CCN
Centro Criptológico Nacional

Informe de Actividades
Activity Report

2011 - 2012

CENTRO CRIPTOLÓGICO NACIONAL

Informe de Actividades
Activity Report

2011 - 2012

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA

1 Carta del secretario de Estado director

Querido lector:

Al cumplir doce años desde su creación, a través de la Ley 11/2002, de 6 de marzo, el **Centro Criptológico Nacional** (CCN), adscrito al **Centro Nacional de Inteligencia** (CNI), abre sus puertas una vez más y presenta este **Informe de Actividad 2011-2012**, con el que dar cuenta de los principales hitos realizados en materia de **ciberseguridad**. Dos años, en los que el CCN ha ido adecuándose, y en la medida de lo posible adelantándose, a una realidad compleja y cambiante, en donde las **ciberamenazas** se incrementan día a día, varían (en función de la motivación de los atacantes o sus objetivos), se modifican los métodos de ataque, aparecen nuevas vulnerabilidades, nuevos dispositivos o nuevas técnicas y se incrementan los servicios ofrecidos a través de Internet. La paradoja estriba en que a medida que crece la importancia, el uso y las posibilidades que ofrece este **ciberespacio**, crecen sus riesgos y amenazas, quedando de manifiesto la fragilidad de nuestras sociedades ante la dependencia cibernética.

Sirva de ejemplo, los más de 6.250 ciberincidentes gestionados entre 2011 y 2012 por el **CCN-CERT** (Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional), una cifra muy superior a la registrada en años anteriores y con un grado de criticidad y repercusión cada vez más elevado.

Esta intensidad y sofisticación de los ciberataques ha puesto en evidencia la capacidad de los atacantes para

LETTER FROM THE SECRETARY OF STATE DIRECTOR

Dear Reader,

On celebrating its twelfth anniversary, through Law 11/2002, dated 6th March, the National Cryptologic Centre (CCN), dependent on the National Intelligence Centre (CNI), is opening its doors once again to present this Activity Report 2011-2012, featuring major cybersecurity milestones. Over the last two years, the CCN has been adapting and, as far as possible, getting one step ahead of a complex, changing reality, where cyber-threats are increasing on a daily basis and vary (depending on the perpetrators' intentions or their targets), the attack methods change, new vulnerabilities, new devices or new techniques emerge and more services are offered over the Internet. The paradox lies in the fact that as the importance, use and possibilities offered by cyberspace grow, its risks and threats also increase, demonstrating just how fragile our societies are in the light of existing cybernetic dependency.

As an example, over 6250 cyber-incidents were managed between 2011 and 2012 by the CCN-CERT (National Cryptologic Centre's Computer Emergency Response Team), a much higher figure than registered in previous years, increasingly critical with greater repercussions.

This cyber-attack intensity and sophistication has once again demonstrated the attackers' capability to cause enormous damage and the challenge

causar enormes daños y el reto que supone para todos los agentes implicados adoptar las medidas de seguridad necesarias que hagan a nuestros sistemas de información más resistentes a las amenazas del ciberespacio. Por ello, la ciberseguridad debe entrar de inmediato en la agenda de todos: gobiernos, empresas y ciudadanos y hacerlo además con voluntad de permanencia.

Así lo han entendido la mayor parte de los gobiernos de todo el mundo y también el nuestro. El **Gobierno de España** está desplegando una significativa actividad para definir su estrategia de **ciberseguridad**, verdadero hilo conductor de las acciones que, sobre tales materias, han de presidir la mesa de trabajo de los responsables públicos y las empresas españolas que hagan uso de redes y sistemas de información, ya sea para la prestación de sus servicios o el cumplimiento de sus misiones.

En esta misma línea, el **Centro Nacional de Inteligencia** está dando la máxima prioridad a las ciberamenazas, reorganizándose internamente, incorporando recursos y coordinando sus capacidades internas. Así, junto con el CCN, contribuye a la mejora de la ciberseguridad en España, articulando la respuesta y gestión de los ciberincidentes en torno al CERT Gubernamental/nacional, y promoviendo y certificando los productos y sistemas utilizados.

Todo ello, impulsando la colaboración internacional y la necesaria implicación de organismos y empresas, particularmente aquellas cuya actividad se enmarca en los sectores estratégicos. El bienestar y futuro de nuestro país depende de ello.

Félix Sanz Roldán
Secretario de Estado director del CNI,
Director del CCN
CNI SECRETARY OF STATE DIRECTOR
CCN DIRECTOR

that this represents for all agents involved, adopting the necessary security measures to strengthen our information systems against cyberspace threats. Consequently, cybersecurity is on everyone's agenda: governments, companies and citizens and it is here to stay.

This is how the situation has been understood by the majority of governments all over the world, including our own. The Spanish Government is deploying a significant workforce to strategically define cybersecurity, a real core theme for appropriate actions that have to be tackled by public decision-makers and Spanish companies that use networks and information systems to provide their services or complete their assignments.

Along this same line, the National Intelligence Centre is giving maximum priority to cyber-threats, undergoing internal reorganisation, adding resources and coordinating its internal skills. Along with the CCN, helps to improve cybersecurity in Spain, organising cyber-incident response and management around the governmental/national CERT and promoting and certifying the products and systems used.

All this involves driving international collaboration and the necessary implication of organisations and companies, particularly any working in strategic sectors. Our country's wellbeing and future depend on it.

2 Índice
TABLE OF CONTENTS

3 Panorama de la ciberseguridad

Insistir, en 2013, en el grado de dependencia que nuestra sociedad tiene de las TIC, constituye un lugar común. Los servicios y aplicaciones que continuamente van apareciendo hacen impensable una sociedad evolucionada que no se sustente en una tecnología que, al mismo tiempo, propicia la aparición de incidentes de ciberseguridad, provocados la mayoría de las veces por agentes dañinos, que pretenden sacar partido de las vulnerabilidades que, inevitablemente, tiene.

Si a ello se le unen los **beneficios** que los atacantes obtienen (económico, político o de otro tipo), no es de extrañar la importancia que en los últimos años viene dándose a la ciberseguridad.

Lamentablemente y pese a que las medidas que instituciones públicas y empresas van adoptando son útiles en muchos casos, en otras tantas ocasiones han resultado, sin embargo, insuficientes. La mayor parte de los ataques sufridos han evidenciado fallos ocasionados por la ausencia de **medidas de seguridad, métodos, procedimientos, productos y herramientas** debidamente implementados y certificados.

Cuando a ello se le suma una **escasa concienciación y/o formación** en materia de ciberseguridad, existe una alta probabilidad de no tomar las medidas de seguridad adecuadas que puedan evitar los incidentes más graves o, cuando menos, limitar sus consecuencias.

Aunque el origen de las ciberamenazas no es reciente, sólo de unos años a esta parte hemos podido comprobar cómo los gobiernos de todo el mundo las han catalogado como fuente de sus mayores preocupaciones, pasando de la incredulidad al desconcierto y de éste a la franca adopción de medidas de prevención, detección y respuesta. Máxime, si tenemos en cuenta que tras las redes y los sistemas de información (púbicos y privados) hay importantes intereses que deben ser defendidos.

Estos intereses no se limitan a la mera información, sino que se extienden a todo tipo de servicios, vitales para el normal desenvolvimiento de las sociedades occidentales.

A raíz de los incidentes que han ocurrido en todo el mundo durante 2012 se ha puesto de manifiesto la necesidad de reforzar la seguridad de nuestras TIC.

CYBERSECURITY LANDSCAPE

It has become a common theme in 2013 to point out just how dependent our society has become on ICTs. The continuous appearance of services and applications make it unthinkable that our evolved society might not be sustained by technology that, at the same time, leads to cybersecurity incidents, caused more often than not by malicious agents attempting to make the most of its inevitable vulnerabilities. If you add to that the benefits that the attackers obtain (economical, political or other types), it comes as no surprise that cybersecurity has become extremely important over the last few years.

Unfortunately and despite the fact that the measures adopted by public institutions and companies are often useful, on just as many occasions however, they have turned out to be insufficient. Most attacks have demonstrated faults caused by the absence of security measures, methods, procedures, products and tools duly implemented and certified. When this is combined with poor awareness and/or training regarding cybersecurity, there is a high probability that the right security measures will not be taken to avoid more serious incidents or, at least limit their consequences.

Although cyber-threats are not a new concept, it has only been during the last few years that governments all over the world have begun to classify them as the source of their greatest concerns. Their reactions have gone from incredulity to bewilderment, leading to adopting prevention, detection and response measures, all the more so if we take into account that there are important interests that should be defended behind the networks and information systems (public and private). These interests are not limited to mere information but they extend to all types of services, vital for normal day to day running of western societies. As a result of incidents that occurred throughout the world during 2012, it has become crystal clear that our ICTs are vulnerable to these attacks.

Main cyber-threats

When analysing the cyber threat situation over the last two years and incidents that have taken place, we would highlight the following aspects [1] :

- **Cyber-espionage** has become the greatest threat for government and business sectors. In addition to work carried out

Principales ciberamenazas

Si analizamos la situación de los dos últimos años con respecto de las ciberamenazas e incidentes ocurridos destacaríamos los siguientes aspectos[1]:

- El **ciberespionaje** se ha erigido en la mayor amenaza para los gobiernos y los sectores empresariales. Además del realizado por los propios estados (o sus colaboradores), los espías corporativos están utilizando técnicas cada vez más avanzadas (**APTs**) para robar secretos empresariales o datos de clientes con fines de lucro y de mejora estratégica. Por tanto, las organizaciones públicas y privadas que manejan información con alto valor estratégico, económico o político, esenciales para la seguridad nacional o para el conjunto de la economía, son hoy más vulnerables que nunca y un objetivo claro de los atacantes.

- A este hecho se suma el incremento continuado del **ciberdelito** realizado por profesionales y destinado a todo tipo de dispositivos a través de código dañino y utilizando, en numerosas ocasiones, técnicas de ingeniería social a través de las **Redes Sociales**.

  En este mismo capítulo conviene citar los **ataques contra servicios web** y la consolidación del *ransomware* (troyanos diseñados para cifrar los datos del disco duro del usuario o bloquearle el acceso al sistema, exigiéndole dinero a cambio de recuperar la información y/o el sistema).

- Los **grupos *hacktivistas*** que han llegado a ocupar las portadas de los medios de comunicación de todo el mundo (Anonymous y LulzSec, particularmente) y cuyos ataques suelen centrarse en la desfiguración de páginas web, ataques DDoS y la difusión de los datos comprometidos tras el ataque. También conviene señalar a los ciberterroristas que utilizan Internet más como un medio que como un objetivo en sí mismo. De igual modo, los denominados **ciberinvestigadores**, que buscan vulnerabilidades de los sistemas o de los sitios web, también han resultado, en ocasiones, una amenaza.

- Las **vulnerabilidades** y ***exploits*** han ido en aumento, no tanto en número, como en importancia. De hecho, uno de los principales métodos que usan los ciberdelincuentes para instalar sus programas dañinos en el ordenador de la víctima consiste en explotar vulnerabilidades en las aplicaciones que no se han actualizado debidamente. Este método se basa, al tiempo, en la existencia de vulnerabilidades y en la dejadez de los usuarios y empresas para parchear sus aplicaciones.

(1) Informe de Amenazas CCN-CERT IA-09/13. "Ciberamenazas 2012 y Tendencias 2013"

(1) CCN-CERT Threat Report (IA-09/13) "Cyber Threats 2012 and Trends 2013"

by each country (or their associates), corporate spies are using increasingly advanced techniques (**APTs**) to steal business secrets or customer data for profitmaking and strategic improvement purposes. Therefore, public and private organisations that handle information with high strategic value, economic or political, essential for national security or for the economy as a whole, are more vulnerable than ever today and a clear target for attackers.

- This point is added to the continual increase of **cybercrimes** carried out by professionals, targeting all types of devices through malicious code and, on many occasions, using social engineering techniques through social networks. This same chapter should also mention **attacks on internet services** and the consolidation of ransomware (Trojan designed to encrypt the data on a user's hard disk and block their access to the system, demanding money in exchange for recovering the information and/or the system).

- **Hacktivist groups** that have managed to grab headlines in the world's media (Anonymous and LulzSec, in particular) and whose attacks usually focus on websites defacement, DDoS attacks and broadcasting compromising information after the attack. It is also worth mentioning cyberterrorists that use the Internet more as a means than as an actual target. In the same way, the so-called cyber-investigators who look for vulnerabilities in systems or websites have also occasionally turned out to be a threat.

- **Vulnerabilities and exploits** are on the rise, no so much in terms of numbers but in terms of importance. In fact, one of the main methods used by cyber-criminals to install their malware programs in a victim's computer involves exploiting vulnerabilities in applications that have not be properly patched. This method is based, over time, on the existence of vulnerabilities and a laissez-faire attitude from users and companies in terms of patching their applications.

Objetivos y grupos de amenazas por su relevancia [2]

GOALS AND THREAT GROUPS BY THEIR RELEVANCE [2]

Relevancia desconocida RELEVANCIA UNKNOW | Baja relevancia RELEVANCIA LOW | Media relevancia RELEVANCIA MEDIUM | Alta relevancia RELEVANCIA HIGH

	Organismos públicos PUBLIC ORGANISATIONS	**Organizaciones privadas** PRIVATE ORGANISATIONS	**Ciudadanos** CITIZENS
Estados STATES	Ciberespionaje CYBER-ESPIONAGE	Ciberespionaje CYBER-ESPIONAGE	Ciberespionaje CYBER-ESPIONAGE
Organizaciones privadas PRIVATE ORGANISATIONS		Ciberespionaje CYBER-ESPIONAGE	
Delincuentes profesionales PROFESSIONAL CRIMINALS	Interrupción como consecuencia de infección por malware y spam INTERRUPTION DUE TO INFECTION BY MALWARE AND SPAM	Interrupción como consecuencia de infección por malware y spam INTERRUPTION DUE TO INFECTION BY MALWARE AND SPAM	Interrupción como consecuencia de infección por malware y spam INTERRUPTION DUE TO INFECTION BY MALWARE AND SPAM
		Fraude de identidad digital DIGITAL IDENTITY FRAUD	Fraude de identidad digital DIGITAL IDENTITY FRAUD
		Chantaje BLACKMAIL	Chantaje BLACKMAIL
	Interrupción de servicios on-line INTERRUPTION TO ONLINE SERVICES	Interrupción de servicios on-line INTERRUPTION TO ONLINE SERVICES	
Ciberterroristas CIBERTERRORISTAS	Sabotaje SABOTAGE	Sabotaje SABOTAGE	
Hacktivisttas HACKTIVISTS	Publicación de información confidencial PUBLICATION OF CONFIDENTIAL INFORMATION	Publicación de información confidencial PUBLICATION OF CONFIDENTIAL INFORMATION	Publicación de información confidencial PUBLICATION OF CONFIDENTIAL INFORMATION
	Interrupción de Infraestructuras Críticas INTERRUPTION OF CRITICAL INFRAESTRUCTURES	Interrupción de Infraestructuras Críticas INTERRUPTION OF CRITICAL INFRAESTRUCTURES	
	Interrupción de servicios *online* INTERRUPTION TO ONLINE SERVICES	Interrupción de servicios *online* INTERRUPTION TO ONLINE SERVICES	
	Engaño FRAUD	Engaño FRAUD	Engaño FRAUD
Script kiddies SCRIPT KIDDIES	Interrupción de servicios *online* INTERRUPTION TO ONLINE SERVICES	Interrupción de servicios *online* INTERRUPTION TO ONLINE SERVICES	
Ciberinvestigadores CIBERINVESTIGATORS	Publicación de información confidencial PUBLICATION OF CONFIDENTIAL INFORMATION	Publicación de información confidencial PUBLICATION OF CONFIDENTIAL INFORMATION	
Actores internos INTERNAL PLAYERS	Publicación de información confidencial PUBLICATION OF CONFIDENTIAL INFORMATION	Publicación de información confidencial PUBLICATION OF CONFIDENTIAL INFORMATION	
		Chantaje Blackmail	
No es actor NOT A PLAYER	Daños por fuego, agua y desastres naturales DAMAGE BY FIRE, WATER OR NATURAL DISASTERS	Daños por fuego, agua y desastres naturales DAMAGE BY FIRE, WATER OR NATURAL DISASTERS	
	Fallo y/o ausencia de hw/sw FAULT AND/OR ABSENCE OF HW/SW	Fallo y/o ausencia de hw/sw FAULT AND/OR ABSENCE OF HW/SW	

(2) Informe de Amenazas CCN-CERT IA-09/13. "Ciberamenazas 2012 y Tendencias 2013"

(2) CCN-CERT Threat Report (IA-09/13) "Cyber Threats 2012 and Trends 2013"

- "*Cloud Computing*": Los atacantes actúan allí donde estén los usuarios, y este camino parece discurrir, incesantemente, hacia la utilización de servicios en la nube. Por tanto, estos servicios constituyen un objetivo de primera magnitud.

- Telefonía móvil: Durante 2012 las muestras de malware detectadas para las plataformas móviles han crecido exponencialmente, especialmente en Android. Este malware se difunde normalmente mediante aplicaciones que aprovechan el comportamiento de un usuario que autoriza a ciegas cualquier permiso solicitado por las mismas al instalarse en el teléfono. Por la permanente conexión de estos dispositivos a Internet, las posibilidades de compromiso de datos y de control del propietario son de mucho interés para el atacante. Además la **seguridad para las plataformas móviles es deficiente**.

  La **concienciación de usuarios** y organizaciones sobre los problemas de seguridad en su empleo e**s muy baja.** No se les suelen aplicar las políticas de seguridad utilizadas en las redes corporativas. Existe una tendencia creciente al empleo del teléfono personal en la gestión de información mediante la recepción de correos, el uso de mensajes instantáneos (mediante aplicaciones tipo WhatsApp) o habilitando el acceso en remoto a diferentes aplicaciones de la red corporativa a través de estos dispositivos (lo que se conoce como BYOD -*Bring Your Own Device*-).

- 0-day: Existe, también, un mercado negro de venta de vulnerabilidades que no permite disponer de una visión completa de las que están disponibles en Internet. Estas vulnerabilidades se conocen como *Zero-Day* (por no ser conocidas por el fabricante) y facilitan al atacante la infección de los sistemas objetivos. **No existe defensa para este tipo de vulnerabilidad**.

  Se constata un elevado interés por parte de algunos Estados y del crimen organizado en la adquisición de este tipo de vulnerabilidades, traducido en un **incremento del precio** en el mercado clandestino, lo que limita el efecto de los programas de recompensas que por su notificación ofrecen empresas como Microsoft, Google o Apple para la mejora de sus productos. Las vulnerabilidades más cotizadas son las del sistema operativo Windows, la de los diferentes navegadores Web y las asociadas a telefonía móvil (especialmente iPhone y Android).

MAIN CYBER-THREATS

- **Cloud Computing:** Attackers are targeting users directly and this path seems to inevitably lead to using cloud computing services. Consequently, these services have become a major goal.
- **Mobile phone:** During 2012, samples of malware detected for the different mobile platforms have grown exponentially, particularly in Android. This malware is normally spread using applications that make the most of average users blindly authorising any permission requested by the applications when installed on the phone. Because these devices are permanently connected to the Internet, the chance of data being compromised and gaining control over the owner makes this very interesting for attackers. It should be highlighted that mobile platform security is severely lacking. In this field, awareness among users and organisations regarding security problems when using these devices is very low. Security policies used in corporate networks are not usually applied. In addition, there is a growing trend to use your own phone to manage information from different organisations by means of receiving mail, instant messaging (using applications like WhatsApp) or enabling remote access to different applications from the corporate network through these devices (known as BYOD-Bring Your Own Device-).
- **0-day**: There is also a black market for selling vulnerabilities, meaning that it cannot be exaclty known what is available over the Internet. These vulnerabilities are known as Zero-Day (as they are not known to the manufacturer) and make it easier for attackers to infect target systems. There are no defences against this type of vulnerability. There is high interest from some States and organised crime to acquire this type of vulnerabilities that has led to their price rising on the clandestine market, limiting the effect of reward programs offered by companies such as Microsoft, Google or Apple to improve their products. The most valued vulnerabilities correspond to the Windows operating system, different Internet browsers and any associated with mobile phones (particularly iPhone and Android).

4 Centro Criptológico Nacional, hoy

El Centro Criptológico Nacional (CCN) es un Organismo, adscrito al Centro Nacional de Inteligencia (CNI), creado en el año 2002 con el fin de garantizar la seguridad TIC 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)**, que incluye al Centro Criptológico Nacional (CCN), y que tiene entre otras misiones actuar contra el ciberespionaje, neutralizando las actividades de inteligencia y mejorando la seguridad de los sistemas de información del país, protegiendo el patrimonio tecnológico de España.

- 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.

NATIONAL CRYPTOLOGIC CENTRE, TODAY

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), including the National Cryptologic Centre (CCN) with assignments including fighting cyber-espionage, neutralising counterintelligence activities and providing security for the country's information system, protecting Spain's technology.

- **Royal Decree 421/2004**, 12th March, regulating and defining the sphere and functions of the National Cryptologic Centre (CCN).

