evaluado y ha obtenido dicha certificación del CCN. Se dispone de distintos tipos de cifradores: IP[9], de datos, voz, fax, PKI[10], generadores de números aleatorios, centros de gestión, etc.

Los productos aprobados para el cifrado de información nacional clasificada o que legalmente requieran protección se incluyen en el **catálogo de productos con certificación criptológica** (Guía CCN-STIC 103, actualizada en julio de 2016), y el **procedimiento de evaluación de productos criptológicos** está recogido en la Guía **CCN-STIC 102**.

Durante los años 2015 y 2016 se realizaron las siguientes actividades:

The CCN is the Organisation in charge of drawing up the Catalogue of Products with Cryptologic Certification that includes products capable of protecting **national classified information**. A crypto product with national cryptologic certification is the one that has gone satisfactorily under a cryptologic evaluation perform by the CCN, and a certification has been granted: IP[9], data, voice, fax, PKI[10], random number generators, management centres, etc.

Products that have been approved to protect national classified information or that legally require protection are included in the **catalogue of products with cryptologic certification** (**CCN-STIC 103** guide updated in July 2016) and the **cryptologic product evaluation procedure** is compiled in the **CCN-STIC 102** guide.

During 2015 and 2016, the following activities were run:

7.3.1 Desarrollo normativo de la evaluación de productos STIC 2015-2016
Standard development of SICT product evaluation

Durante 2016 se ha desarrollado una nueva normativa para la aprobación y cualificación de productos de seguridad TIC en línea con el resto de normas internacionales. En un mercado cada vez más globalizado, esto permitirá a las empresas españolas poder vender sus productos, de manera más ágil, en entornos con altos requerimientos de seguridad como OTAN o UE.

During 2016, a new standard has been developed for the approval and qualification of CIS security products in line with other international standards. In an increasingly globalised market, this will allow Spanish companies to be able to sell their products, in a more streamlined way, in environments with high security requirements such as NATO or the EU.

Sistema Färist Mobile
Färist Mobile System

El sistema "Färist Mobile" proporciona comunicaciones móviles seguras mediante una red privada virtual (VPN) desde los terminales móviles seguros (Terminal Móvil Nexus 5 y Sony Xperia X) hasta la infraestructura TIC de la organización.

Este producto fue aprobado por el CCN en 2014 para procesar información nacional clasificada hasta nivel DIFUSIÓN LIMITADA. Durante 2015 y 2016 se ha continuado evaluando la evolución del producto a **Android 6.0 Marshmallow** así como su migración a nuevas plataformas (**Sony Xperia X**).

The "Färist Mobile" system provides secure mobile communications by means of a virtual private network (VPN) from secure mobile terminals (Nexus 5 and Sony Xperia X Mobile Terminal) to the organisation's CIS infrastructure.

This product was approved by the CCN in 2014 to process national classified information up to the level of RESTRICTED. During 2015 and 2016, evaluation has continued on the evolution of the product to **Android 6.0 Marshmallow** as well as its migration to new platforms (**Sony Xperia X**).

[9] *Internet Protocol*
[10] *Public Key Infrastructure*

Aplicación KeyOne
KeyOne application

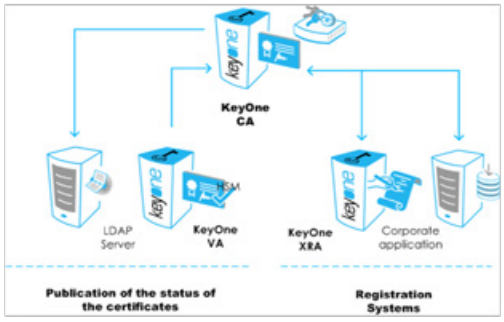
Durante 2015 se ha certificado la aplicación KeyOne, de la empresa Safelayer, para la gestión de infraestructura de clave pública (PKI). Está compuesta por los siguientes productos:

- Keyone CA. Elemento principal de una familia de productos que se integran en un sistema para permitir el despliegue de una tecnología PKI con certificados X509 v3. Conforma la figura de la Autoridad de Certificación.
- KeyOne XRA. Aplicación que implementa la funcionalidad de registro (usuarios, entidades o datos) de la PKI.
- KeyOne VA. Aplicación de validación de certificados y firmas (basado en un OCSP[11]).
- KeyOne TSA. Componente del producto encargada de realizar el sellado de tiempo.