- Real Decreto 03/2010, de 8 de enero, de desarrollo del **Esquema Nacional de Seguridad** (ENS), 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, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte del CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos. Asimismo en sus artículos 36 y 37 establece en torno al **CCN-CERT** la capacidad de respuesta ante incidentes de las Administraciones Públicas.

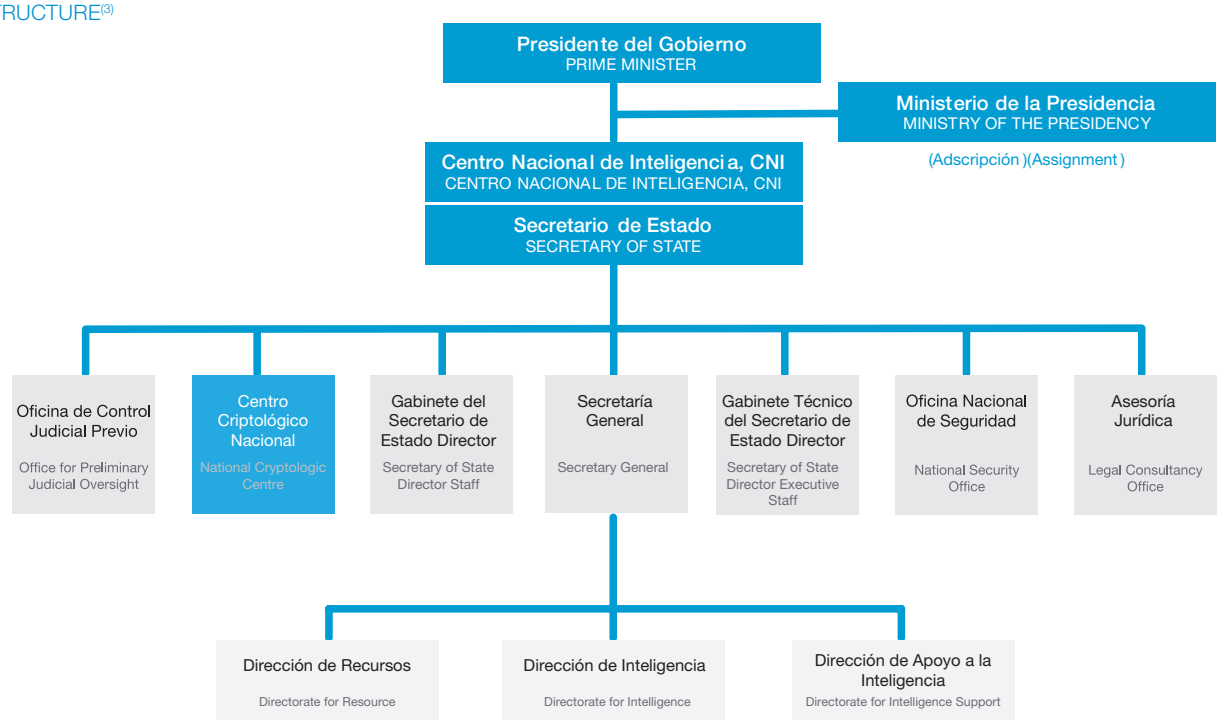
- Comisión Delegada del Gobierno para Asuntos de Inteligencia, que define anualmente los objetivos del CNI mediante la Directiva de Inteligencia, que marca la actividad del Centro.

- **Presidential Ministerial Order PRE/2740/2007**, dated 19th September , that regulates the National Evaluation Framework 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, establishing basic principles and minimum requirements, as well as protection measures to be implanted in Administration systems. It also promotes CCN writing and sending out information and communication technology security guides to help improve compliance with these minimum requirements. In addition, articles 36 and 37 give the CCN-CERT the capability to tackle incidents in Public Administrations.

- **Delegate Government Commission for Intelligence** Matters that defines the CNI's annual targets through the Intelligence Directive setting out the Centre's work.

Estructura del CNI[3]
CNI STRUCTURE[3]



(3) Estructura básica está definida en los Reales Decretos 436/2002, de 10 de mayo y 612/2006, de 19 de mayo

(3) BASIC CNI STRUCTURE DEFINED IN ROYAL DECREES 436/2002, DATED 10TH MAY AND 612/2006, 19TH MAY

Es función del CCN contribuir a la **mejora de la ciberseguridad** en España, articulando la respuesta y **gestión de los ciberincidentes** en torno al CCN-CERT, CERT Gubernamental/ nacional, con responsabilidad en los ciberataques sobre sistemas clasificados y sobre sistemas de la **Administración** y de **empresas** pertenecientes a **sectores** designados como **estratégicos**.

4.1 Secretario de Estado director

Corresponde al secretario de Estado director del Centro Nacional de Inteligencia impulsar la actuación del Centro y coordinar sus unidades para la consecución de los objetivos de inteligencia fijados por el Gobierno, asegurar la adecuación de las actividades del Centro a dichos objetivos y ostentar la representación de aquel.

Asimismo, le corresponde:

- Elaborar la propuesta de estructura orgánica del Centro Nacional de Inteligencia y nombrar y separar a los titulares de sus órganos directivos
- Aprobar el anteproyecto de presupuesto
- Mantener los procedimientos de relación necesarios para el desarrollo de las actividades específicas del Centro Nacional de Inteligencia, así como la celebración de los contratos y convenios con entidades públicas o privadas que sean precisos para el cumplimiento de sus fines.
- Mantener y desarrollar, dentro del ámbito de su competencia, la colaboración con los servicios de información de las Fuerzas y Cuerpos de Seguridad del Estado, y los órganos de la Administración civil y militar, relevantes para los objetivos de inteligencia
- Ejercer las facultades que otorgue la legislación vigente a los Presidentes y Directores de Organismos públicos y las que les atribuyan las disposiciones de desarrollo
- Desempeñar las funciones de Autoridad Nacional de Inteligencia y Contrainteligencia y la dirección del Centro Criptológico Nacional.
- Realizar cuantas otras funciones le sean atribuidas legal o reglamentariamente

It is the CCN`s role to help improve cybersecurity in Spain, organising how to tackle and manage cyber-incidents around the CCN-CERT, governmental/national CERT with responsability for cyber-attacks on classified systems and on Administration and business systems from designated strategic sectors.

4.1 SECRETARY OF STATE DIRECTOR

It is role of the Secretary of State Director from the National Intelligence Centre to drive the Centre's work and coordinate its units to attain the intelligence goals set by the Government, ensure that the Centre's activities are adapted to these targets and represent it. It also has to:

- Draw up the organic structure proposal for the National Intelligence Centre and appoint and separate the holders of these management bodies.
- Approve the preliminary budget project.
- Maintain the relationship procedures required for developing the National Intelligence Centre's specific activities and hold the contracts and agreements with public and private entities that are required to meet its purpose.
- Within the field of its competence, maintain and develop relevant collaboration with the State Law Enforcement Forces and Agencies information services and the civil and military Administration bodies concerning intelligence targets.
- Exercise the faculties awarded by the legislation in force to the Presidents and Directors of Public Organisations and any attributed to it by development arrangements.
- Deploy the role of National Intelligence and Counter-Intelligence Authority and the National Cryptologic Centre Board.
- Carry out as many functions as are attributed to it legally or in due form.

4.2 Ámbito de actuación y funciones del CCN

El ámbito de actuación del Centro Criptológico Nacional comprende la seguridad de los sistemas de las tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, que normativamente requiere protección, y que incluyen medios de cifra. De igual modo, vela por la seguridad de los sistemas de las tecnologías de la información que procesan, almacenan o transmiten **información clasificada**.

Las funciones asignadas al CCN son:

- Elaborar y difundir **normas, instrucciones, guías y recomendaciones** para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.
- **Formar** al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.
- Constituir el **Organismo de Certificación** del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito.
- **Valorar y acreditar** la capacidad de los **productos de cifra** y de los **sistemas** de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.
- Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas antes mencionados.
- Velar por el **cumplimiento de la normativa** relativa a la protección de la información clasificada en su ámbito de competencia.
- Contribuir a la **mejora de la ciberseguridad** en España, articulando la respuesta y **gestión de los ciberincidentes** en torno al CCN-CERT, CERT Gubernamental/nacional, con responsabilidad en los ciberataques sobre sistemas clasificados y sobre sistemas de la **Administración** y de **empresas** pertenecientes a **sectores** designados como **estratégicos**. Así en el año 2012, se encargó al CCN la elaboración de un borrador de la **Estrategia Española en Ciberseguridad, pendiente de aprobación**.
- Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

Para el desarrollo de estas funciones, el CCN debe establecer la coordinación oportuna con las comisiones nacionales a las que las leyes atribuyan responsabilidades en el ámbito de los sistemas de las tecnologías de la información.

4.2 CCN SPHERE OF ACTIVITY AND FUNCTIONS

The National Cryptologic Centre's sphere of activity includes security for Administration IT systems that process, store or send out information in electronic format that, according to the standard, requires protection and that involves encryption devices. In the same way, it monitors security for IT systems that process, store or send out classified information.

The functions assigned to the CCN are:

- Drawing up and disseminating standards, instructions, guides and recommendations to guarantee security for the Administration's information and communication technology systems.
- **Training** Administration staff specialising in the sphere of security for information and communication technology systems.
- Setting up the **Certification Body** for the National Evaluation Framework and certification of information technology security, to be applied to products and systems in its field.
- **Assessing and accrediting** the capacity of encryption products and information technology systems that include encryption devices to process, store or send out information securely.
- Coordinating promotion, development, obtaining, purchasing and operating plus the use of security technology for the aforementioned systems.
- **Making sure that standards** are met relating to protecting classified information in its field of competence.
- Helping to **improve cybersecurity in Spain,** organising how to tackle and manage cyberincidents around the CCN-CERT, governmental/national CERT with responsibility for cyber-attacks on classified systems and on Administration and business systems from designated strategic sectors. So, in 2012, the CCN was commissioned to draw up a rough draft of the Spanish Cybersecurity Strategy, pending approval.
- Establishing the necessary relationships and signing relevant agreements with similar organisations from other countries to develop the aforementioned functions.

In order to develop these functions further, the CCN should appropriately coordinate national commissions that have been legally allocated responsibilities in the field of information technology systems.

4.3 Adaptación a las necesidades

Desde su creación en el año 2002, el Centro Criptológico Nacional ha ido adecuándose e intentando anticiparse a una realidad cambiante, en donde las ciberamenazas se incrementan día a día, varían (en función de la motivación de los atacantes o sus objetivos), se modifican los métodos de ataque, aparecen nuevas vulnerabilidades o se renuevan los dispositivos de los usuarios, los servicios ofrecidos a través de Internet o la tecnología empleada.

Así, la creación en el año 2006 de la **Capacidad de Respuesta a Incidentes** (CCN-CERT) -y sus múltiples servicios orientados a una defensa preventiva frente a los ciberataques a las Administraciones Públicas y empresas estratégicas- y del **Organismo de Certificación** (OC) en 2007, es la respuesta más importante en los últimos años al desafío planteado por la evolución de las amenazas, las cuales cobran cada vez más relevancia y alcanzan una mayor repercusión en todas las capas de la sociedad. De dichas respuestas se hablará en las siguientes páginas de este informe.

4.3 ADAPTING FOR THE NEEDS

Since it was set up in 2002, the National Cryptologic Centre has been adapting and, as far as possible, getting one step ahead of a changing reality, where cyber threats are increasing on a daily basis and constantly varying (depending on the perpetrators' intentions or their targets), attack methods change, new vulnerabilities emerge or there is continual renewal of user devices, services offered over the Internet or the technology used.

Setting up the Incident Response Capability (CCN-CERT) in 2006 plus its multiple services aiming to provide a preventive defence against cyber-attacks on Public Administrations and strategic companies and the Certification Body (OC) in 2007 have been the most important responses over the last few years to the challenge presented by evolving risks, becoming more significant and making a greater impact on all layers of society. These responses will be mentioned over the next few pages of this report.

4.3.1 Guías e informes CCN, un marco de referencia en ciberseguridad

Dentro de esta actualización constante, y en virtud de las funciones asignadas al CCN, en los últimos doce años se han ido elaborando **normas, instrucciones, guías y recomendaciones** para mejorar el grado de ciberseguridad en España.

A finales del año 2012 existían **197 documentos** enmarcados en la **serie CCN-STIC**, con normas, procedimientos y directrices técnicas para optimizar la seguridad de las tecnologías de la información en nuestro país. De ellas, 73 se han elaborado o actualizado en los dos últimos años y abarcan todo tipo de temática, siendo algunas de difusión limitada para el personal de las Administraciones Públicas y empresas estratégicas, o de difusión abierta para todos los usuarios que accedan al portal del CCN-CERT (www.ccn-cert.cni.es).

Entre estas se encuentran la **serie CCN-STIC 800**, elaboradas en colaboración con el Ministerio de Hacienda y Administraciones Públicas, de desarrollo del Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad**.

También son públicas las Guías de la Herramienta **PILAR** (Procedimiento Informático Lógico para el Análisis de Riesgos), (versión 5.2 de 2012) y las destinadas a la seguridad de los dispositivos móviles (Windows Mobile, iPhone, Android o iPad).

Las series CCN-STIC (cuyo listado aparece en este mismo Informe) son actualizadas periódicamente y enviadas a más de 300 organismos diferentes de la Administración además de publicarse en la parte privada del portal del CCN-CERT.

A finales de 2012 había **197 Guías CCN-STIC**, 73 de las cuales habían sido elaboradas o actualizadas en los dos últimos años.

By the end of 2012 197 CCN-STIC guides had been published, 73 of which had been drawn up or updated over the last two years

4.3.1 CCN GUIDES AND REPORTS, A CYBERSECURITY REFERENCE FRAMEWORK

Within this constant updating and by virtue of functions assigned to the CCN, over the last twelve years rules, instructions, guides and recommendations have been drawn up to improve the extent of cybersecurity in Spain. Consequently, by the end of 2012 there were 197 documents within the CCN-STIC series, featuring rules, procedures and technical directives to optimise information technology security in our country. Of these, 73 have been drawn up or updated over the last two years and cover a wide range of topic areas. Some are limited to distribution among staff from public administrations and strategic companies and some are open to all CCN-CERT website users (www.ccn-cert.cni.es). These documents include the CCN-STIC 800 series, drawn up in collaboration with the Ministry of Inland Revenue and Public Administrations, developing Royal Decree 3/2010, dated 8th January, regulating the National Security Framework.

The PILAR Tool Guides (version 5.2 from 2012) are also public plus guides intended for mobile device security (Windows Mobile, iPhone, Android or iPad).

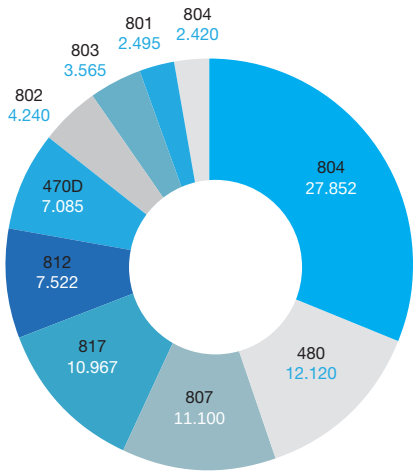
The entire CCN-STIC series (list featured in this report) is updated periodically and sent to over 300 different Administration organisations, whilst also published privately on the CCN-CERT website.
In addition to this series, the National Cryptologic Centre has drawn up and sent out technical reports over these last two years, within the study requested by the Permanent Commission for Electronic Administration (CP-CSAE) that governs it. These reports have led to security audits being carried out on internet services run by the following organisations:

- ENS implantation Studies.
- Ministry of Inland Revenue and Public Administrations.
- Royal Family (2012).
- Ministry of Employment and Social Security 2012 (2 audits).
- Government President`s Office 2012.
- Ministry of Economy and Competition 2012.
- Ministry of the Economy and Inland Revenue (Cadastre Service) 2011.
- State Tax Office: income tax and VAT 2011 and

Junto a esta serie, el Centro Criptológico Nacional ha continuado elaborando y difundiendo informes técnicos, requeridos por la **Comisión Permanente de Administración Electrónica (CP-CSAE)** a la que pertenece.

Estos informes han versado sobre análisis forense, ingeniería inversa de código dañino y sobre auditorías de seguridad realizadas a los servicios Web de los siguientes organismos:

- Estudios de implantación del ENS.
- MINHAP (Ministerio de Hacienda y Administraciones Públicas).
- Casa Real. 2012.
- Ministerio de Empleo y Seguridad Social. 2012 (2 auditorías)
- Presidencia de Gobierno. 2012.
- Ministerio de Economía y Competitividad. 2012.



Top 10 guías descargadas del portal CCN-CERT en 2012
TOP 10 DOWNLOADS GUIDES OF THE PORTAL CCN-CERT, 2012

- Spanish Ministry of Civil Works. 2012.
- President's Office 2012 (3 audits).
- National Statistics Institute 2011 and 2012 (2 audits).
- Nuclear Security Council 2012.
- Secretary of State for Public Administration). 2012 (3 audits).
- Social Security (Work record certificate and pensions services). 2011.
- Unemployment Benefit). 2011.
- Driving licence points enquiry and traffic fine management service). 2011.
- Ministry of Industry, Energy and Tourism (CIRCE service). 2011.

- Ministerio de Economía y Hacienda (Servicio del Catastro). 2011.
- Agencia Estatal de Administración Tributaria: servicios de IRPF e IVA. 2011 y 2012.
- Ministerio de Educación Cultura y Deportes. 2011 y 2012 (2 auditorías).
- Ministerio de Fomento. 2012.
- Ministerio de Presidencia. 2012 (3 auditorías).
- Instituto Nacional de Estadística. 2011 y 2012 (2 auditorías).
- Consejo de Seguridad Nuclear. 2012.
- MINHAP-SEAP (Secretaria de Estado de la Administración Pública). 2012 (3 auditorías).
- Seguridad Social (Servicios de certificado de vida laboral y pensiones). 2011.
- SEPE (Servicio de Prestación por Desempleo). 2011.
- DGT (Servicio de Consulta de puntos y gestión de multas). 2011.
- Ministerio de Industria, Energía y Turismo (servicio CIRCE). 2011.

Top 10 guías descargadas del portal CCN-CERT en 2012
TOP 10 DOWNLOADS GUIDES OF THE PORTAL CCN-CERT, 2012

	Guía GUIDE	Nº descargas Nº DOWNLOADS
804	Medidas_de_implantacion_del_ENS-20111026.pdf	**27.852**
480	Seguridad_sistemas_SCADA-mar10.pdf	**12.120**
807	Criptologia_de_empleo_ENS-sep11.pdf	**11.100**
817	Gestion_incidentes_seguridad-ago12.pdf	**10.967**
812	Entornos-y-aplicaciones-web_20111026.pdf	**7.522**
470D	Manual_de_usuario_PILAR_5.1-may11.pdf	**7.085**
802	Auditoria_ENS-jun10.pdf	**4.240**
803	ENS-valoracion_ene-11.pdf	**3.565**
801	ENS-responsabilidades_feb-11.pdf	**2.495**
804	ENS-medidas_2010-07-23.pdf	**2.420**

Listado de Guías CCN-STIC 2012
LIST OF CCN-STIC GUIDES 2012

Serie 000: Políticas
SERIE 000: POLICIES

001	Seguridad de las TIC en la Administración ICT SECURITY IN THE PUBLIC ADMINISTRATION	MAR 11
002	Coordinación Criptológica CRYPTOLOGY COORDINATION	MAR 11
003*	Uso de Cifradores Certificados USE OF CERTIFIED CIPHER EQUIPMENT	DIC 06

Serie 100: Procedimientos
SERIE 100: PROCEDURE

101	Procedimiento de Acreditación Nacional NATIONAL ACCREDITATION PROCEDURE	MAR 05
103*	Catálogo de Productos Certificados CERTIFIED PRODUCTS CATALOGUE	ABR 13
104	Catálogo de Productos con clasificación Zoning ZONING PRODUCTS CLASIFICATION CATALOGUE	ENE 13
150**	Evaluación y Clasificación TEMPEST de Cifradores con Certificación Criptológica TEMPEST EVALUATION AND CLASSIFICATION OF EQUIPMENT WITH CRYPTOLOGY CERTIFICATION	DIC 06
151*	Evaluación y Clasificación TEMPEST de Equipos TEMPEST EVALUATION AND CLASSIFICATION OF EQUIPMENT	DIC 06
152*	Evaluación y Clasificación ZONING de Locales FACILITY ZONING, EVALUATION AND CLASSIFICATION	DIC 06
153	Evaluación y Clasificación de Armarios Apantallados EVALUATION AND CLASSIFICATION OF SHIELDED CABINETS	FEB 10
154*	Medidas de protección TEMPEST para instalaciones PROTECTION TEMPEST MEASURES FOR FACILITIES	NOV 11

Serie 200: Normas
SERIE 200: STANDARDS

201	Estructura de Seguridad SECURITY ORGANIZATION	ENE 09
202	Estructura y Contenido DRS SSRS. STRUCTURE AND CONTENT	MAR 05
203	Estructura y Contenido POS SECOPS. STRUCTURE AND CONTENT	MAR 05
204	CO-DRES-POS Pequeñas Redes CONCEPT OF OPERATION, SSRS AND SECOPS FOR LITTLE NETWORKS	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 SAFETY STANDARD EMANATIONS	JUL 12

Serie 300: Instrucciones Técnicas
SERIE 300: TECHNICAL INSTRUCTIONS

301*	Requisitos STIC IT SECURITY REQUIREMENTS	DIC 07
302*	Interconexión de CIS CIS SYSTEMS INTERCONNECTION	JUL 12
303*	Inspección STIC IT SECURITY INSPECTION	ENE 09
304	Baja y Destrucción de Material Criptológico DESTRUCTING AND TAKING CRYPTOLOGY MATERIAL OUT OF CIRCULATION	MAR 11
305*	Destrucción y Sanitización de Soportes MEDIA SANITIZATION AND DESTRUCTION	
307*	Seguridad en Sistemas Multifunción SECURITY IN MULTIFUNCTION SYSTEMS	ENE 09

Serie 400: Guías Generales
SERIE 400: GENERAL GUIDES

400	Manual STIC ICT SECURITY MANUAL	MAY 13
401	Glosario / Abreviaturas GLOSSARY / ABBREVIATIONS	MAY 13
402	Organización y Gestión STIC ICT 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 WIRELESS SECURITY	DIC 06
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 equipo de cifra SECURITY LABELS	MAY 13
410	Análisis de 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 de Seguridad en 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 VPN,s 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)	JUL 13
430	Herramientas de Seguridad SECURITY TOOLS	ENE 09
431	Herramientas de Análisis de Vulnerabilidades TOOLS FOR VULNERABILITIES ASSESSMENT	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

* Difusión limitada
LIMITED DIFUSSION

** Confidencial
CONFIDENTIAL

Cumple con el ENS
COMPLIES WITH ENS

Adaptables al ENS
ADAPTED TO ENS

Pendientes de publicar
PENDING PUBLICATION

437	Herramientas de Cifrado Software ENCRYPTED SOFTWARE TOOLS	DIC 07
438	Esteganografía STEGANOGRAPHIA	SEP 11
440	Mensajería Instantánea INSTANT MESSAGING	DIC 07
441	Configuración Segura de VMWare SECURE CONFIGURATION OF VMWARE	ENE 10
442	Seguridad en VMWare ESXi VMWARE ESXI SECURITY	
443	RFID RFID	ENE 09
444	Seguridad en WiMAX WIMAX SECURITY	MAR 11
445A	Curso de Especialidades Criptológicas (correspondencia) – Probabilidad CRYPTOLOGY SPECIALISED COURSE (CEC) – PROBABILITY	JUL 10
445B	Curso de Especialidades Criptológicas (correspondencia) – Principios digitales CSC- DIGITAL PRINCIPLES	JUL 10
445C	Curso de Especialidades Criptológicas (correspondencia) – Teoría de números 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	MAR 11
452	Seguridad en Windows Mobile 6.5 SECURITY ON WINDOWS MOBILE 6.5	MAR 11
453	Seguridad en Android 2.1 SECURITY IN ANDROID	MAY 13
454	Seguridad en iPad SECURITY IN IPAD	MAY 13
455	Seguridad en iPhone SECURITY IN IPHONE	MAY 13
456	Seguridad en entornos BES BES SECURITY ENVIROMENTS	
457	Seguridad en MDM MDM SECURITY ENVIROMENTS	
470A	Manual de la Herramienta de Análisis de Riesgos PILAR 4.1 RISK ANALYSIS TOOL MANUAL PILAR 4.1	DIC 07
470B	Manual de la Herramienta de Análisis de Riesgos PILAR 4.3 RISK ANALYSIS TOOL MANUAL PILAR 4.3	DIC 08
470C	Manual de la Herramienta de Análisis de Riesgos PILAR 4.4 RISK ANALYSIS TOOL MANUAL PILAR 4.4	FEB 10
470D	Manual de la Herramienta de Análisis de Riesgos PILAR 5.1 RISK ANALYSIS TOOL MANUAL PILAR 5.1	MAY 11
470E1	Manual de la Herramienta de Análisis de Riesgos PILAR 5.2 RISK ANALYSIS TOOL MANUAL PILAR 5.2	JUL 12
470E2	Manual de la Herramienta de Análisis de Riesgos PILAR 5.2. Análisis del Impacto y Continuidad del Negocio. RISK ANALYSIS TOOL MANUAL PILAR 5.2 IMPACT ANALYSIS AND BUSINESS CONTINUITY	JUL 12
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
472A	Manual de la Herramienta de Análisis de Riesgos PILAR BASIC 4.3 RISK ANALYSIS TOOL MANUAL PILAR BASIC V.4.3	DIC 08
472B	Manual de la Herramienta de Análisis de Riesgos PILAR BASIC 4.4 RISK ANALYSIS TOOL MANUAL PILAR BASIC V.4.4	FEB 10
472C	Manual de la Herramienta de Análisis de Riesgos PILAR BASIC 5.2 RISK ANALYSIS TOOL MANUAL PILAR BASIC 5.2	JUL 12
473A	Manual de la Herramienta de Análisis de Riesgos µPILAR RISK ANALYSIS TOOL MANUAL (MPILAR)	MAR 11
473B	Manual de la Herramienta de Análisis de Riesgos µPILAR 5.2 RISK ANALYSIS TOOL MANUAL MPILAR 5.2	JUL 12
480	Seguridad en Sistemas SCADA SECURITY ON SCADA SYSTEMS	MAR 10
480A	Seguridad en Sistemas SCADA – Guía de Buenas SCADA- BEST PRACTICES	FEB 10
480B	Seguridad en Sistemas SCADA – Comprender el Riesgo del Negocio SCADA- UNDERSTANDING BUSINESS RISKS	MAR 10
480C	Seguridad en Sistemas SCADA – Implementar una Arquitectura Segura SCADA- IMPLEMENTING SECURE ARCHITECTURE	MAR 10
480D	Seguridad en Sistemas SCADA – Establecer Capacidades de Respuesta SCADA- ESTABLISHING RESPONSE CAPABILITIES	MAR 10
480E	Seguridad en Sistemas SCADA – Mejorar la Concienciación y las Habilidades SCADA IMPROVING AWARENESS AND CAPABILITIES	ENE 10
480F	Seguridad en Sistemas SCADA – Gestionar el Riesgo de Terceros SCADA- DEALING WITH RISKS DERIVED FROM THIRD PARTIES	MAR 09
480G	Seguridad en Sistemas SCADA – Afrontar Proyectos SCADA- CONFRONT PROJECTS	MAR 09
480H	Seguridad en Sistemas SCADA – 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 de Parámetros de Rendimiento en Dispositivos Biométricos EVALUATION OF PERFORMANCE PARAMETERS IN BIOMETRIC DEVICES	MAR 11

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 en Windows XP SP2 (cliente independiente) WINDOWS XP SP2 SECURITY (INDEPENDENT CLIENT)	DIC 07
502	Seguridad en 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	Seguridad en Windows 2003 Server (servidor independiente WINDOWS 2003 SERVER SECURITY (INDEPENDENT SERVER)	DIC 07
504	Seguridad en Internet Information Server INTERNET INFORMATION SERVER SECURITY	OCT 05
505	Seguridad en Bases de Datos SQL 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 en Windows 2003 Server. Servidor de Ficheros SECURITY ON WINDOWS 2003 SERVER. FILE SERVER	DIC 07
510	Seguridad en Windows 2003 Server. Servidor de Impresión SECURITY ON WINDOWS 2003 SERVER. PRINTING SERVER	ENE 09
512	Gestión de Actualizaciones de Seguridad en Sistemas Windows | Windows SECURITY UPDATES MANAGEMENT	DIC 05
517A	Seguridad en Windows Vista (cliente en dominio) WINDOWS VISTA SECURITY (CLIENT WITHIN A DOMAIN)	ENE 10
517B	Seguridad en Windows Vista (cliente independiente) WINDOWS VISTA SECURITY (INDEPENDENT CLIENT)	ENE 09
519A	Configuración Segura del Internet Explorer 7 y Outlook en Windows XP SECURE CONFIGURATION OF INTERNETEXPLORER 7 AND OUTLOOK IN WINDOWS XP	ENE 10
521A	Seguridad en Windows 2008 Server (controlador de dominio) WINDOWS 2008 SERVER SECURITY (DOMAIN CONTROLLER)	AGO 10
521B	Seguridad en Windows 2008 Server (servidor independiente) WINDOWS 2008 SERVER SECURITY (INDEPENDENT SERVER)	AGO 10
521C	Seguridad en Windows 2008 Server Core (controlador de dominio) WINDOWS 2008 SERVER CORE SECURITY (DOMAIN CONTROLLER)	
521D	Seguridad en Windows 2008 Server Core (servidor independiente) WINDOWS 2008 SERVER CORE SECURITY (INDEPENDENT SERVER)	JUN 13
522	Seguridad en Windows 7 (cliente en dominio) WINDOWS 7 SECURITY (DOMAIN CLIENT)	JUN 11
522B	Seguridad en Windows 7 (cliente independiente) WINDOWS 7 SECURITY (INDEPENDENT CLIENT)	NOV 10
523	Seguridad en Windows 2008 Server. Servidor de Ficheros. WINDOWS 2008 SERVER SECURITY. FILE SERVER	FEB 12
524	Seguridad en Bases de Datos SQL Server 2008 DB SQL SERVER SECURITY	
525	Seguridad en Microsoft Exchange Server 2007 sobre Windows 2003 Server MICROSOFT EXCHANGE SERVER 2007 ON WINDOWS 2003 SECURITY	JUL 13
526	Seguridad en Microsoft Exchange Server 2007 sobre Windows 2008 Server MICROSOFT EXCHANGE SERVER 2007 ON WINDOWS 2008 SECURITY	
527	Failover Clustering para Windows 2008 Server R2 FAILOVER CLUSTERING PARA WINDOWS 2008 SERVER R2	
530	Seguridad en Microsoft Office 2010 SEGURIDAD EN MICROSOFT OFFICE 2010	JUL 13
531	Seguridad en Sharepoint Server 2007 SHAREPOINT SERVER SECURITY 2007	DIC 12

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
610	Seguridad en Red Hat Linux 7 RED HAT LINUX 7 SECURITY	DIC 06
611	Seguridad en Suse Linux SUSE LINUX SECURITY	DIC 06
612	Seguridad en Debian DEBIAN SECURITY	DIC 06
613	Seguridad en Entornos basados en Debian SECURITY ON DEBIAN-BASED ENVIRONMENTS	
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. SUN-SOLARIS 10 SECURITY FOR ORACLE 9.2	DIC 06
625	Seguridad en Sun Solaris 10 para 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
632	Seguridad en Base de Datos Oracle 11g sobre Suse Linux Enterprise Server 11 SECURITY FOR DB ORACLE 11G ON SUSE LINUX ENTERPRISE SERVER	
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 Equipos de Comunicaciones. ROUTERS CISCO | SECURITY FOR COMMUNICATION EQUIPMENT. ROUTERS CISCO	DIC 06
642	Seguridad en Equipos de Comunicaciones. Switches Enterasys SECURITY FOR COMMUNICATION EQUIPMENT. SWITCHES ENTERASYS	DIC 06
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

* Difusión limitada
LIMITED DIFUSSION

** Confidencial
CONFIDENTIAL

Cumple con el ENS
COMPLIES WITH ENS

Adaptables al ENS
ADAPTED TO ENS

Pendientes de publicar
PENDING PUBLICATION

655	Guía de Securización para Sun Solaris 9 con Oracle 10 SECURITY GUIDE FOR SUN SOLARIS 9 WITH ORACLE 10	DIC 07
656	Guía de Securización para Sun Solaris 9 con Oracle 10 y VCS 4.1 | Security GUIDE FOR SUN SOLARIS 9 WITH ORACLE 10 AND VCS 4.1	DIC 07
660	Seguridad en Proxies PROXIES SECURITY	FEB 11
661	Seguridad en Firewalls de Aplicación APPLICATION FIREWALLS SECURITY	MAR 11
662	Seguridad en Apache Traffic Server SECURITY OF APACHE TRAFFIC SERVER	NOV 12
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	Guía de Securización de Oracle Application Server 10gR2 para Red Hat 3 y 4 SECURITY IN ORACLE APPLICATION SERVER 10GR2 FOR RED HAT 3 Y 4	DIC 07
692	Guía de Securización de Oracle Application Server 10gR2 para Solaris 9 y 10 SECURITY IN ORACLE APPLICATION SERVER 10GR2 FOR SOLARIS 9 Y 10	DIC 07
693	Guía de Securización de 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	Categorización de los Sistemas en el ENS SYSTEMS EVALUATION IN THE NATIONAL SECURITY FRAMEWORK	ENE 11
804	Implementación de Medias en el ENS (BORRADOR) IMPLEMENTATION MEASURES IN THE NATIONAL SECURITY FRAMEWORK	MAR 13
805	Modelo de Política de Seguridad SECURITY POLICY IN THE NATIONAL SECURITY FRAMEWORK	SEP 11
806	Modelo de Plan de Adecuación al ENS ADAPTATION PLAN IN THE NATIONAL SECURITY FRAMEWORK	ENE 11
807	Criptología de Empleo en el ENS (BORRADOR) ENCRYPTION IN THE NATIONAL SECURITY FRAMEWORK	NOV 12
808	Verificación del Cumplimiento de las Medidas en el ENS (BORRADOR) VERIFICATION OF COMPLIANCE WITH MEASURES ESTABLISHED BY THE NATIONAL SECURITY FRAMEWORK	SEP 11
810	Guía de Creación de CERT,s CERTS CONSTRUCTION GUIDE	SEP 11
811	Interconexión en el ENS ENS INTERCONNECTION	NOV 12
812	Seguridad en Servicios Web en el ENS SECURITY IN ENS WEB SERVICES	OCT 11
813	Componentes Certificados en el ENS ENS COMPONENTS CERTIFICATES	FEB 12
814	Seguridad en Servicio de Correo en el ENS (BORRADOR) SECURITY IN ENS MAIL	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 Incidentes de Seguridad en el ENS INCIDENT MANAGEMENT ENS	AGO 12
818	Herramientas de seguridad en el ENS(BORRADOR) SAFETY TOOLS NATIONAL SECURITY FRAMEWORK	OCT 12
819	Guía de contratos en el marco del ENS ENS FRAMEWORK CONTRACTS GUIDE	
820	Guía de protección contra Denegación de Servicio DDOS PROTECTION GUIDE	JUN 13
821	Ejemplos de Normas de Seguridad EXAMPLES OF SAFETY STANDARDS	ABR 12
822	Ejemplos de Procedimientos de Seguridad EXAMPLES OF SECURITY PROCEDURES	OCT 12
823	Requisitos de seguridad en entornos CLOUD SAFETY REQUIREMENTS CLOUD ENVIRONMENTS	OCT 12
824	Informe del estado de seguridad SECURITY STATUS REPORT	NOV 12

Serie 900: Informes técnicos

SERIE 900: TECHNICAL REPORTS

903	Configuración Segura de HP-IPAQ HP-IPAQ SECURE CONFIGURATION	DIC 05
911A*	Ciclo de un APT APT GENERAL RECOMENDATIONS	JUL 13
911B*	Recomendaciones generales ante un APT APT GENERAL RECOMENDATIONS	JUL 13
912	Procedimiento de investigación de un código dañino MALWARE INVESTIGATION PROCEDURE	JUN 13
920	Análisis de malware con Cuckoo Sandbox ANÁLISIS DE MALWARE CON CUCKOO SANDBOX	
951	Recomendaciones de Empleo de la Herramienta Ethereal/Wireshark RECOMMENDATIONS FOR USING ETHEREAL/ WIRESHARK TOOL	DIC 06
952	Recomendaciones de 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 USAGE RECOMMENDATIONS FOR GNUPG TOOL	DIC 07
956	Entornos Virtuales VIRTUAL ENVIRONMENTS	DIC 07
957	Recomendaciones de empleo de TrueCrypt TRUECRYPT RECOMENDATIONS	MAR 13
958*	Procedimiento de empleo Crypto Token USB CRYPTO TOKEN USB EMPLOYMENT PROCEDURE	ENE 13
970**	Interconexión de Sistemas Mediante Cifradores IP. Redes Públicas USE OF IP CYPHERS IN PUBLIC NETWORKS	MAR 10

4.3.2 Herramienta PILAR de Análisis de Riesgos

Dentro de la función del Centro Criptológico Nacional de coordinar la promoción y desarrollo de herramientas que garanticen la seguridad de los sistemas, se ha venido desarrollando y financiando parcialmente la **herramienta PILAR** (Procedimiento Informático Lógico para el Análisis de Riesgos) cuya última **versión, la 5.2,** se presentó en el año 2012.

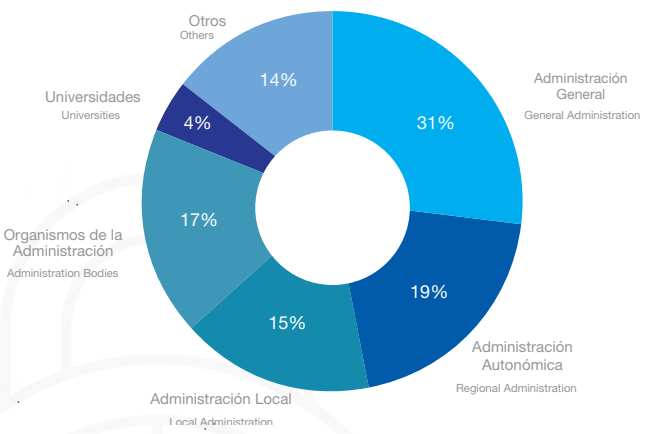
Esta herramienta sigue el modelo MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) que también ha ido actualizándose en los últimos años. Su última versión, **MAGERIT v3**, elaborada por el Consejo Superior de Administración Electrónica (CSAE), fue publicada en octubre de 2012 en el portal del CCN-CERT y se está extendiendo para soportar los mecanismos de conocimiento anual del estado de seguridad de las Administraciones Públicas requeridos por el art, 35 del RD 3/2010 (Esquema Nacional de Seguridad), es decir, los indicadores del estado de la seguridad.

El CCN ha traducido la herramienta a diferentes idiomas y ha ido creando herramientas de apoyo como la herramienta **μPILAR** (una versión de PILAR reducida, destinada a la realización de análisis de riesgos muy rápidos). Al mismo tiempo la ha ido adaptando a otras herramientas y, en 2011, construyó una biblioteca para la OTAN y, en 2012, desarrolló los módulos de cumplimiento del Esquema Nacional de Seguridad.

PILAR es en la actualidad una herramienta indispensable para los organismos de las Administraciones Públicas que la utilizan, así como para otras organizaciones internacionales como la Unión Europea y la OTAN. Prueba de ello son los casi 69.000 accesos que tuvo a través del portal del CCN-CERT en 2012.

PILAR es en la actualidad una herramienta indispensable para los organismos de las Administraciones Públicas que la utilizan (así como para otras organizaciones internacionales como la Unión Europea y la OTAN). Prueba de ello son los casi **69.000 accesos** que tuvo a través del portal del CCN-CERT en 2012

PILAR is currently an essential tool for the Public Administration organisations that use it (and for other international organisations such as the European Union and NATO). This is demonstrated by 69.000 hits in 2012 by the website CCN-CERT



Distribución de usuarios de la Herramienta PILAR (2005-2012)
PILAR TOOL USER DISTRIBUTION (2005-2012)

4.3.2 PILAR RISK ANALYSIS TOOL

The PILAR tool (Logical Computer Procedure for Risk Analysis) has been developed and partially financed within the National Cryptologic Centre's role to coordinate promoting and developing tools that guarantee system security. Its latest version, 5.2, was presented in 2012.

This tool follows the MAGERIT system model (Information Systems Risk Analysis and Management Methodology) that has also been updated over the last few years. Its latest version, MAGERIT v3, drawn up by the Higher Council for Electronic Administration (CSAE), was published in October 2012 on the CCN-CERT website.

The CCN has translated the tool into many different languages and has been creating support tools such as the μPILAR tool (a lighter version of PILAR, intended for very fast risk analysis). At the same time, it has been adapted to other tools: in 2011, it built a library for NATO and in 2012, it developed National Security Framework compliance modules.

PILAR has become an essential tool for the public administration organisations that use it (and for other international organisations such as the European Union and NATO). This is demonstrated by more than 69,000 hits on its public version in 2012.

4.3.3 Formación, una apuesta por la actualización

Disponer de personal cualificado en todos los niveles de la Administración (dirección, gestión e implantación) es un aspecto fundamental para proteger los sistemas de las ciberamenazas. De ahí que una de las funciones principales del Centro Criptológico Nacional a lo largo de sus casi doce años de historia sea formar al personal de la Administración a través de un amplio programa, en el que se incluyen los Cursos STIC (presenciales, a distancia y on-line), jornadas de sensibilización, participación en ponencias y mesas redondas, etc.

A las tradicionales **Jornadas STIC CCN-CERT** (de las que se hablará en el apartado del CERT Gubernamental) y del **Sistema de Alerta Temprana de Internet** (SAT-INET), se les une la impartición de jornadas de sensibilización y concienciación sobre ciberseguridad y sobre el Esquema Nacional de Seguridad en muy diversos organismos: Secretaría de la Vicepresidencia, Casa Real, Cuartel General del Ejército, Ministerio de la Presidencia, altos cargos de la Guardia Civil, etc. Asimismo, durante 2011 y 2012, se ha participado en más de 110 mesas redondas o jornadas como las desarrolladas por el Ministerio de Defensa (Jornadas SIC), Fundación Círculo, EMACOT, Jornadas SEGINFOSIT, CNIS, Foro ABUSES, ISMS Fórum, Jornadas PSCIC Isdefe-CNPIC, Cursos de verano MADOC, Securmática, etc).