COMSEC Admin+
COMSEC Admin+

El sistema COMSEC Admin+, creado por la empresa española INDRA SCS, asegura la confidencialidad de las comunicaciones de voz y mensajería. Durante 2016, el CCN ha realizado la revisión de la última versión de esta aplicación en la que se incluyen importantes mejoras de seguridad.

The COMSEC Admin+ system, created by the Spanish company INDRA SCS, ensures the confidentiality of voice and messaging communications. During 2016, the CCN reviewed the latest version of this application including important security improvements.



During 2015, the KeyOne application of Safelayer has been certified for public key infrastructure (PKI) management. It is composed of the following products:

Keyone CA. Main elements of a product family including a system to allow deployment of PKI technology with X509 v3 certificates. It shapes the figure of the Certification Authority.

KeyOne XRA. Application that implements the PKI register functional feature (users, entities or data).

KeyOne VA. Application to validate certificates and signatures (based on an OCSP[11]).

KeyOne TSA. Time stamping product component.

Crypto Token USB EP851
Crypto Token USB EP851

Se ha realizado una revisión de la nueva versión del equipo (Crypto Token USB), tras haber sido adquirido por la empresa Epicom a Datatech. Dicha versión ha sido aprobada para proteger información clasificada.

The new version of the equipment (Crypto Token USB) has been reviewed, after having been acquired by the EPICOM company, Datatech. This version has been approved to protect classified information.

[11] Online *Certificate Status Protocol*

Cifrador EP430TX y EP430TN
EP430TX and EP430TN IP Crypto

Cifrador de la empresa Epicom que admite la preinstalación de dos criptologías distintas, pudiendo ser empleado el mismo cifrador en distintas redes. En función de la criptología instalada en el cifrador, existe la versión nacional denominada EP430TX y la versión OTAN EP430TN.

Durante 2016 se ha realizado una evaluación criptológica y se ha aprobado de manera interina hasta la finalización de su evaluación funcional que actualmente se está llevando a cabo.

Tras finalizar la evaluación del cifrador nacional EP430TX, se comenzará con la evaluación nacional del EP430TN, que es compatible con el EP430GN, y se enviará a SECAN para su evaluación OTAN.

EPICOM IP Crypto allows pre-installation of two types of cryptologic allowing the use of the same crypto productin different networks. Depending on the cryptologic installed in the equipment, there is the national version called EP430TX and the NATO version EP430TN.

During 2016, a cryptologic evaluation was carried out and has received interim approval whilst its on-going functional evaluation is completed.

After completing the evaluation of the EP430TX national encryptor, national evaluation will begin on the EP430TN, compatible with the EP430GN and it will be sent to SECAN for its NATO evaluation.

Cifrador EP430GU
EP430GU Crypto Product

El equipo EP430GU es un cifrador IP de alta velocidad desarrollado por la empresa EPICOM. Cumple todas las normas de seguridad exigidas por la Union Europea. Este equipo ha sido elegido para proteger las comunicaciones terrenas del sistema GALILEO.

Actualmente se encuentra en proceso de evaluación. Ha sido aprobado de manera provisional hasta la finalización de su evaluación funcional.

EP430GU equipment is a high speed IP encryptor developed by EPICOM that meets all EU security standards. This equipment has recently received a great boost as it was chosen to protect land communications for the GALILEO system.

It is currently being under evaluation and has received interim approval until the end of its functional evaluation.

7.4 CERTIFICACIÓN TEMPEST
TEMPEST CERTIFICATION

El término TEMPEST hace referencia a las investigaciones y estudios de emanaciones comprometedoras relacionadas con la información clasificada que está siendo transmitida, recibida, manejada o de alguna manera procesada por equipos o sistemas electrónicos. Estas emanaciones no intencionadas, una vez detectadas y analizadas, pueden llevar a la obtención de la información. Asimismo, el término TEMPEST se refiere también a las medidas aplicadas para la protección contra dichas emanaciones comprometedoras.

El CCN, como Autoridad de Certificación de seguridad TIC en el ámbito EMSEC (seguridad de las emanaciones), tiene entre otras misiones, el desarrollo de normativa nacional en este campo, la evaluación y certificación de equipos, sistemas e instalaciones, así como la participación y asesoramiento en diferentes foros. Actúa en todos ellos como Autoridad TEMPEST Nacional (NTA).