Evolución de la oferta formativa del CCN
HOW TRAINING BY THE CCN HAS EVOLVED

	2008	2009	2010	2011	2012	Total
Alumnos STUDENTS	380	450	510	500	500	2.340
Cursos presenciales CLASSROOM COURSES	17	18	17	14	14	80
Horas lectivas CLASS HOURS	1.200	1.400	1.200	900	900	5.600
Cursos *online* ONLINE COURSES	-	1	3	5	6	15
Jornadas de sensibilización AWARENESS-RAISING SESSIONS	2	4	3	6	7	22
Participación en mesas / jornadas PARTICIPATION IN ROUND TABLES/SESSIONS	8	10	15	51	64	148

4.3.3 TRAINING, BACKING UPGRADES

Having qualified personnel at all Administration levels (executives, management and implementation) is fundamental to protect systems from cyber threats. This means that one of the National Cryptologic Centre's main functions over the twelve years and more that it has been running is to train Administration staff through a broad programme, including STIC (ICT security) Courses (classroom, distance learning and on-line), awareness-raising sessions, participation in papers and round table workshops, etc.

As well as the traditional STIC CCN-CERT Workshops (mentioned below in the Governmental CERT section) and the Internet Early Warning System (SAT-INET), workshops are also given on awareness-raising concerning cybersecurity and the National Security Framework in very different organisations: Vice-President's Secretariat, Royal Family, Air Force Headquarters, Ministry of the President's Office, Civil Guard executives, etc. In addition, during 2011 and 2012, it participated in over 50 round table discussions or sessions run by entities such as the Ministry of Defence (Information Security Workshops in Defence SIC), Fundación Círculo, EMACOT, SEGINFOSIT Workshops, CNIS, ABUSES Forum, ISMS Forum, PSCIC Workshops, Isdefe-CNPIC, MADOC Summer Courses, Securmática, etc.)

Cursos 2011 - 2012

Cursos Informativos y de Concienciación en Seguridad

- VII, VIII y IX Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) (Con fase *online*).
  Online: 30 horas / Presencial: 50 h. TOTAL: 80 h.

Cursos Básicos de Seguridad

- VI y VII Curso Básico STIC - Infraestructura de Red. 25 h.
- VI y VII Curso Básico STIC - Base de Datos. 25 h.

Cursos Específicos de Gestión de Seguridad

- IV Curso Common Criteria. 25 h.
- VIII y IX Curso de Gestión STIC- Implantación del ENS
  Online: 30 horas / Presencial: 50 h. Total 80 h.
- XXIII Curso de Especialidades Criptológicas (Fase por correspondencia). A distancia: 125 horas / Presencial: 75 h. Total: 200 h.

Cursos de Especialización en Seguridad

- VI y VII Curso STIC – Seguridad en Redes Inalámbricas. 25 h.
- I y II Curso STIC – Seguridad en Dispositivos Móviles (Nuevo en 2012). 25 h.
- III y IV Curso STIC – Seguridad en Aplicaciones Web. 25 h.
- VII y VIII Curso STIC – Cortafuegos. 25 h.
- VII y VIII Curso STIC – Detección de Intrusos. 25 h.
- VIII y IX Curso Acreditación STIC - Entornos Windows. 25 h.
- IV y V Curso STIC – Búsqueda de Evidencias. 25 h.
- VI y VII Curso STIC – Inspecciones de Seguridad. 25 h.
- II y III Curso STIC – Herramienta PILAR.
  Online: 10 horas / Presencial: 25 h. TOTAL: 35 h.

NOTA: Los contenidos de los cursos están accesibles en la parte privada del portal del CCN-CERT (www.ccn-cert.cni.es)

2011 – 2012 COURSES

Security Information and Awareness Courses

- VII, VIII and IX Security Information and Communication Technologies Course (STIC) (blended learning)

Basic Security Courses

- VI and VII Basic STIC Course - Network Infrastructure
- VI and VII Basic STIC Course - Databases

Specific Courses on Security Management

- IV STIC Course – Common Criteria
- VIII and IX STIC Management Course. Application to ENS (blended learning)
- XXIII Cryptology Specialized Course (CEC) (blended learning)

Courses Specializing on Security

- VI and VII STIC Course - Wireless Network
- I and II STIC Course – Security in Mobile Devices (New in 2012)
- III and IV STIC Course – Security in Web Applications
- VII and VIII STIC Course – Firewall
- VII and VIII STIC Course - Intrusion Detection Systems
- VIII and IX Accreditation STIC Course - Windows Environments
- IV and V STIC Course – Search for Evidence and Integrity Control
- VI and VII STIC Course – Security Inspections
- II and III STIC Course – PILAR Tool (online)

NOTE: Course content is available in the private section of the CCN-CERT website (www.ccn-cert.cni.es)

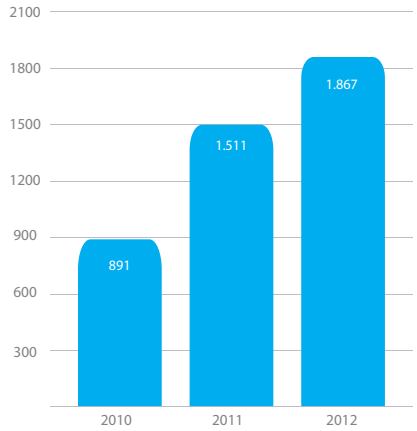
Cursos *online*

En estos dos últimos años, el Centro Criptológico Nacional ha ido ampliando su oferta formativa, adaptándose a las necesidades de muchos usuarios y facilitando, a través de un método de *e-learning*, algunos de sus cursos más demandados. De esta forma, a finales de 2012, estaban disponibles en el portal del CCN-CERT, los siguientes cursos:

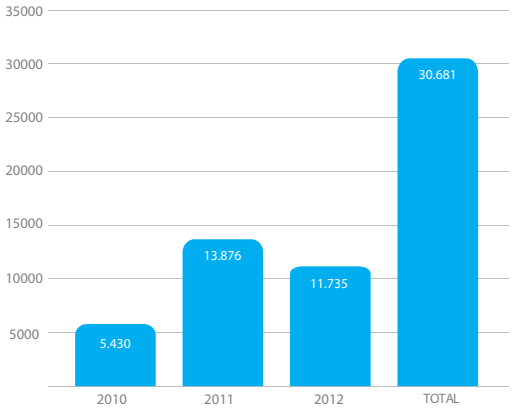
- Curso de Seguridad de las Tecnologías de la Información y las Comunicaciones STIC.
- Curso PILAR (Manejo de herramienta / Funciones más usadas).
- Curso básico de seguridad. Entorno Windows.
- Curso básico de seguridad. Entorno Linux.
- Curso del Esquema Nacional de Seguridad (acceso público).
- Curso de Análisis y Gestión de Riesgos de los Sistemas de Información (acceso público).
- Curso de Common Criteria.

En apenas tres años desde la puesta en funcionamiento del primero de los cursos, se ha conseguido un total de 1.887 alumnos y más de 30.000 accesos al apartado del portal web.

Nº DE ALUMNOS INSCRITOS A LOS CURSOS *ONLINE*
NUMBERS OF STUDENTS SIGNED UP



Nº DE ACCESOS A LOS CURSOS *ONLINE*
NUMBER OF HITS ON ONLINE COURSES



Evolución de los cursos on-line (www.ccn-cert.cni.es)
HOW ON-LINE COURSES HAVE EVOLVED (WWW.CCN-CERT.CNI.ES)

	2010	2011	2012	Total
Número de accesos a los cursos *online* NUMBER OF HITS ON ONLINE COURSES	**5.430**	**13.876**	**11.735**	**30.681**
Número de alumnos inscritos NUMBER OF STUDENTS SIGNED UP	**891**	**1.511**	**1.887**	**1.887**

ON-LINE COURSES

Over the last two years, the National Cryptologic Centre has been extending its training offer, incorporating many users' needs and providing access to some of its most sought-after courses through an e-learning method. In this way, at the end of 2012, the following courses were available on the CCN-CERT website:

- STIC Information and Communication Technology Security Course
- PILAR Course (Using the tool / Most used functions)
- Basic Security Course. Windows environment
- Basic Security Course. Linux environment
- National Security Framework Course (public access)
- Information System Risk Analysis and Management Course (public access)
- Common Criteria Course

In barely three years since the first courses were up and running, there have been a total of 1887 students and over 30,000 hits on the website section.

4.4 Esquema Nacional de Seguridad

El 30 de enero de 2014 concluye el plazo de 48 meses fijado por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica para la adecuación de los sistemas de las Administraciones Públicas a dicho Esquema. Este Real Decreto, publicado en el BOE el 29 de enero de 2010 y en cuyo desarrollo participó activamente el Centro Criptológico Nacional, se hacía necesario para establecer **aspectos y metodologías comunes** relativos a la seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, al objeto de crear las condiciones necesarias para la confianza en el uso de los citados medios electrónicos que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Con el fin de impulsar su desarrollo e implantación, el **secretario de Estado director del Centro Nacional de Inteligencia (CNI), Félix Sanz Roldán**, la **secretaria de Estado para la Función Pública** del Ministerio de Política Territorial y Administración Pública (hoy Ministerio de Hacienda y

Espacio del portal web del CCN-CERT destinado al ENS
CCN-CERT WEBSITE AREA INTENDED FOR THE NSF

4.4 NATIONAL SECURITY FRAMEWORK

29th January 2014 will be the second and final deadline set by Royal Decree 3/2010, dated 8th January, regulating the National Security Framework for adapting Public Administration systems to this Framework. This Royal Decree, published in the State Gazette on 29th January 2010, actively worked on by the National Cryptologic Centre, was necessary to establish common aspects and methodologies relating to security when public administrations implement and use electronic resources, in order to create the necessary trust conditions when using the aforementioned electronic resources to exercise rights and fulfil duties using these resources.

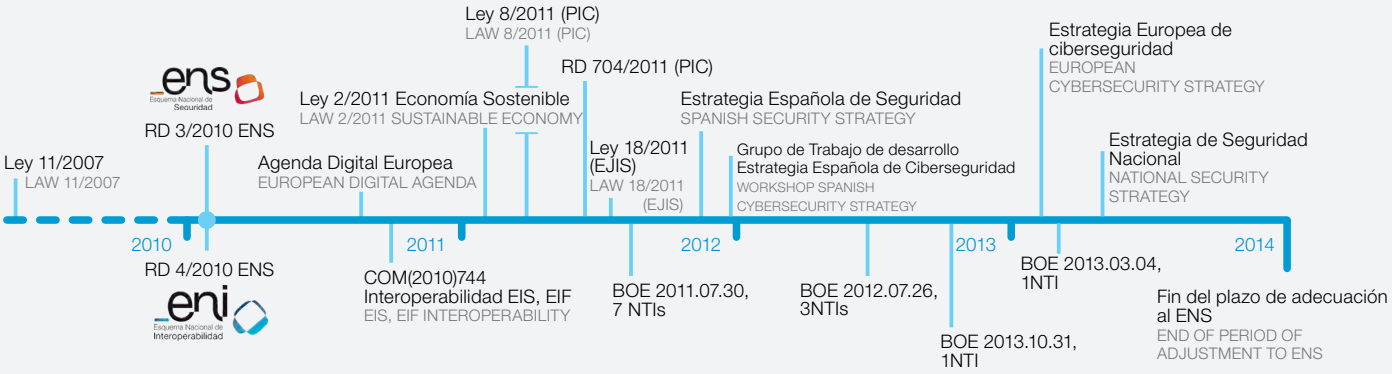
In order to drive its development and implantation, an agreement was signed in 2011 by the Executive Secretary of State for the National Intelligence Centre (CNI), Félix Sanz Roldán, the Secretary of State for Public Functions within the Ministry of Territorial Policy and Public Administration (now Ministry of the Inland Revenue and Public Administrations), Consuelo Rumí, and director of the National Institute of Public Administration (INAP), Ángel Manuel Moreno. By virtue of this agreement, the CCN promised to draw

Administraciones Públicas), Consuelo Rumí, y el director del **Instituto Nacional de Administración Pública (INAP)**, Ángel Manuel Moreno, firmaron un convenio en julio de 2011. En virtud de dicho acuerdo, el CCN se comprometía a elaborar y proporcionar una serie de guías CCN-STIC, colaborar en la formación del personal de las Administraciones Públicas y proporcionar seguridad a la Intranet Administrativa.

A finales de 2012, este compromiso se había materializado en el desarrollo y publicación, por parte del CCN y de la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica de la Secretaría de Estado de Administraciones Públicas, de 22 guías de la serie 800, de desarrollo del RD 3/2010, 14 de ellas nuevas (*véase listado de Guías CCN-STIC*).

Estas guías se encuentran disponibles en el portal web del CCN-CERT, cuyo espacio destinado al ENS se ha ido ampliando paulatinamente. Así, a finales de 2012, este espacio disponía de programas de apoyo (controles de aplicación en el ENS, Herramienta PILAR y MAGERIT versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), módulos de cumplimiento y adecuación, documentación y preguntas frecuentes con las dudas recibidas por parte de los diferentes organismos a lo largo de estos tres años, incluyendo consultas de tipo jurídico y legal.

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS



Acciones desarrolladas en relación con la implantación del RD 3/2012 y RD 4/2010

ACTIONS TAKEN RELATING TO IMPLANTING THE RD 3/2012 AND RD 4/2010

up and provide a series of CCN-STIC guides intended for Administration managers, working on Public Administration staff training and providing security for Administrative Intranet.

At the end of 2012, the CCN and the PA Secretary of State met this commitment by developing and publishing 22 guides from the 800 series, developing the RD 3/2010, 14 of which were news (see list of CCN-STIC guides).

All these guides are available on the CCN-CERT website that boasts an ever-growing section devoted to the NSF. By the end of 2012, this area offered support programs (application checks in the NSF, PILAR tool and Risk Analysis and Management Methodology), compliance and adaptation modules, documentation and FAQs compiling all enquiries received from different organisations over the last three years, including legal enquiries or legal consultancy.

4.5 Investigación y desarrollo de productos

Una de las funciones del Centro Criptológico Nacional (recogidas en el artículo 2.2 del RD 421/2004) es la de coordinar la promoción, desarrollo, obtención, adquisición y puesta en explotación y la 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 que utiliza la Administración Pública, y representa un apoyo al desarrollo de empresas españolas que apuestan por la innovación. Durante los años 2011 y 2012, el CCN ha participado y/o llevado la dirección técnica en los siguientes proyectos:

Criptosistema EP430GN, financiado en parte con fondos de la Dirección General de Armamento y Material del Ministerio de Defensa (DGAM) entre los años 2005-2009, bajo la dirección técnica del CCN y desarrollado por la empresa Epicom.

- Sistema de cifrado que protege las comunicaciones multimedia (voz IP, video, datos,…), y permite el despliegue de redes privadas virtuales (VPN) de un modo completamente seguro.
- Evaluado durante 2012 por la agencia OTAN SECAN (Military Committee Communications and Information Systems Security and Evaluation Agency) y aprobado en mayo de 2013 por NAMILCOM (NATO Military Committee) para manejar información OTAN y Nacional clasificada. Esta aprobación, por primera vez, de un cifrador nacional para procesar información OTAN clasificada, avala a España como uno de los pocos países que dentro de la Alianza tienen capacidad para producir productos de cifra de alto nivel de seguridad y permite su incorporación al grupo exclusivo de las llamadas naciones productoras, entre las que se encuentran Estados Unidos, Gran Bretaña, Alemania, Francia, Noruega, Turquía, Italia y Holanda.
- Desarrollo de una versión de dicho cifrador para su presentación a evaluación por parte de la UE, con objeto de que España se pueda convertir en organismo AQUA (Appropriated Qualified Authority).

4.5 PRODUCT RESEARCH AND DEVELOPMENT

One of the National Cryptologic Centre's functions (compiled in article 2.2 of RD 421/2004) is coordinating promotion, development, obtaining, purchasing, operating and using ICT systems' security technology including encryption to process, store or send out information securely. This RTD chapter is fundamental to guarantee security for ICT systems used by public administrations and it represents support for developing Spanish companies that are backing innovation. Over 2011 and 2012, the CCN has participated and/or taken over technical management in the following projects:

- **Cripto System IP EP430GN,** partly financed by Ministry of Defence General Board for Arms and Materials funds between 2005-2009, with CCN technical management, developed by Epicom.
  Encrypting system that protects multimedia communications (IP voice, video, data, etc.) and means that virtual private networks can be deployed entirely securely.
  Evaluated during 2012 by the NATO SECAN agency (Military Committee Communications and Information Systems Security and Evaluation Agency) and approved in May 2013 by NAMILCOM (NATO Military Committee) to handle NATO and National classified information. This first-time approval of a national encryption device to process NATO classified information, endorses Spain as one of the few countries within the Alliance that has the capability to produce high security encrypted products, opening the door for it to join the exclusive group known as producing nations including United States, Great Britain, Germany, France, Norway, Turkey, Italy and the Netherlands. Developing a version of this encryption device to be presented for EU evaluation, so that Spain might become an AQUA organisation (Appropriated Qualified Authority).

Criptoper Scap Procif, continuación y seguimiento del desarrollo de diversas aplicaciones y funcionalidades (financiado por la DGAM y desarrollado por la empresa Tecnobit).

- Cifrador (voz y datos) con protocolo de interoperabilidad SCIP para transmitir información nacional clasificada y OTAN de forma segura a través del sistema satélite IRIDIUM. Primer producto de cifra nacional que ha sido adquirido por OTAN.
- Participación en la sesión de interoperabilidad cripto de la NC3A (NATO Consultation, Command and Control Agency), verificando la correcta implementación del protocolo SCIP de este producto.
- Desarrollo de la versión para sistema satélite INMARSAT.

TMSDef: continuación y seguimiento del desarrollo de nuevas funcionalidades. Terminal Móvil Seguro del Ministerio de Defensa para redes de telefonía móvil 3G.

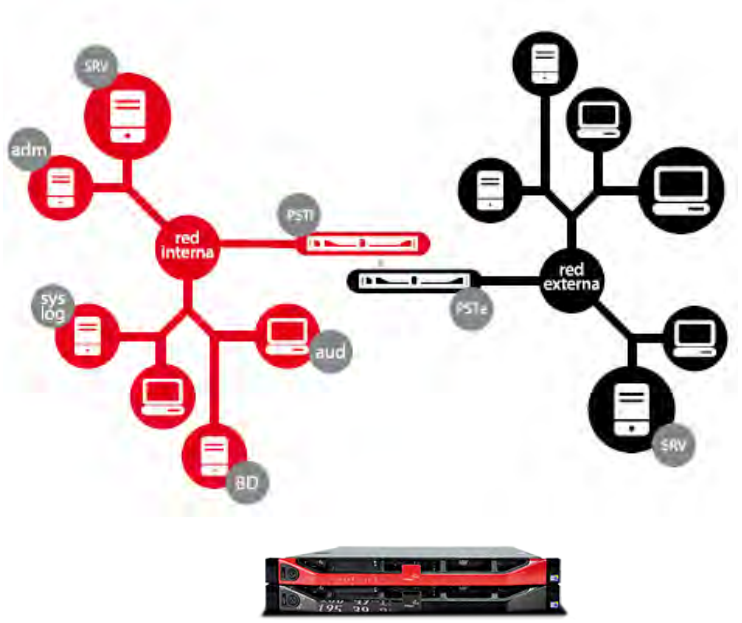
Terminal móvil, tipo PDA: para autoridades, financiado con fondos de Presidencia del Gobierno, entre 2009 y 2012. Este terminal permite la transmisión de voz de forma segura.

La aprobación por el Comité Militar de la OTAN, por primera vez, de un cifrador nacional (el EP430GN) para procesar información OTAN clasificada, es un hito histórico y avala a España como uno de los pocos países que dentro de la Alianza tienen capacidad para producir productos de cifra de alto nivel de seguridad.

First-time approval of a national encryption device (EP430GN) by the NATO Military Committee to process classified NATO information represents a historical milestone and endorses Spain as one of the few countries in the Alliance with capability to produce high security encryption products

- **Criptoper SCAP Procif,** continuation and monitoring of how different applications and functional features are being developed (funded by DGAM) and work is carried out by Tecnobit). Encryption device (voice and data) with SCIP interoperability protocol to send out classified national and NATO information securely over the IRIDIUM satellite system. First national encryption product sold to NATO. Participation in the encryption interoperability session from the NC3A (NATO Consultation, Command and Control Agency), verifying correct implementation of the SCIP protocol for this product. Development of the version for the INMARSAT satellite system.
- **TMSDef,** continuation and monitoring of new functional feature development. Ministry of Defence Secure Mobile Terminal for 3G mobile phone networks.
- **PDA type mobile terminal**, for authorities, financed by Government President's Office funds between 2009 and 2012. This terminal transmits voice information securely.