En los dos últimos años se realizaron las siguientes actividades de evaluación EMSEC:

The term TEMPEST refers to research and studies on compromising emanations related to classified information that is being sent out, received, handled or in any way processed by electronic equipment or systems. These unintentional emanations, once detected and analysed, can lead to information being obtained. In addition, the term TEMPEST also refers to measures applied to prevent against these compromising emanations.

The CCN's many assignments, as the Certification Authority for CIS security in the EMSEC field (Emanations Security), include developing a national standard in this field, evaluation and certification of equipment, systems and facilities, plus participation and consultancy in different forums, acting in all of them as the national TEMPEST Authority (NTA).

Regarding the security evaluation of the emanations and facilities where they are located, over the last two years the following activities have been carried out:

Certificación ZONING de locales
ZONING certification for premises

Se ha llevado a cabo las certificaciones ZONING de instalaciones (213 expedientes). Casi la mitad de ellos han sido renovaciones de certificados cuya validez había caducado. Esta cifra se ha incrementado notablemente debido a que la renovación de los certificados debe hacerse cada cinco años.

Por otra parte, el CCN también ha realizado evaluaciones tanto para empresas como para organismos de la Administración Pública dentro de los procesos de acreditación de sistemas para manejo de información clasificada.

También ha crecido el número de trabajos para empresas debido a los nuevos requisitos marcados por la Oficina Nacional de Seguridad (ONS), en los que se especifica que siempre será necesaria la acreditación de un sistema para procesar la información clasificada.

ZONING certifications have been carried out for installations, covering 213 dossiers. Almost half of them were renewals of certificates that were no longer valid. This figure has increased considerably due to the fact that certificates must now be renewed every five years.

On the other hand, the CCN has also carried out evaluations both for companies and Public Administration organisations within the system accreditation processes to handle classified information.

There has been a considerable increase in the number of jobs for companies due to new requirements set by the National Security Office (ONS), specifying that accreditation will always be necessary to process classified information.

Certificación ZONING/TEMPEST de equipos y sistemas
ZONING / TEMPEST certification for equipment and systems

La actividad se ha centrado en la evaluación ZONING de equipos y sistemas para diferentes organismos. También se han realizado evaluaciones ZONING de sistemas para empresas.

Este tipo de trabajos de certificaciones ZONING de equipos ha sufrido un notable incremento por la normalización requerida en cualquier proceso de acreditación de un sistema, en el que se deben evaluar los equipos empleados e instalarlos de acuerdo a las condiciones de seguridad de los locales.

Es importante resaltar la importancia de solicitar a las empresas proveedoras de equipamiento informático los certificados ZONING de los equipos, antes de su adquisición. En la **Guía CCN-STIC 104 de Catálogo Productos ZONING** se pueden consultar los resultados de los equipos comerciales ya evaluados.

Activity has focussed on ZONING evaluation for equipment and systems for different organisations. System ZONING evaluations have also been carried out for companies.

This type of equipment ZONING certification work has increased considerably due to the standardisation required in any accreditation process for a system, that should assess the equipment used and install it according to the premises' security conditions.

It is important to highlight the importance of asking the companies providing computer equipment for the ZONING certificates for this equipment, prior to purchase. In the C**CN-STIC 104 Guide on ZONING Product Catalogue**, it is possible to consult results from previously assessed commercial equipment.

Evaluación TEMPEST del A400M
TEMPEST evaluation of the A400M

Evaluación y certificación TEMPEST de plataformas
TEMPEST evaluation and certification for platforms

El CCN sigue participando en los procesos de certificación de las plataformas del Eurofighter (EF2000) y del Airbus A400M. Dentro de este último programa, durante 2015 se han desarrollado actividades de coordinación con la empresa Airbus Defence & Space para la documentación y la preparación de aspectos técnicos para la evaluación del A400M. En los meses de abril y mayo de 2016 se llevaron a cabo los trabajos de evaluación y certificación del avión con asistencia de representantes de las naciones que desarrollan el programa. Se ha dado respuesta a cuantas aclaraciones fueron solicitadas por las distintas Autoridades Nacionales de los países participantes.