Criptoper SCAP Procif



Pasarelas seguras: el CCN ha participado en su análisis y diseño junto con la empresa Autek. Permiten garantizar el intercambio de información de forma segura y controlada entre redes de diferente nivel de acreditación.

- PSTMail: gestiona cuentas de correo de redes externas desde redes aisladas.
- PSTfile: pasarela para intercambio de ficheros automáticamente.
- PSTDoc: pasarela de acceso seguro a documentos externos bajo demanda, desde una red aislada, con el fin de intercambiar ficheros situados en otra red.

Diverso: desarrollo del sistema de distribución de versiones de software y documentación de equipos de cifra. El CCN ha participado en su diseño y desarrollo junto con la empresa EPICOM

Demostrador de Cifrador IP Táctico: financiado con fondos de I+D de la DGAM (2011 y 2012). Desarrollo de un cifrador con arquitectura de seguridad mejorada y capacidad media de transmisión de información (200 Mb/s) rugerizado para su empleo en entornos tácticos.

Cifrador Personal Interoperable SCIP Multipropósito: financiado con fondos de la DGAM (2011 y 2012). Desarrollo de un cifrador (voz y datos) con capacidad para transmitir información clasificada nacional y OTAN de forma segura a través de diferentes redes de comunicaciones, fundamentalmente inalámbricas.

Disco duro de estado sólido cifrado para almacenamiento seguro de información en ordenadores portátiles y personales (seguimiento de su desarrollo).

4.5 PRODUCT RESEARCH AND DEVELOPMENT

- Secure gateways, the CCN has participated in their analysis and design alongside Autek. Secure gateways guarantee secure, controlled information exchange between networks with different levels of accreditation.
  - PSTMail: secure email exchange gateway.
  - PSTfile: gateway for automatic file exchange.
  - PSTDoc: gateway giving secure access to external documents on demand, from an isolated network, in order to exchange files in another network.
- Diverso, development of the distribution system for encryption equipment software versions and documentation. The CCN was involved in its design and development, working alongside EPICOM.
- Tactical IP Encryption Device Demonstrator, financed with DGAM RTD funds (2011 and 2012). Development of an encryptor with improved security architecture and medium information transmission capacity (200 Mb/s) rugged up for use in tactical environments.
- Multipurpose SCIP Interoperable Personal Encryption Device, financed with DGAM RTD funds (2011 and 2012). Development of an encryption device (voice and data) with capacity to send out national and NATO classified information securely over the different, fundamentally wireless, communications networks.
- Encrypted Solid State Drive (SSD) to store information securely on laptops and personal computers (monitoring its development).

4.5.1 Apoyos técnicos más significativos

El CCN realizo durante los años 2011 y 2012 una intensa actividad de apoyo técnico a distintos desarrollos de productos y sistemas de cifra. Conviene destacar los siguientes:

- A la empresa EADS-CASA para la evaluación TEMPEST de distintas plataformas aéreas para repostaje en vuelo. Los aviones fueron adquiridos por varios países y, entre los requisitos que deben cumplir, se encuentran los requisitos TEMPEST sobre seguridad de las emanaciones. Los trabajos se efectúan en las instalaciones de la empresa en Getafe (Madrid). Ejemplo de ello es la evaluación y certificación de aviones de suministro en vuelo para el gobierno australiano (A330-MRTT), plataforma ya certificada, y la versión para el gobierno inglés (FSTA).

- Asesoramiento a organismos de la Administración para la adquisición de sistemas de protección TEMPEST. Principalmente instalaciones del Ministerio de Defensa y del Ministerio de Asuntos Exteriores y de Cooperación.

- Gestión y programación de los algoritmos de cifrado en todos los equipos producidos por la empresa EPICOM para la Administración del Estado.

- Participación y ejecución de actividades técnicas en grupos de trabajo internacionales sobre aspectos COMSEC y TEMPEST del futuro avión de transporte militar A400M, del EF2000, sistema GALILEO, así como sobre cuestiones criptológicas del terminal MIDS. (Multifunctional Information Distribution System)

- Laboratorio TEMPEST acreditado para la realización de las medidas de evaluación al avión A400M que se está montando en la factoría de EADS-CASA en Sevilla, en las distintas versiones disponibles para cada uno de los países participantes en el Programa.

- Apoyo a la Administración en la resolución de cuestiones técnicas relacionadas con el empleo de la criptología en el ENS y en el DNIe, así como sobre aspectos relacionados con la evaluación y certificación de la seguridad funcional de los productos STIC.

GALILEO

4.5.1 MOST SIGNIFICANT TECHNICAL SUPPORTS

In this task of assessing and accrediting the capacity of encryption products and information technology systems, including encryption resources and their promotion, the CCN carried out intense technical support work for different developments in 2011 and 2012. The following should be highlighted:

- EADS-CASA for the TEMPEST evaluation on different aerial platforms for refuelling in-flight. These planes were bought by several countries and the requirements they must meet include TEMPEST requirements on leak security. This work currently takes place in the company's facilities in Getafe (Madrid) and as an example, we might mention the evaluation and certification of in-flight supply planes for the Australian government (A330-MRTT) (this platform has already been certified), and the version for the British government (FSTA).

- Consultancy for several different Administration organisations to purchase TEMPEST protection systems. This mainly refers to Ministry of Defence and Ministry of Foreign Affairs and Cooperation facilities.

- Management and programming of encryption algorithms in all equipment produced by EPICOM for State Administration.

- Participation and execution of technical activities in international working groups on COMSEC and TEMPEST aspects of the future A400M military transportation, the EF2000, GALILEO system, and on encryption matters for the MIDS terminal.

- TEMPEST laboratory accredited to carry out evaluation measurements on the A400M plane that is being assembled at the EADS-CASA plant in Seville in the different versions available for each of the countries participating in the Programme.

- Support for the Administration in resolving technical issues related to the use of cryptology in the NSF and the DNIe (electronic ID document), as well as aspects related to evaluating and certifying the functional security of STIC products.

5 CCN-CERT, contención frente a los ciberataques

El Gobierno, consciente de la necesidad de incrementar las capacidades de prevención, detección, análisis, respuesta y coordinación ante las ciberamenazas sufridas por las Administraciones Públicas y los sistemas clasificados, creó la capacidad de respuesta ante incidentes Gubernamental (CCN-CERT), dependiente del Centro Criptológico Nacional.

Desde entonces, el **CERT Gubernamental/nacional**, cuyas funciones quedan recogidas en la **Ley 11/2002** reguladora del Centro Nacional de Inteligencia, el **RD 421/2004** de regulación del CCN y en el **RD 3/2010**, de 8 de enero, regulador del Esquema Nacional de Seguridad, ha sido un factor clave en la protección del ciberespacio español.

En un primer momento, fijó su actividad en los sistemas de las distintas Administraciones (general, autonómica y local) para, ya en los dos últimos años, ampliar esta responsabilidad a los ciberataques sobre sistemas de **empresas** pertenecientes a **sectores** designados como **estratégicos**, esenciales para la seguridad nacional y para el conjunto de la economía del país. Así, su misión en estos momentos es la de *contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a las* ***Administraciones Públicas*** *y a las* ***empresas estratégicas****, y afrontar de forma activa las nuevas ciberamenazas.*

Esta misión se desarrolla a través de numerosos servicios, en constante actualización, en función del universo cambiante de los ciberataques:

- Gestión de incidentes
- Sistemas de Alerta Temprana.
- Sistema de Información, alertas, avisos y vulnerabilidades.
- Auditorías web.
- Sistema multiantivirus.
- Formación y sensibilización.
- Capacidad forense y de ingeniería inversa

CCN-CERT, CONTAINMENT AGAINST CYBER-ATTACKS

Spanish Government was aware of the need to increase capabilities involving prevention, detection, analysis, tackling and coordination in the light of cyber threats inflicted on public administrations and classified systems, so it set up CCN-CERT, under the National Cryptologic Centre (CCN). Ever since, the governmental/national CERT, whose functions are compiled in Law 11/2002 regulating the National Intelligence Centre, RD 421/2004 regulating the CCN and RD 3/2010, dated 8th January, regulating the National Security Framework, has taken a key role in protecting Spanish cyber-space.

First of all, it defined its workplace as the different (general, regional and local) Administration systems so that, over the last two years, it could broaden this responsibility to cyber-attacks on systems in companies belonging to designated strategic sectors, essential for national security and for the country's overall economy. Consequently, its assignment right now involves helping to improve Spanish cybersecurity, as the national alarm and response centre that cooperates and helps to provide a fast and effective response to public administrations and strategic companies and actively tackle new cyber threats.

This assignment involves working on many constantly updated services, depending on the changing world of cyber-attacks:

- Incidents management
- Early Warning Systems
- Information System, alarms, warnings and vulnerabilities
- Web audits
- Multi-anitivirus system
- Training and awareness raising
- Forensic and reverse engineering capacities

5.1 Gestión de incidentes

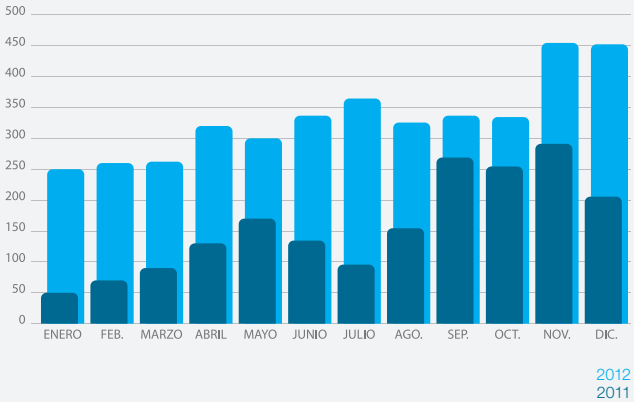
El CERT Gubernamental brinda apoyo técnico y operativo a las Administraciones Públicas y empresas estratégicas que sufren ciberataques, tanto en las etapas de detección, como en la reacción y la contención. A ello se une una política preventiva, en la que trabaja un equipo de expertos destinados a investigar sobre técnicas empleadas, soluciones y procedimientos más adecuados para hacerlos frente.

Durante los dos últimos años, y a través de distintas fuentes de notificación (Servicios SAT, CARMEN, Portal Web…) el CCN-CERT gestionó 6.256 ciberincidentes (2.253 en 2011 y 4.003 en 2012), una cifra muy superior a la registrada en años anteriores, con crecimientos exponenciales y, lo que es más preocupante, con un grado de criticidad cada vez más elevado. Así, mientras que en el año 2011 los incidentes catalogados por el equipo del CCN-CERT con un riesgo de "muy alto" o "crítico" fueron 94; en 2012, este número se elevó hasta los 231, siendo las Amenazas Persistentes Avanzadas (APT)[1] las más alarmantes por ser el foco del ciberespionaje gubernamental e industrial.

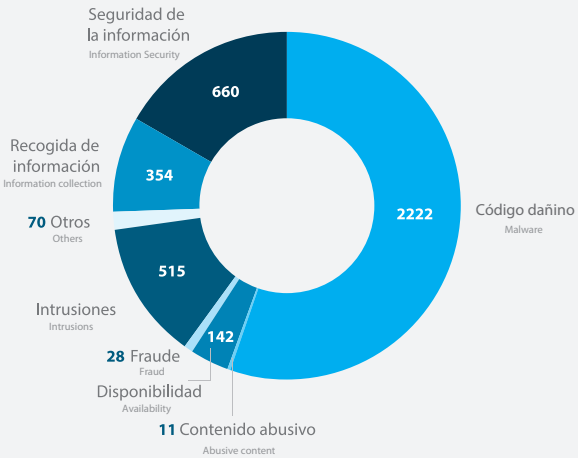
En este sentido, el CCN-CERT elabora y facilita a los organismos unos Indicadores de Compromiso (IOC) para la mejor gestión de un ataque.

[1]Advanced Persistent Threats (APT): La persistencia en el tiempo y lo avanzado o complejo (tanto por las técnicas empleadas como por los procedimientos de actuación desarrollados) son las características que definen a este tipo de ataques cada vez más comunes y que eligen a su víctima convenientemente.

Número de incidentes gestionados por el CCN-CERT
NUMBER OF INCIDENTS MANAGED BY THE CCN-CERT



Tipología de incidentes gestionados por CCN-CERT (2012)
INCIDENT TYPES MANAGED BY THE CCN-CERT (2012)



5.1 INCIDENT MANAGEMENT

The Governmental CERT offers technical and operative support to public administrations and strategic companies undergoing cyber-attacks, in detection, reaction and containment stages. This goes along with a preventive policy involving a team of experts working on techniques used, the most appropriate solutions and procedures to tackle them.

Over the last two years, and through different notification sources (SAT services, CARMEN, Web Portal, etc.) the CCN-CERT managed 6256 cyber-incidents (2253 in 2011 and 4003 in 2012), a much higher figure than registered in previous years, with exponential growth and, what is most worrying, with an ever-growing degree of critical severity. So, whilst there were 94 incidents in 2011 catalogued by the CCN-CERT team with a "very high" or "critical" risk; in 2012, this number had risen to 231, where Advanced Persistent Threats (APT) were the most alarming as they were the focus of governmental and industrial cyber-espionage (on strategic companies).

In this respect, the CCN-CERT draws up and provides organisations with Commitment Indicators (IOC) to manage an attack more successfully.

[1]Advanced Persistent Threats (APT): These types of attacks are defined by their persistence over time and their advanced or complex nature (due to techniques used and action procedures developed). They are increasingly common and specifically pick their victims.

5.2 Sistemas de Alerta Temprana, SAT

Para garantizar el nivel de seguridad adecuado en los sistemas de las Administraciones Públicas es necesario actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance.

Por este motivo, desde el año 2008, el CCN-CERT viene desarrollando soluciones que permitan la detección rápida de incidentes y anomalías dentro de la Administración, con el fin de realizar acciones preventivas, correctivas y de contención.

El S.A.T. cuenta con dos vertientes con un denominador común: la detección temprana de intrusiones. En ambos casos existe un portal de informes al que los responsables de seguridad autorizados pueden acceder para la consulta en tiempo real de eventos de seguridad y para la generación de informes a medida.

Durante los dos últimos años, y a través de distintas fuentes de notificación (Servicios SAT, CARMEN, Portal Web…) el CCN-CERT gestionó 6.256 ciberincidentes, una cifra muy superior a la registrada en años anteriores y con un grado de criticidad cada vez más elevado.

Over the last two years, and through different notification sources (SAT services, CARMEN, Web Portal, etc.) the CCN-CERT managed 6256 cyber-incidents, a much higher figure than registered in previous years, with an ever-higher degree of critical severity

5.2 EARLY WARNING SYSTEMS, SAT

In order to guarantee the right level of security in public administration systems, it is necessary to act now rather than wait for an incident to occur or, at least, detect it immediately to reduce its impact and scope.

For this reason, since 2008, the CCN-CERT has been developing an Early Warning System (SAT) to speed up incident and anomaly detection within the Administration, to be able to carry out preventive, corrective and containment actions.

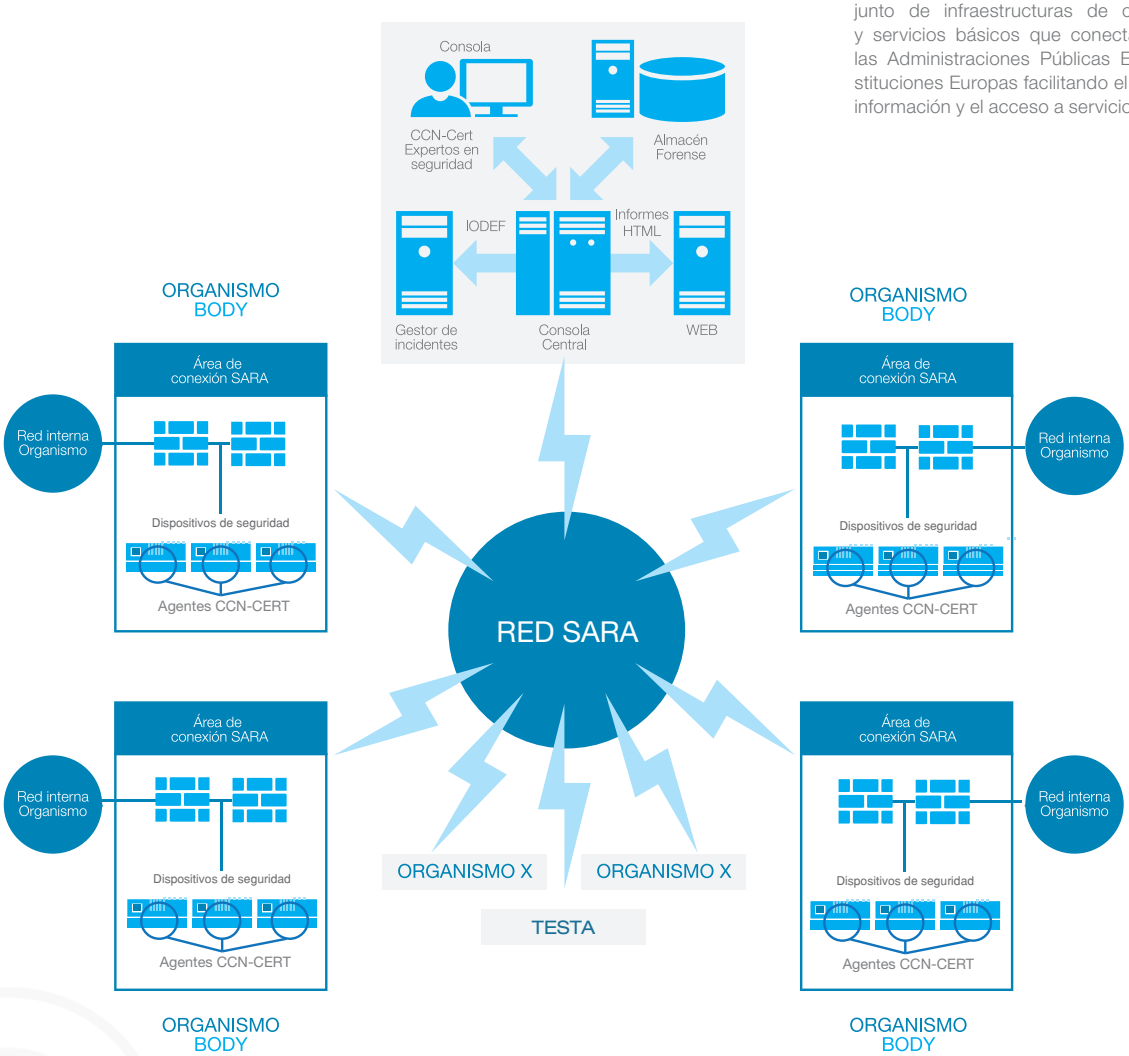
The SAT has two aspects with a common denominator: early detection of intrusions. In both cases, there is a report website that authorised security supervisors can consult to see security events in real time and to generate custom-made reports

5.2.1 SAT-SARA

En colaboración con el Ministerio de Hacienda y Administraciones Públicas, el CCN-CERT inició la implantación del **Sistema de Alerta Temprana de la red SARA**[2] en el año 2008. Su principal objetivo es la detección en tiempo real de ataques y amenazas, después del análisis y correlación de los registros generados por las diferentes herramientas que analizan el tráfico circulante entre los organismos de las Administraciones Públicas conectados a dicha Red.

Al término del año 2012, son **51 los organismos públicos** (incluyendo la totalidad de Ministerios, Comunidades Autónomas y otros organismos clave de la Administración) que disponen de este servicio. En total, en el año 2012 se notificaron **430 incidentes**, frente a los **322** del ejercicio anterior.

[2]SARA: Sistema de Aplicaciones y Redes para las Administraciones. La Red SARA es un conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las Administraciones Públicas Españolas e instituciones Europas facilitando el intercambio de información y el acceso a servicios.



5.2.1 SAT-SARA

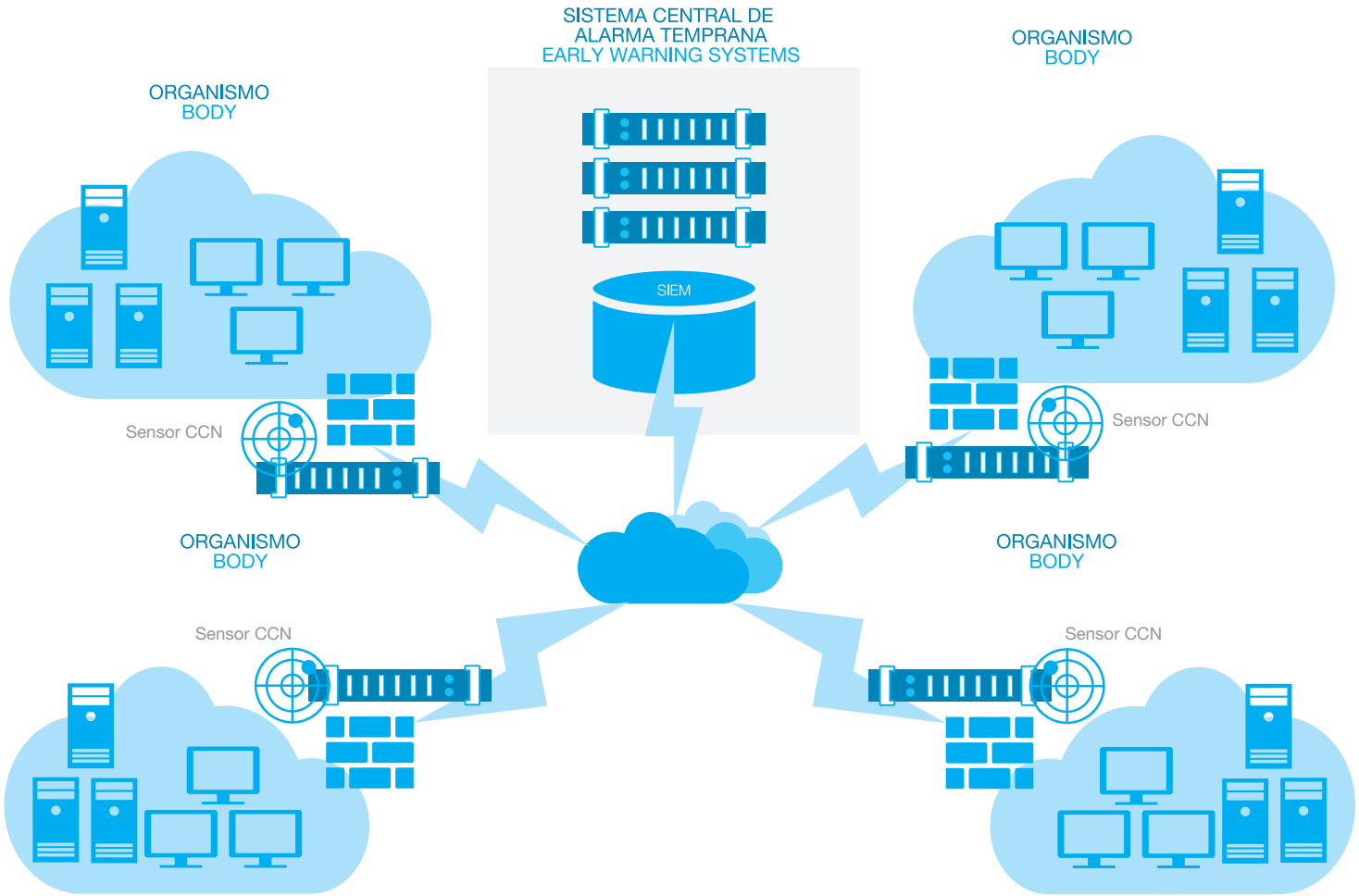
Working with the Ministry of Inland Revenue and Public Administrations, the CCN-CERT began to implant the SARA network Early Warning System in 2008. Its main aim is to detect attacks and threats in real time, carried out after analysing the network traffic among the networks of Public Administration organisations connected to this Network.

By the end of 2012, 51 public organisations had joined this service (including all the Ministries, other key Administration organisations and Autonomous Communities). In total, notification was received concerning 430 incidents in 2012, compared to 322 the previous year.

[2]SARA: Applications and Networks Systems for Administrations (Sistema de Aplicaciones y Redes para las Administraciones). The SARA Network is a set of communications infrastructures and basic services that connect Spanish Public Administration and European institution networks, making it easier to exchange information and access services.

5.2.2 SAT de Internet

En el año 2009, y tras los buenos resultados cosechados por el SAT en la Red SARA, el CCN-CERT desarrolló un nuevo servicio de detección rápida de incidentes y anomalías, en esta ocasión en las salidas de Internet de los distintos organismos de la Administración. El SAT-INET inició su andadura con el despliegue de sondas individuales orientadas a la detección en tiempo real de las amenazas existentes en el tráfico que fluye entre las redes internas de las distintas Administraciones Públicas e Internet. En estos cuatro años, **38 organismos públicos** se han adscrito al Sistema (entre ellos algunas Comunidades Autónomas) y han disfrutado de las ventajas que se le ofrecen para la protección de sus sistemas, así como para la contención y eliminación de sus ciberamenazas. De hecho, a través de este servicio se gestionaron en 2012 un total de **3.363 incidentes de ciberseguridad**, más del doble que los 1.457 detectados en 2011.



5.2.2 INTERNET SAT

In 2009, following good SAT results in the SARA network, the CCN-CERT developed a new fast incident and fault detection service, on this occasion for Internet outlets to the different Administration organisations.

The SAT-INET began by deploying individual probes for real time detection of threats in the traffic flowing through the different Public Administration and Internet internal networks. Over the last four years, 38 public organisations have joined the System (including some Autonomous Communities) and have enjoyed the advantages it offered in terms of protecting their systems, plus containing and eliminating their cyber threats. In 2012, this service managed a total of 3363 cybersecurity incidents, more than double the 1457 detected in 2011.

5.3 CARMEN

Dentro de las ciberamenazas existentes, en los dos últimos años, el CCN-CERT ha detectado una especial virulencia en las denominadas APT (*Advanced Persistent Threat*). El objetivo de estos ataques es mantener una presencia prolongada (incluso de años) sobre los sistemas de información o dispositivos de la víctima que, además, es escogida convenientemente por el valor de la información que albergan y/o por la repercusión de su actividad. Otra de sus señas de identidad es que están especialmente diseñados para no ser detectados, de manera que los sistemas tradicionales de detección de código dañino presentan una tasa de detección extremadamente baja para este tipo de amenazas.

Por este motivo, y a partir del conocimiento adquirido tras la resolución de diversos incidentes de seguridad, particularmente APT, que han afectado a la Administración Pública española y a otras empresas estratégicas, el CCN-CERT ha desarrollado el sistema **CARMEN (Centro de Análisis de Registros y Minería de Eventos)** que, mediante la utilización de minería de datos, proporciona una mejor visión del tráfico generado por un organismo, lo que permite la detección de un APT en curso. Durante el año 2012 se puso en marcha un piloto para evaluar los resultados obtenidos por esta herramienta, para lo cual se desplegaron cinco equipos en diferentes organismos. Los resultados de esta prueba han sido altamente satisfactorios.

5.4 Sistema de Información, alertas, avisos y vulnerabilidades

Conocer de primera mano y de fuentes especializadas (en algunos casos cerradas), el estado de la ciberseguridad es un aspecto fundamental para anticiparse a cualquier ataque y, llegado el caso, poder responder y contener su alcance. Por este motivo, el CCN-CERT ofrece a toda su comunidad información, entre la que destacan las vulnerabilidades, alertas y avisos de nuevas amenazas que vienen a reducir el riesgo y, en consecuencia, disminuir la probabilidad de incidentes.

A través de este servicio, el CERT Gubernamental pretende reducir tanto las **vulnerabilidades técnicas** (de hardware o software), como **humanas** (sitios web y aplicaciones que carecen de suficiente seguridad, debilidad de contraseñas, software sin actualizar, etc.) y de **organización**, intentando evitar que los atacantes penetren en los sistemas y aplicaciones e influyan en su funcionamiento.

De este modo, durante el año 2011 y 2012, el CCN-CERT informó sobre más de **22.500 vulnerabilidades** y **245.000 muestras de código dañino**. Además se enviaron a más de 3.900 usuarios de la Administración Pública 28 avisos o alertas sobre distintas materias de ciberseguridad.

5.3 CARMEN

Within existing cyber threats, over the last two years, the CCN-CERT has detected particular virulence in what are known as APT (Advanced Persistent Threat). These attacks aim to remain (possibly for years) in the victim's information systems or devices.

The victim is also hand-picked (due to the value of the information they store and/or the repercussions of their work). Another identifying feature is that they are specifically designed not to be detected so that traditional malicious code detection systems have an extremely low detection rate for this type of threat.

For this reason, and working from knowledge acquired from resolving a variety of security incidents, particularly APTs, that have affected the Spanish Public Administration and other strategic companies, the CCN-CERT developed the **CARMEN** system (**Registry Analysis and Events Mining Centre**) that, by using data mining, provides a better view of the traffic generated by an Organisation allowing it to detect an APT in operation. During 2012, a pilot was set up to evaluate results obtained by this tool, deploying five teams in different organisations. The results for this test were highly satisfactory.

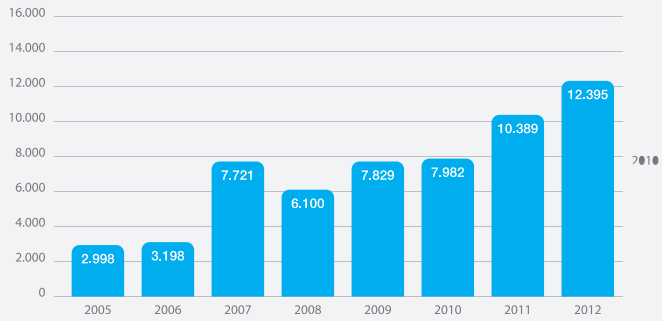
Por otra parte, el CCN-CERT elabora y difunde estudios, análisis e informes sobre las posibles técnicas de agresión que pueden afectar a los sistemas de información y comunicaciones de distintos organismos, así como la resolución de incidentes de seguridad. En ocasiones, además, se incluye parámetros (firmas de ataque) que permiten identificar determinado software dañino.

De igual modo, y a través de su portal web, se difunde.

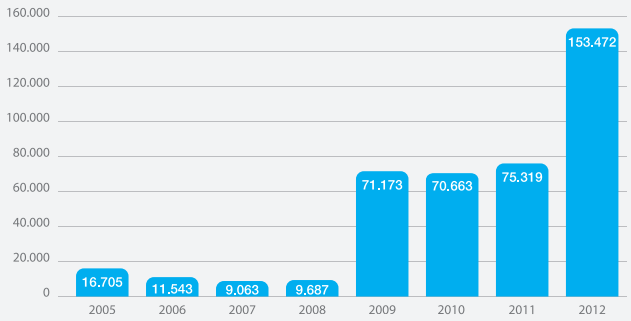
- Informes de Amenazas (17 en 2012 y 14 en 2011).
- Informes de Actualidad (24 cada año).
- Informes de Código Dañino (6 cada ejercicio).

Evolución de las vulnerabilidades y código dañino publicadas en el porta del CCN-CERT
EVOLUTION OF VULNERABILITIES AND MALICIOUS CODE PUBLISHED ON THE WEBSITE CCN-CERT

Número de Vulnerabilidades
NUMBER OF VULNERABILITIES



Número de Código Dañino
NUMBER OF MALICIOUS CODE INCIDENTS



5.4 INFORMATION SYSTEM, ALARMS, WARNINGS AND VULNERABILITIES

Knowing the state of your cybersecurity first hand and from specialised sources (in some cases closed) is fundamental to anticipate any kind of attack and, should the case arise, be able to respond and contain its scope. For this reason, the CCN-CERT offers a variety of information to its entire Community, including vulnerabilities, alarms and warnings of new threats that reduce risks and consequently lower the probability of incidents.

Through this service, the Governmental CERT aims to reduce both technical (concerning hardware or software) and human vulnerabilities (websites and applications with insufficient security, weak passwords, software that has not been updated, etc.) and organisational vulnerabilities, attempting to prevent attackers from penetrating the systems and applications and influencing their operation.

In this way, during 2011 and 2012, the CCN-CERT informed on over 22,500 vulnerabilities and 245,000 samples of malicious code. In addition, over 3,900 public administration users were sent 28 warnings or alarms on different cybersecurity issues.

On the other hand, the CCN-CERT draws up and sends out studies, analysis and reports on possible aggression techniques that might affect information and communications systems in different organisations as well as resolving security incidents. Occasionally, parameters (attack signatures) are also included to be able to identify certain malicious software.

In the same way, through the website it sends out

- Threat Reports (17 in 2012 and 14 in 2011)
- News Reports (24 a year)
- Malicious Code Reports (6 each exercise)

5.5 Sensibilización, por una cultura de ciberseguridad

Contribuir a la mejora de la ciberseguridad en España, una de las funciones del Centro Criptológico Nacional, pasa, ineludiblemente, por concienciar a todos los agentes que participan en este área de los riesgos de operar en el ciberespacio. Por ello, y para crear una sólida **cultura de ciberseguridad** en todos los ámbitos (Administraciones Públicas, empresas y usuarios finales) es fundamental promover las acciones de información y sensibilización necesarias, así como facilitar los conocimientos y el acceso a las herramientas que posibilitan una mejor protección frente a ataques y amenazas.

En este sentido, el CCN-CERT utiliza algunas de las principales herramientas de formación y comunicación a su alcance: jornadas y conferencias, portal web, redes sociales, comunicados de prensa, artículos en revisas especializadas, etc.

5.5.1 Portal www.ccn-cert.cni.es

El portal web del CCN-CERT es una de las herramientas básicas a la hora de fomentar la cultura de ciberseguridad y de coordinar y dar soporte a todos los responsables TIC de las Administraciones Públicas y de empresas estratégicas (y en menor medida a los usuarios finales que pueden acceder a la parte pública del portal). Más allá de ofrecer unos contenidos, actualizados diariamente, el portal es un reflejo de gran parte de la actividad del CERT Gubernamental y un elemento coordinador de todos sus servicios puestos a disposición de su Comunidad. En él destacan, entre otras, las siguientes secciones, todas ellas con material sin clasificar:

- Servicios SAT: en donde se incluyen estadísticas extraídas de los portales de informes de ambos sistemas (SAT-SARA y SAT-INET).
- Esquema Nacional de Seguridad: Legislación, guías, programas de apoyo, adecuación al ENS y Seguimiento del progreso, documentación, FAQ y contacto.
- Guías CCN-STIC: tanto públicas como de acceso restringido.
- Herramientas: PILAR, Sistema Multiantivirus, etc.
- Cursos CCN-STIC: presenciales y on-line.
- Boletines diarios de vulnerabilidades (públicos y privados).
- Informes de amenazas, actualidad y código dañino.

Buena prueba del éxito de este portal son los casi **4.000 usuarios registrados,** a 31 de diciembre de 2012 (procedente de las distintas administraciones públicas y de empresas de seguridad y de sectores estratégicos), así como los números de accesos mensuales, con más de **250.000 de media.** Toda la información del portal es sin clasificar.

5.5 AWARENESS-RAISING, WORKING ON CYBERSECURITY CULTURE

Helping to improve cybersecurity in Spain, a fundamental part of the National Cryptologic Centre's work, undoubtedly involves raising awareness among all agents participating in this area concerning cyberspace operating risks. For this reason, and to create a solid cybersecurity culture in all fields (public administrations, companies and end users), it is fundamental to promote the necessary information and awareness raising actions and facilitate knowledge and access to the tools that improve protection against attacks and threats.

In this respect, the CCN-CERT uses some of the main training and communication tools around: workshops and conferences, website, social networks, press releases, articles in specialist magazines, etc.

5.5.1 WWW.CCN-CERT.CNI.ES WEBSITE

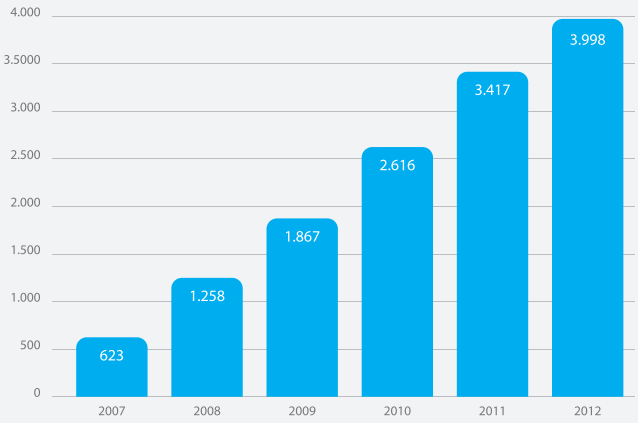
The CCN-CERT website is a basic tool for promoting cybersecurity culture and coordinating and providing support for all ICT managers in public administrations and strategic companies (and to a lesser extent, end users who can access the public website). Beyond offering contents, updated on a daily basis, the website reflects much of the Governmental CERT's activity and a coordinating element for the services it provides to its Community. This includes the following sections:

- SAT services: including statistics extracted from both systems' report websites (SAT- SARA and SAT-INET)
- National Security Framework: legislation, guides, support programmes, adapting the NSF and Monitoring progress, documentation, FAQ and contact
- CCN-STIC guides: both public and restricted access
- Tools: PILAR, Multiantivirus system, etc.
- CCN-STIC Courses: classroom and on-line
- Daily vulnerability updates (public and private)
- Reports on threats, security and malicious code

Almost 4,000 registered users, on 31st December 2012 (from a variety of public administrations, security companies and strategic sectors) offer conclusive proof of this website's success as well as monthly hits totalling an average of over 250,000. Not all the website's information has been classified.

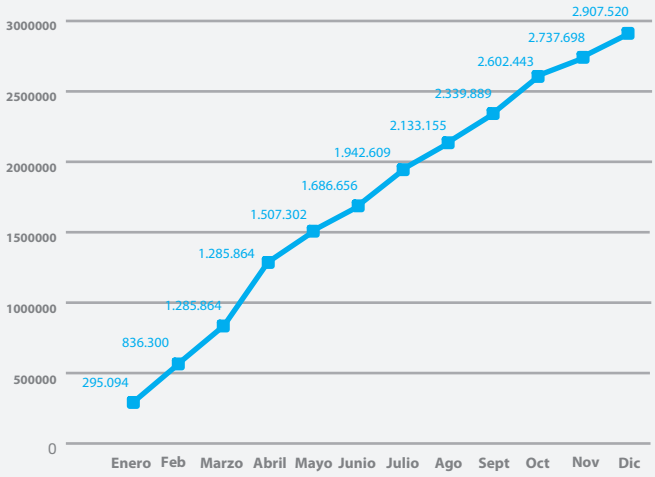
Evolución del número de usuarios registrados en el Portal del CCN-CERT

EVOLUTION OF NUMBER OF USERS REGISTERED ON THE CCN-CERT WEBSITE



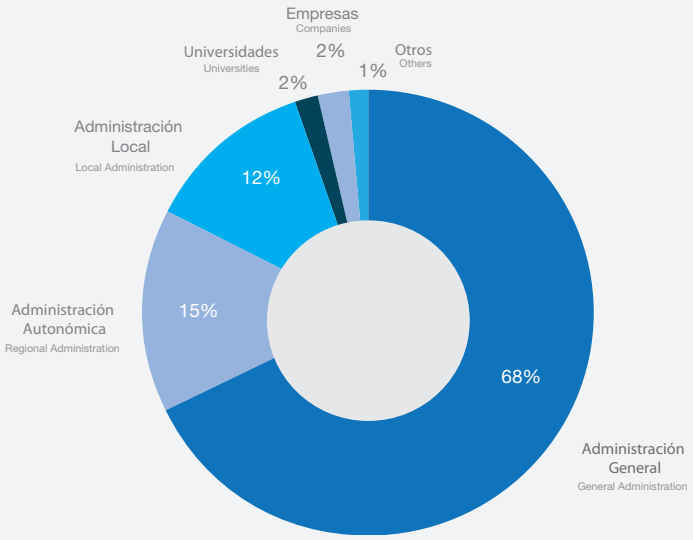
Número de accesos acumulados en 2012

NUMBER OF HITS IN 2012



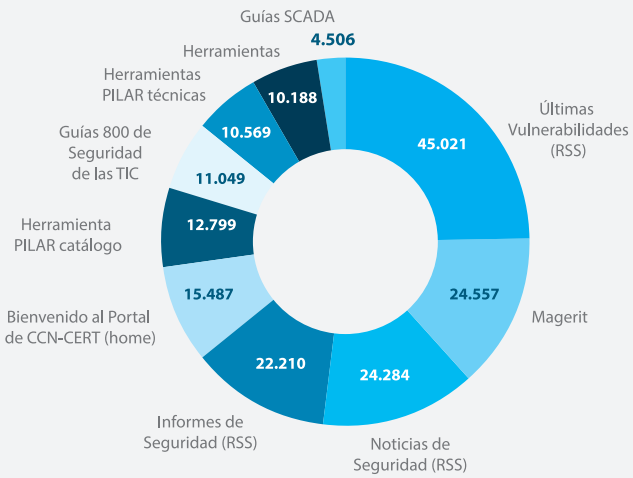
Usuarios registrados totales por organismo

NUMER OF REGISTERED USERS



TOP 10: páginas más visitadas de la parte pública en 2012

TOP 10: PAGES MOST VISITED BY THE PUBLIC IN 2012



5.5.2 Jornadas STIC CCN-CERT y SAT-INET

El CCN-CERT ha venido organizando, desde el año 2007, unas jornadas en las que compartir, con todos los responsables de seguridad TIC de las distintas Administraciones (general, autonómica y local), la situación del sector.

Durante los últimos seis años, las jornadas **STIC CCN-CERT** se han convertido en una cita ineludible del personal de la Administración (y desde el año 2011 de las empresas estratégicas) para la puesta en común de conocimientos, el análisis de las amenazas y el estudio de las soluciones y tendencias con las que hacer frente a estos ciberataques.

El enorme interés despertado hasta la fecha, queda reflejado en el incremento, año tras año, del número de asistentes, pasando de los 200 de su primera edición, a los **500** del año 2012 (**VI Jornadas STIC CCN-CERT**), celebradas en diciembre e inauguradas por el secretario de Estado director del CNI, Félix Sanz.