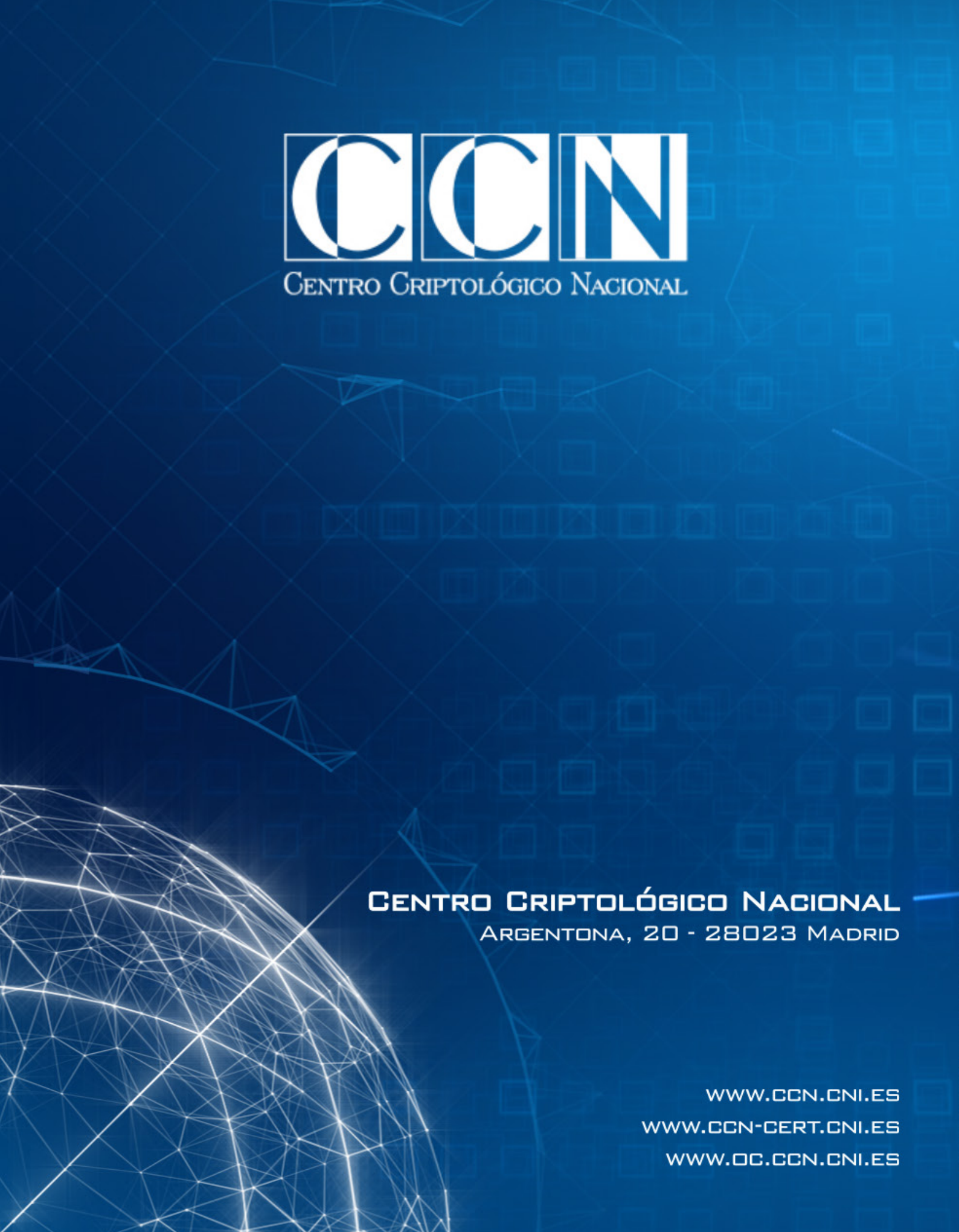
The CCN continues participating in the certification processed for Eurofighter (EF2000) and Airbus A400M platforms. Within the latter program, coordination activities have been developed during 2015 with Airbus Defence & Space to document and prepare technical aspects for the A400M evaluation.

In April and May 2016, evaluation and certification work was done on the plane. At the same time, representatives from the different nations taking part in the Programme were invited, providing clarifications for any queries raised by the different National Authorities from the participating countries.

Edita: Centro Criptológico Nacional
Edit: National Cryptologic Centre

Diseño, maquetación e infografías/design: Ariel Pernas Mencia
Fotografía/photography: Centro Criptológico Nacional
Imprime/print: Imprenta Sarabia SL

D.L. M-9770-2017



Centro Criptológico Nacional
Argentona, 20 - 28023 Madrid

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