Del mismo modo, el CERT Gubernamental ha organizado sus **Jornadas del SAT-INET** (llegando a su tercera edición en febrero de 2013) implicando a todos los organismos públicos y a empresas privadas que están adscritos al Servicio de Alerta Temprana, en la mejora de la detección, el intercambio ágil y seguro de la información y en la mejora de la capacidad de defensa.

VI Jornadas STIC CCN-CERT, celebradas en la FNMT en 2012 e inauguradas por el secretario de Estado director del CNI, Félix Sanz (derecha)
6TH CCN-CERT STIC WORKSHOP, HELD IN DECEMBER AND INAUGURATED BY THE SECRETARY OF STATE - CNI DIRECTOR, FÉLIX SANZ (RIGHT)

5.5.2 CCN-CERT AND SAT-INET WORKSHOPS

Since 2007, the CCN-CERT has been organising workshops to share the sector's situation with all ICT managers from the different public administrations (general, regional and local).

Over the last six years, the CCN-CERT STIC workshops have become essential for Administration staff (and also for strategic companies since 2011) to pool knowledge, analyse threats and study solutions and trends to tackle these cyber-attacks.

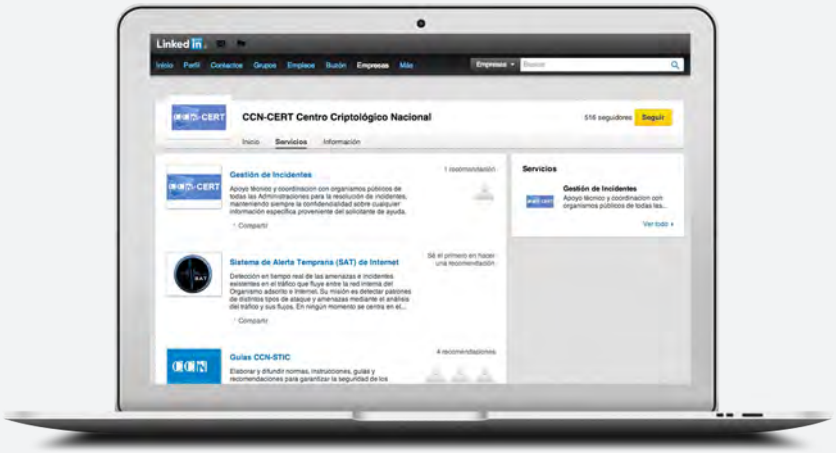
The enormous interest aroused to date is reflected in the year on year increase of the number of participants, rising from 200 in the first edition, to 500 in 2012 (6th CCN-CERT STIC Workshop), held in December and inaugurated by the Secretary of State - CNI Director, Félix Sanz.

In the same way, the Governmental CERT has organized its SAT-INET Workshops (third edition in February 2013) implicating all public organisms and private companies who are signed up to the Early Warning Service, on improving detection, smooth and secure information exchange and improving defences.

5.5.3 Linkedin

Conscientes del fenómeno social que representan las redes sociales, el Centro Criptológico Nacional, a través del CCN-CERT, abrió un nuevo canal de comunicación, en este caso bidireccional. Así, en 2012 creó un perfil de usuario y de empresa en la mayor red social profesional: Linkedin (con más de 135 millones de usuarios en el mundo, de los cuales dos millones están en España).

En apenas cuatro meses, el CCN-CERT contaba con 500 seguidores y 140 impresiones semanales de media.



5.5.3 LINKEDIN

Aware of the phenomena represented by social networks, the National Cryptologic Centre, through the CCN-CERT, opened up a new channel of communication, in this case two-way. Consequently, in 2012 it created a user and company profile in the largest professional social network: Linkedin (over 135 million users throughout the world, 2 million in Spain).

In barely 4 months, the CCN-CERT had 500 followers and 140 weekly hits on average.

6 Organismo de Certificación OC

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 y Certificación TEMPEST**.

Este Organismo de Certificación (OC), en lo relativo a la **Certificación Funcional** de la seguridad de las TI, se articuló 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 por su propia normativa interna adaptada a los requisitos necesarios para ser reconocido tanto a nivel nacional, según la norma EN45011, como a nivel internacional, de acuerdo con el **«Arreglo de Reconocimiento de Certificados de Criterios Comunes» (CCRA),** como entidad de certificación de la seguridad de las TIC.

Para la **Certificación Criptológica** y para la **Certificación TEMPEST**, que también realiza y cuyo ámbito de actuación son los sistemas de la Administración que vayan a manejar información clasificada, el Organismo de Certificación se basa en criterios y metodologías propias.

Durante el año 2012, el Organismo de Certificación estrenó **nuevo portal web**, en el que se ofrece información sobre las distintas certificaciones y acreditaciones de laboratorios, la normativa de referencia, los formularios necesarios para su tramitación y la actualización constante de los productos certificados.

En el marco del CCRA y del Acuerdo SOGIS, el OC/CCN ha seguido participando activamente en los diferentes grupos técnicos y de gestión de ambos acuerdos. También está participando en la nueva versión del CCRA y en las implicaciones que estos cambios pueden tener en ámbitos como OTAN.

Nuevo portal web del Organismo de Certificación (www.oc.ccn.cni.es)
NEW CERTIFICATION BODY WEBSITE (WWW.OC.CCN.CNI.ES)

CERTIFICATION BODY, OC

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

This Certification Body (OC), regarding the Functional Certification for IT security, was organised 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 standard adapted to the necessary requirements to be recognised nationally, according to standard EN45011, and internationally, in accordance with the "**Common Criteria Certificate Recognition Arrangement**" (CCRA) as an ICT security certification entity.

For the Cryptological Certification and TEMPEST Certification, also carried out for Administration systems that are going to handle classified information, the Certification Body uses its own criteria and methodologies.

During 2012, the Certification Body brought out its new website, offering information on different certifications and laboratory accreditations, the reference standard, the forms required to process it and constant updates on certified products.

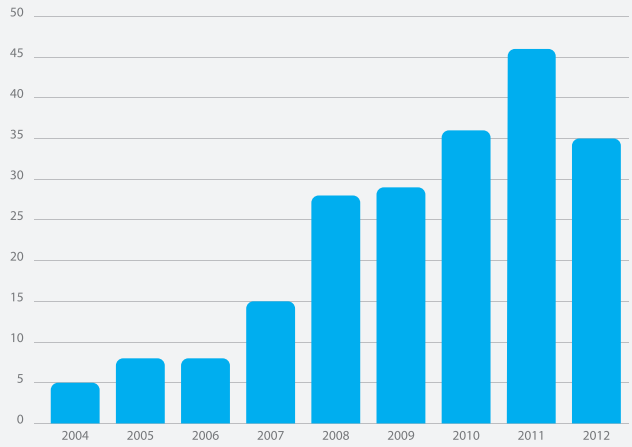
Within the CCRA framework and the SOGIS Agreement, the OC/CCN has continued to participate actively in the different technical and management groups for both agreements. It is also participating in the new version of the CCRA and in the implications that these changes might have in fields such as NATO.

6.1 Certificación funcional

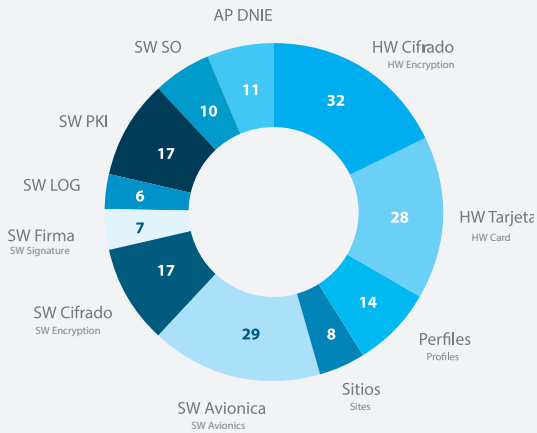
El Organismo de Certificación certifica la **seguridad de productos y sistemas** de Tecnologías de la Información, según lo establecido en el Reglamento anteriormente citado y tras considerar, entre otras pruebas, los informes de evaluación emitidos por los laboratorios acreditados y realizados conforme a los criterios, métodos y normas de evaluación de la seguridad indicados en la Orden ministerial.

El OC/CCN viene operando desde finales del año 2004 con diversas normas de evaluación de la seguridad de las TIC, entre ellas, la de mayor reconocimiento internacional, la denominada **Common Criteria for Information Technology Security Evaluation** (también publicado como norma ISO/IEC15408). De ella se han venido recibiendo y tramitando diversas solicitudes de certificación de productos para su posible uso en la Administración electrónica española. Esta norma define niveles de evaluación entre **EAL1 y EAL7**, siendo el **CCRA** el acuerdo internacional que da cobertura al reconocimiento mutuo de certificados entre los niveles EAL1 a EAL4.

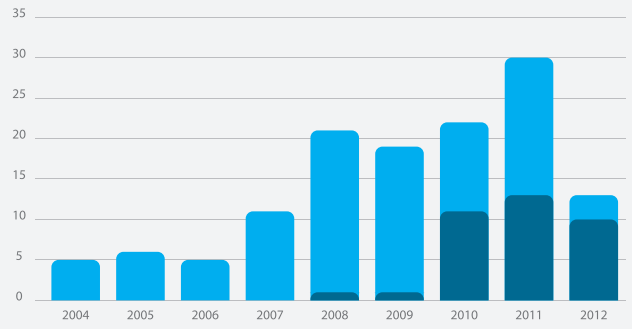
Expedientes de Certificación Funcional
FUNCIONAL CERTIFICATION CASES



Tipos de productos certificados TYPES OF CERTIFIED PRODUCTS

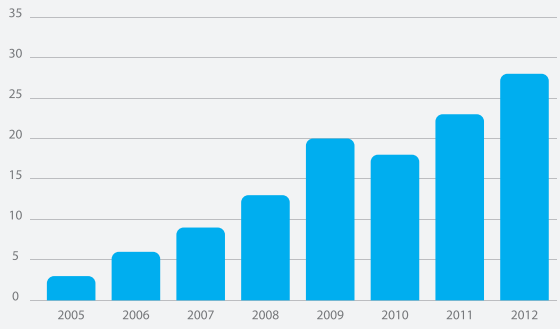


Expedientes de certificación de nuevos productos
NEW PRODUCT CERTIFICATION CASES



ESPAÑOLES/ SPANIISH
EXTRANJEROS/FOREIGN

Resoluciones publicadas en el BOE
RESOLUTIONS PUBLISHED IN THE BOE



6.1 FUNCTIONAL CERTIFICATION

The Certification Body certifies product and system security for information technologies, according to what is established in the aforementioned regulation, and after considering evaluation reports issued by the accredited labs, among other procedure investigation proof, carried out in compliance with the criteria, methods and evaluation rules for security indicated in it.

Since late 2004, the OC/CCN has been operating under a variety of ICT security evaluation rules including the most internationally recognised: Common Criteria for Information Technology Security Evaluation (also published as standard ISO/IEC15408). This has involved receiving and sending out different product certification applications for possible use in Spanish Electronic Administration. This standard defines evaluation levels between EAL1 and EAL7, and CCRA is the international agreement that covers mutual certificate recognition between EAL1 and EAL4 levels. In this respect, during 2011 and 2012, Certifica-

Durante los años 2011 y 2012, el Organismo de Certificación del CCN (OC/CCN) inició 81 expedientes de certificación (entre nuevas solicitudes y mantenimiento o revisión de vigencia de los certificados ya existentes), observándose un descenso en las solicitudes en 2012, sobretodo de productos nacionales.

Esta situación viene motivada por la situación económica y por la falta de una normativa clara que fomente y valore la utilización de productos de seguridad confiables, que hayan sido certificados siguiendo un proceso formal.

Por otra parte, durante los años 2011 y 2012 se han publicado en el Boletín Oficial del Estado, BOE, 49 resoluciones de certificación de productos o sistemas, que habían pasado satisfactoriamente el proceso de evaluación, y tres resoluciones de anulación del certificado de aquellos productos que no han mantenido las condiciones en las que se certificaron. (Ver tabla 1 y tabla 2)

Resoluciones BOE año 2011
BOE RESOLUTIONS 2011

OBJETO A EVALUAR	SOLICITANTE DE LA CERTIFICACIÓN	TIPO RESOLUCIÓN	NÚMERO DE RESOLUCIÓN EN EL BOE
MRTT_MPS-S	EADS-CASA	CERTIFICADO	1A0/38077/2011, de 25 de marzo
MRTT_AS	EADS-CASA	CERTIFICADO	1A0/38078/2011, de 28 de marzo
EP430G	EPICOM	CERTIFICADO	1A0/38255/2011, de 8 de noviembre
TEMD	IGECIS	REVOCADO	1A0/38202/2011, de 12 de julio
PSTmail	AUTEK	CERTIFICADO	1A0/38204/2011, de 14 de julio
HERMES PI3 1.0	SEC.EST.SEGURID AD	CERTIFICADO	1A0/38257/2011, de 14 de noviembre
HERMES ARGOS v1.0	SEC.EST.SEGURIDAD	CERTIFICADO	1A0/38254/2011, de 14 de noviembre
LOGICA 3.0 SP2 PATCH 11	ICA	CERTIFICADO	1A0/38179/2011, de 16 de junio
ERASE-IT CORE	RECOVERY LABS	CERTIFICADO	1A0/38081/2011, de 1 de abril
SECURE AUDIT VAULT v1.3.6	KINAMIK	CERTIFICADO	1A0/38118/2011, de 5 de mayo
PP GROUND SEGMENTS SYSTEM ISSUE B	EADS-CASA	CERTIFICADO	1A0/38116/2011, de 5 de mayo
CGP	HUAWEI	CERTIFICADO	1A0/38199/2011, de 12 de julio
VRP/NETENGINE40ECX600	HUAWEI	CERTIFICADO	1A0/38200/2011, de 12 de juilo
DNI-e CAMBIO PIN	FNMT-RCM	CERTIFICADO	1A0/38079/2011, de 29 de marzo
PP AIRSEGMENT SYSTEM ISSUE B	EADS-CASA	CERTIFICADO	1A0/38117/2011, de 5 de mayo
PP HSM REALIA TECH.	REALIA TECH.	CERTIFICADO	1A0/38181/2011, de 21 de junio
PP APPLIANCE REALIA TECH.	REALIA TECH.	CERTIFICADO	1A0/38180/2011, de 21 de junio
PP SERVICIOS EN RED REALIA TECH.	REALIA TECH.	CERTIFICADO	1A0/38177/2011, de 21 de junio
EF2000 OGSE-IGS 3.1.1	EADS-CASA	CERTIFICADO	1A0/38080/2011, de 1 de abril
EP430D v1.35.34	EPICOM	CERTIFICADO	1A0/38178/2011, de 21 de junio
ADVANTIS CRYPTO v3.1	SERMEPA	REVOCADO	1A0/38201/2011, de 12 de julio
LOGICA 2.1	ICA	REVOCADO	11A0/38256/2011, de 11 de noviembre

tion Body (OC/CCN) started 81 certification cases (including new applications and maintenance or review of validity for existing certificates), noting a drop in applications for new certificates in 2012, above all from national products. This situation is partly caused by the economic situation and partly due to a lack of clear standards to promote and evaluate the use of reliable security products certified following a formal process.

On the other hand, over 2011 and 2012, the BOE (Spanish State Gazette) published 49 certification resolutions for products or systems satisfactorily passing the evaluation process and three resolutions cancelling the certificate for products that had not kept up the conditions for which they had been certified, (as seen in Table 1 and Table 2).

Resoluciones BOE año 2012

BOE RESOLUTIONS 2012

OBJETO A EVALUAR	SOLICITANTE DE LA CERTIFICACIÓN	TIPO RESOLUCIÓN	NÚMERO DE RESOLUCIÓN EN EL BOE
EP1140	EPICOM	CERTIFICADO	9460, de 19 de junio
EF2000 OGSE-IGS 3.1R	EADS-CASA	CERTIFICADO	8498, de 25 de mayo
GBTS	HUAWEI	CERTIFICADO	4642, de 23 de febrero
HERT-BBU	HUAWEI	CERTIFICADO	4643, de 23 de febrero
IMANAGER-M2000	HUAWEI	CERTIFICADO	3063, de 13 de enero
IMAP-OSS	HUAWEI	CERTIFICADO	3062, de 13 de enero
LTE	HUAWEI	CERTIFICADO	3917, de 14 de febrero
MBSC	HUAWEI	CERTIFICADO	5401, de 7 de marzo
WCDMA-NODEB	HUAWEI	CERTIFICADO	5568, de 26 de marzo
WIMAX-DBS3900	HUAWEI	CERTIFICADO	6746, de 3 de abril
EPASSPORT KONA 102 BAC	KEBT	CERTIFICADO	7328, de 17 de abril
SITE REALSEC	REALSEC	CERTIFICADO	9459, de 19 de junio
DISKCRYPT	CASSIDIAN	CERTIFICADO	8911, de 11 de junio
VIRTUAL AIR GAP	ASELSAN	CERTIFICADO	14870, de 13 de noviembre
EPASSPORT KONA 102 EAC	KEBT	CERTIFICADO	7329, de 17 de abril
EPASSPORT KONA 102J1 BAC	KEBT	CERTIFICADO	7330, de 17 de abril
EPASSPORT KONA 102J1 EAC	KEBT	CERTIFICADO	7331, de 17 de abril
ESIGNACRYPTO	INDENOVA, S.L.	CERTIFICADO	13821, de 7 de agosto
CRYPTO.X	INIXA	CERTIFICADO	13820, de 7 de agosto
GSS 4.1 SP	EADS-CASA	REVOCADO	4641, de 22 de febrero
GSS 4.1.1	EADS-CASA	REVOCADO	4641, de 22 de febrero
GSS 5.0 ITALY	EADS-CASA	CERTIFICADO	8203, de 17 de mayo
DRIVER DNIE CARD MODULE V1.0	FNMT-RCM	CERTIFICADO	9459, de 19 de junio
DRIVER DNIE PKCS#11	FNMT-RCM	CERTIFICADO	13822, de 21 de agosto
GSS 4.2	EADS-CASA	REVOCADO	4641, de 22 de febrero
EF2000 OGSE-IGS 3.1R PLUS	EADS-CASA	CERTIFICADO	9457, de 15 de junio
CONTROLADOR JAVA DNIe	MINHAP	CERTIFICADO	13942, de 11 de octubre

6.2 Certificación Criptológica

Como ya se ha señalado, el Centro Criptológico Nacional (CCN) es el organismo responsable de la elaboración del Catálogo de Productos con Certificación Criptológica que incluye los productos capaces de proteger la **información nacional clasificada**. De esta forma, tiene la consideración de cifrador nacional, con certificación criptológica, aquel equipo de cifra que ha sido evaluado y ha obtenido dicha certificación del CCN. Se dispone de distintos tipos de cifradores: IP, de datos, voz, fax, PKI, generadores de números aleatorios, centros de gestión, etc.

Durante el año 2012 se modificó la guía **CCN-STIC-103 "Catálogo de Productos con Certificación Criptológica"** para incluir sólo información clasificada hasta el grado DIFUSIÓN LIMITADA.

En cuanto a la evaluación y certificación criptológica durante los años 2011 y 2012 se realizaron las siguientes actividades:

- Cifrador IP EP430GN. Evaluado y certificado por el CCN en 2011 (como ya se ha indicado en el apartado de Investigación y Desarrollo de Productos) para, ya a principios del año 2013, haber sido el primer equipo de cifra nacional aprobado (de forma interina) por el Comité Militar de la OTAN.

- Cifrador CRIPTOPER SCAP PROCIF PARA IRIDIUM
  Durante el año 2012, se ha llevado a cabo la reevaluación y certificación de tres nuevas versiones del cifrador personal de voz y datos para su uso sobre los satélites Iridium debido a las solicitudes de nuevas funcionalidades solicitadas por OTAN.

  Hay que señalar que este cifrador es el primer cifrador operativo y desplegado con el nuevo protocolo de interoperabilidad de la OTAN (SCIP), así como el primer producto de cifra nacional que ha sido vendido a OTAN.

- Centro de gestión CRIPTOPER CMAP PROCIF PARA IRIDIUM
  Durante el año 2012 se ha llevado a cabo la reevaluación de dos nuevas versiones del Centro de Gestión de los cifradores CRIPTOPER SCAP para Iridium.

- Cifrador CRYPTO TOKEN USB
  Se ha revisado y certificado la nueva versión del cifrador de datos sin conexión a redes Crypto Token USB. Esta nueva versión es compatible con los sistemas operativos Windows Vista y Windows 7.

- GSMSEC v 2.10 Crypto 3.20 D gpp.
  El dispositivo de comunicaciones móviles seguras de voz sobre sistema de telefonía móvil GSM ha sido reevaluado por parte del CCN debido a un cambio en la versión del firmware del mismo.

6.2 CRYPTOLOGICAL CERTIFICATION

As previously mentioned, the National Cryptologic Centre (CCN) is the organisation responsible for drawing up the Catalogue of Products with Cryptological Certification, including products capable of protecting classified national information. Consequently, any equipment that has been evaluated and has obtained this certificate from the CCN is considered to be a national encryption devices, with cryptological certification. Encryption devices come in many guises: IP, data, voice, fax, PKI, random number generators, management centres, etc.

During 2012, the **CCN-STIC-103** guide "**Catalogue of Products with Cryptological Certification**" was modified to only include information classified to the degree of LIMITED DISTRIBUTION.

Regarding evaluation and certification during 2011 and 2012, the following activities were carried out:

- IP EP430GN encryption devices. Evaluated and certified by the CCN in 2011 (as previously mentioned in the Product Research and Development section) to later be evaluated by SECAN, in May 2013 it became the first national encrypting equipment to be approved by the NATO Military Committee to process classified NATO information.

- CRIPTOPER SCAP PROCIF FOR IRIDIUM encryption devices. During 2012, three new versions of the personal voice and data encryption devices were reassessed and certified for use on Iridium satellites due to NATO applications for new functional features. It should be mentioned that this encryption devices is the first encryption devices to be operated and deployed with the new NATO interoperability protocol (SCIP), plus the first national encryption devices product that has been sold to NATO.

- CRIPTOPER CMAP PROCIF FOR IRIDIUM management centre. During 2012, two new versions of the CRIPTOPER SCAP for Iridium encryptors' Management Centre were reassessed.

- CRYPTO TOKEN USB encryption devices. The new version of the data encryption devices with no connection to Crypto Token USB networks has been reviewed and certified. This new version is compatible with Windows Vista and Windows 7 operating systems.

- GSMSEC v 2.10 Crypto 3.20 D gpp. The secure voice mobile communications device on GSM mobile phone system has been reassessed

6.3 Certificación TEMPEST

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, actuando en todos ellos como Autoridad TEMPEST Nacional (NTA).

En julio de 2012 se publicó la Guía CCN-STIC 210 que recoge la norma **TEMPEST** de aplicación para la información nacional clasificada CONFIDENCIAL o superior. Por tanto, afecta a equipos, sistemas e instalaciones, tanto fijas como móviles en las que se genera o procesa esta información. Dicha normativa es compatible con la equivalente en OTAN o UE.

Respecto a evaluación de la seguridad de las emanaciones de los sistemas que procesan información clasificada (TEMPEST) y las instalaciones donde están ubicados, en los dos últimos años se realizaron las siguientes actividades:

En julio de 2012 se publicó la Guía CCN-STIC 210 que recoge la norma **TEMPEST** de aplicación para la información nacional clasificada CONFIDENCIAL o superior. Por tanto, afecta a equipos, sistemas e instalaciones, tanto fijas como móviles en las que se genera o procesa esta información. Dicha normativa es compatible con la equivalente en OTAN o UE.

6.3 TEMPEST CERTIFICATION

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 guard against these compromising emanations.

The CCN's many assignments, as the Certification Authority for ICT security in the EMSEC field (Emanations Security), include developing a national standard in this field, assessment 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).

In July 2012, the CCN-STIC 210 guide was published compiling the applicable TEMPEST standard for national information classified as CONFIDENTIAL or higher. Therefore, this affects equipment, systems and facilities, both fixed and mobile, where this information is generated or processed. This standard is compatible with its equivalent in NATO or the EU.

Regarding the security evaluation of the emanations from systems that process classified information (TEMPEST) and facilities where they are located, over the last two years the following activities have been carried out:

Certificación ZONING de locales:

La actividad de certificación ZONING de locales por parte del CCN ha aumentado ligeramente respecto a años anteriores habiéndose llegado a ejecutar un total de 10 expedientes de certificación. Estos expedientes han correspondido tanto a empresas como a organismos de la Administración Pública.

Certificación ZONING/TEMPEST de equipos y sistemas:

La actividad se ha centrado principalmente en la evaluación TEMPEST del cifrador IP EP-430GN como parte del proceso necesario para su aceptación por SECAN como cifrador para OTAN, de la última versión de CRIPTOPER que permite el envío de mensajes cifrados y del sistema de gestión de audio AMS de TECNOBIT para el A400M.

A400M

The CCN-STIC 210 guide was published in July 2012 compiling the applicable TEMPEST standard for national information classified as CONFIDENTIAL or higher. Therefore, this affects both fixed and mobile equipment, systems and facilities where this information is generated or processed. This standard is compatible with its equivalent in NATO or the EU

ZONING certification for premises

CCN ZONING certification for premises has increased slighted on previous years, reaching a total of 10 certification cases. These cases involve both companies and public administration organisations.

ZONING/TEMPEST certification for equipment and systems

The activity has mainly focussed on TEMPEST evaluation for the IP EP-430GN encryption device (as part of the necessary SECAN acceptance process as a NATO encryption device), the latest version of CRIPTOPER to send encrypted messages and the AMS audio management system by TECNOBIT for the A400M.

7 Acuerdos y colaboraciones

Para el óptimo desempeño de todas sus funciones, el Centro Criptológico Nacional ha venido estableciendo las necesarias relaciones y firmado los acuerdos pertinentes a lo largo de sus diez años de funcionamiento, tanto en el ámbito nacional como en el internacional. Así, en el plano nacional, es miembro o ha colaborado con:

Ministerio de Hacienda y Administraciones Públicas / Ministry of Inland Revenue and Public Administrations

- Consejo Superior de Administración Electrónica (CSAE) / Higher Council for Electronic Administration.
- Comisión Permanente del Consejo Superior para la Administración Electrónica y sus grupos dependientes (CPCSAE) / Higher Council for Electronic Administration Permanent Commission and its dependent groups.
- Acuerdo con el Instituto Nacional de Administración Pública (INAP) y 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 / Agreement with the National Public Administration Institute (INAP) and Secretary of State for Public Function to boost security in the field of Electronic Administration. This agreement includes developing the National Security Framework.
- Grupos de trabajo sobre comunicaciones electrónicas seguras; transposición de la directiva europea de medios de pago (SEPA), identificación y autenticación y servicios WEB de la Administración / Working groups on secure electronic communications; transposition of the European Directive on payment methods (SEPA), identification and authentication of Administration internet services.
- Grupo de Trabajo del Esquema Nacional Seguridad / National Security Framework Working groups.
- Grupo de Trabajo de Seguridad del Comité Sectorial de la Administración Electrónica (CCAA) / Electronic Administration Sector-Based Committee Security Working groups (regions).

AGREEMENTS AND JOINT PROJECTS

For optimum deployment of all its functions, the National Cryptologic Centre has been establishing the necessary relationships and signed relevant agreements over its ten years in operation, both nationally and internationally. So, nationally, it is a member or has worked with the following:

Ministerio de Defensa / Ministry of Defence

- Grupo de Trabajo sobre Seguridad de la Información y sobre cifra del Comité CIS de las Fuerzas Armadas (COMCISFAS) / Working groups on Information Security and on encrypting for the Armed Forces CIS Committee (COMCISFAS).
- Grupo Técnico C3 OTAN / NATO C3 Technical Group.
- Grupo de Trabajo de Apoyo al Sistema de Mando y Control Militar / Military Command and Control System Support Working groups.
- Grupo de Trabajo sobre Comunicaciones Tácticas / Working Group on Tactical Communications.
- Jornadas INFOSEC del EMAD y de Equipos de Inspección / INFOSEC workshop from the EMAD and Inspection teams.
- Coalition Warrior Interoperability Demonstration (CWID) Nacional: Demostraciones de tecnologías de carácter militar organizadas anualmente / Coalition Warrior Interoperability Demonstration (CWID) National Military technology demonstrations organised every year.

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Ministerio del Interior / Home Office

- Grupo de Trabajo sobre DNI electrónico con la Dirección General de la Policía / Working Group on electronic identity documents with the General Police Board.
- Grupo de Trabajo de Infraestructuras Críticas con la Secretaría de Estado de Seguridad /

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

Ministerio de Industria Turismo y Comercio / Spanish Ministry of Industry, Tourism and Trade

- Grupos de trabajo de los proyecto Rescata, Seguridad y Confianza, usabilidad del DNIe / Working Group for the Rescue, Security and Trust project, using DNIe (electronic ID cards)

dni electrónico

GOBIERNO DE ESPAÑA MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Resto de organismos / Other agencies

- Federación Española de Municipios y Provincias: Acuerdo de colaboración en materia de seguridad de la Información en los entidades locales) / Spanish Towns and Provinces Federation: Joint work agreement in information security in local entities.
- Miembro de CSIRTes: grupo de trabajo CERT nacionales / Member of CSIRTes: national CERT Working Group.
- Junta de Castilla y León: asistencia a conferencias y apoyo a su centro de operaciones de seguridad / Castilla y León government: attending conferences and support for its security operations centre.
- Generalitat Valenciana: Convenio firmado y apoyo al CSIRT-CV / Valencia Government. Agreement signed and support for the CSIRT-CV.
- Generalitat de Catalunya: Firma de convenio de colaboración y apoyo al CESICAT (Centro de Seguridad) / Catalonia Government: Agreement signed for joint projects and support for the CESICAT (Security Centre).
- Junta de Andalucía: Convenio de colaboración para el Impulso de la Sociedad de la Información y apoyo al Andalucía-CERT / Andalusia Regional Government: Joint work agreement to drive the information.
- Junta de Extremadura y Gobiernos de Aragón, Canarias, Principado de Asturias, Juntas de Comunidades de Castilla-La Mancha: Adhesión al Servicio de Alerta Temprana, SAT, del CCN-CERT / Extremadura Regional Government and governments from Aragon, Canary Islands, Principality of Asturias, Castilla-La Mancha: Joining the Early Warning System (SAT) from the CCN-CERT.
- AENOR: Subcomités de seguridad TIC e identificación biométrica / AENOR: ICT security sub-committees and biometric identification.
- Foro ABUSES: Grupo de Trabajo con Proveedores de Servicio de Internet (ISP) / ABUSES Forum: ISP vendors workshop.

Ámbito empresarial / Business field

- 52 empresas de sectores estratégicos (defensa, aeronautico, TIC, energético y financiero) / 52 etrategic sector companies (defense, aeronautical, ICT, energy and financial).

- Medios de comunicación / Media:
  Artículos y colaboraciones en: Revista SIC, Red Seguridad, Unidad Editorial, Fundación SOCINFO, Fundación DINTEL, Revista Seguridad Total, Revista Española de Defensa y Congreso Nacional de Interoperabilidad y Seguridad / Articles and contributions in: SIC journal, Red Seguridad, Unidad Editorial, SOCINFO Foundation, DINTEL Foundation, Seguridad Total journal, Spanish Defence Journal and National Interoperability and Security Congress.

Jornadas / Workshops

- SID (Seguridad de la Información en Defensa) / Information Security in Defence (Ministry of Defence) .
- ENISE (Encuentro Nacional de la Industria de Seguridad en España) / ENISE (National Security Industry Meeting in Spain).
- Conferencias ESTAER (Escuela de Técnicas Aeronáuticas del Ejército del Aire) / ESTAER conferences (Air Force Aeronautical Technique School).
- Conferencias EMACOT (Escuela de Técnicas de Mando, Control y Telecomunicaciones) / EMACOT conferences (Command, Control and Telecommunications Technique School).
- Fundación Círculo de Tecnologías de Defensa / Defence Technologies Circular Foundation.
- Cursos de verano MADOC (Mando de Adiestramiento y Doctrina del Jefe de Estado Mayor del Ejército) / MADOC summer courses (Drilling Command and Army Doctrine).
- CNIS: Congreso Nacional de Interoperabilidad y Seguridad / CNIS: National Interoperability and Security Congress.
- RAI (Real Academia de Ingeniería) / RAI (Royal Engineering Academy).
- Congreso Securmática (Revista SIC) / Securmatica Congress.
- Seminarios Fundación SOCINFO / SOCINFO Fundation Seminaries.
- Seminarios Fundación DINTEL / DINTEL Fundation Seminaries.

7.1 Internacional

En cuanto al ámbito internacional, el Centro Criptológico Nacional está presente o mantiene una estrecha relación con:

7.1 INTERNACIONAL

As far as the international field is concerned, the National Cryptologic Centre is present or maintains a close relationship with:

Unión Europea / European Union

- Comité INFOSEC del Consejo de la Unión Europea / INFOSEC committee from the European Union Council
- Panel de Acreditación conjunto de la UE / EU joint accreditation panel
- Paneles TEMPEST de la UE / EU TEMPEST panels
- Colaboración en la preparación de la Estrategia Europea de Ciberseguridad / Joint work in preparing the European Cybersecurity Strategy
- ENISA (European Network&Information Security Agency) / ENISA (European Network&Information Security Agency)

CERT

- FIRST (Forum of Incident Response and Security Teams).
- TF-CSIRT (Terena Forum Computer Security Incident Response Teams).
- EGC Group (European Goverment CERT Group).
- CERT/CC (CERT Coordination Center).
- APWG (Anti-Phishing Working Group).
- Comité INFOSEC del Consejo de la Unión Europea / Council of the European Union - INFOSEC Committee.

Ejercicios / Exercises

- International Cyber Defence Exercise Locked Shields 2012 (NATO CCD COE).
- NATO CMX Crisis Management Exercise 2012.
- NATO annual exercise Cyber Coalition (CC).
- Participación en el ejercicio de ciberseguridad e infraestructuras críticas: UE-Estados Unidos: Cyber Atlantic 2011 / Participation in the cybersecurity exercise and critical infrastructures: EU-United States: Cyber Atlantic 2011.
- Ejercicio Paneuropeo de Ciberseguridad, Ciber Europe 2012, Pan-European Cyber Security Exercise, Cyber Europe 2012.

OTAN / NATO

- Grupo de Trabajo de Respuesta a Incidentes de OTAN – NCIRC. Además se firmó en 2012 un Memorándum de Entendimiento para la cooperación en ciberdefensa / NATO Incident Response Group - NCIRC A cyber-defence cooperation Memorandum of Understanding was also signed in 2012.
- S/C4 Information Assurance & Cyber Defence y sus grupos de trabajo asociados.
- Paneles de Acreditación / Accreditation Panels.
- Grupo de trabajo sobre Information Assurance del Comité de Seguridad (AC/35 – WG/1).
- NATO Security Risk Assessment Group (Análisis de Riesgos de OTAN).
- NIAS2012 (NATO Information Assurance Symposium).
- NISWG (Networking and Information Infraestructure Working Group).
- NINE (Networkin Internet Protocol Network Encryption).
- ISpec (Interoperability Specification) Working Group.
- NINE TC (NINE Technical Characteristics Syndicate).
- Grupos de Trabajo sobre Interoperabilidad Cripto: SCIP TF (Secure Communications Interoperability Protocol Task Force), NSG (NINE Steering Group), NCITF (NATO Crypto Interoperability Task Force).
- Grupo de Expertos en Ciberseguridad / Cybersecurity Expert Groups.
- International Interoperability Control Working Group IICWG.
- STWG (Security Technical Working Group) de OCCAR: SRD (Software Defined Radio) dentro del programa ESSOR / inside ESSOR program.

Multinacional/ Multinational

- Programa A400M: Diferentes paneles del avión europeo de transporte A400 / Different accreditation panels, European transport plane comsec A400/M.
- EF2000: Diferentes grupos del EF2000/TCG (Grupo TEMPEST-COMSEC) / Different groups from the EF2000/TCG.
- ESA: Comité INFOSEC para la protección de Información Clasificada de los sistemas de la Agencia Europea del Espacio / ESA INFOSEC committee to protect European Space Agency systems' Classified Information.
- GALILEO: Diferentes comités y paneles de seguridad / Different committees and security panels.
- Common Criteria Recognition Arrangement (CCRA) y sus grupos de trabajo asociados.
- SOGIS MRA (Senior Officials Group Information Systems Security).

8 Cronología

2011

Enero

- Informe de Ciberamenazas 2010 y Tendencias 2011.

Febrero

- II Jornadas del Sistema de Alerta Temprana en Internet del CCN-CERT, en las dependencias del Centro Criptológico Nacional.
- Nueva versión de las Guías CCN-STIC: "Seguridad en Proxies" (660).
- Realización y publicación de distintas Guías del Esquema Nacional de Seguridad:
  - "Glosario de términos y abreviaturas del ENS" (800)
  - "Responsabilidades y Funciones en el ENS" (801)
  - "Valoración de Sistemas en el ENS" (803)
  - "Plan de Adecuación del ENS" (806)

Marzo

- Nuevas versiones de las Guías CCN-STIC: "Baja y Destrucción de material criptológico" (304), " Evaluación de Parámetros de Rendimiento en Dispositivos Biométricos" (492), "Sistemas de Gestión de Red (Cisco WorksLMS)" (645) "Seguridad en Firewalls de Aplicación" (661).
- Publicada la nueva Guía CCN-STIC: "Manual de la Herramienta de Análisis de Riesgos μPILAR" (473A).

Abril

- Nuevas versiones de las Guías CCN-STIC: "Seguridad en WMAX" (444), "Seguridad en Windows Mobile 6.1" (451) y "Seguridad en Windows Mobile 6.5" (452).
- Cursos de Especialización en Seguridad: Curso de Inspecciones de Seguridad.
- Cursos Básicos de Seguridad: Base de datos e ingeniería de Red.

CRONOLOGY

8.1 2011

JANUARY

- 2010 Cyber Threat and 2011 Trends report

FEBRUARY

- 2nd Workshop on the CCN-CERT Internet Early Warning System, in National Cryptologic Centre dependencies.
- New version of CCN-STIC guides: "Security in Proxies" (660).
- Different National Security Framework Guides produced and published:
  - "NSF glossary of terms and abbreviations"(800)
  - "Responsibilities and Functions in the NSF" (801)
  - "Systems Assessment in the NSF" (803)
  - "NSF Adaptation Plan" (806)

MARCH

- New versions of CCN-STIC Guides: "Cancellation and Destruction of cryptological material" (304), "Evaluation of Performance Parameters in Biometric Devices" (492), "Network Management Systems (Cisco WorksLMS)" (645) "Security in Applicable Firewalls" (661).
- New CCN-STIC guide published: "Risk Analysis Tool Manual μPILAR" (473A)

APRIL

- Basic Security Courses: Database and Network Infrastructure
- Security Specialisation Courses: Security Inspections Course
- New versions of CCN-STIC Guides: "Security in WMAX" (444), "Security in Windows Mobile 6.1" (451) and "Security in Windows Mobile 6.5" (452).

MAY

- First Course on Security in Mobile Devices
- New CCN-STIC guide: "Risk Analysis Tool Manual PILAR 5.1" (470D)

JUNE

- New version of the "Security in Windows 7" guide (customer in domain). (522A).
- BOE published functional certification for five new products (see page 47)

JULY

- CNI agreement with the Secretary of State for Public Function from the Ministry of Territorial and Public Administration Policy and the National Public Administration Institute (INAP) to boost security in the field of Electronic Administration.
- Four new products obtained functional certification (published in the BOE this month)

Mayo

- Primer Curso de Seguridad en Dispositivos Móviles.
- Nueva Guía CCN-STIC: "Manual de la Herramienta de Análisis de Riesgos PILAR 5.1"" (470D).

Junio

- Nueva versión de la Guía "Seguridad en Windows 7" (cliente en dominio). (522A)
- Publicada en el BOE la Certificación funcional de cinco nuevos productos (véase página 47).

Julio

- Convenio del CNI, la secretaria de Estado para la Función Pública del Ministerio de Política Territorial y Administración Pública y del Instituto Nacional de Administración Pública (INAP) para impulsar la seguridad en el ámbito de la Administración Electrónica.
- Cuatro nuevos productos obtienen la Certificación funcional (publicado en el BOE en este mes).

Agosto

- Nuevas Guías CCN-STIC: "Manual de Usuario de RMAT 5.1"" (471C), "Seguridad en Servicio de Correo en el ENS" (814) Borrador y "Recomendaciones de Empleo de la Herramienta Nessus" (952).

Septiembre

- Nuevas Guías CCN-STIC: "Esteganografía" (438), "Política de Seguridad de la Información" (805) y "Verificación del Cumplimiento de las Medidas en el ENS" (808). Borrador.
- XXIII Curso de Especialidades Criptológicas impartido por el CCN.

Octubre

- Convenido de colaboración con Centre de Seguretat de la Informació de Catalunya (CESICAT) para impulsar los aspectos de seguridad dentro del desarrollo de la Sociedad de la Información.
- Firma de un acuerdo entre CNI-CCN y **Microsoft** para reafirmar su compromiso de colaboración en materia de ciberseguridad.

Firma del acuerdo entre CNI-CCN y Microsoft. 6 de octubre de 2011
SIGN OF AN AGREEMENT BETWEEN CNI-CCN AND MICROSOFT. OCTOBER 2011

AUGUST

- New CCN-STIC guides: "RMAT 5.1 User Manual" (471C), "Security in Mail Service in the NSF" (814) Draft and "Recommendations for Using the Nessus Tool" (952)

SEPTIEMBRE

- New CCN-STIC guides: "Steganography" (438), "Information Security Policy" (805) and "Verification of Measure Compliance in the NSF" (808). Draft
- 23rd Cryptological Specialities Course (CEC), given by CCN

OCTOBER

- Joint work agreement with the Centre de Seguretat de la Informació de Catalunya (CESICAT) to work on security aspects within Information Society development.
- CNI-CCN signed an agreement with Microsoft to restate its commitment to work together on cybersecurity issues.

- Nueva versión de **MAGERIT** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT v3)) elaborada por el Consejo Superior de Administración Electrónica (CSAE).

- Nueva Guía CCN-STIC: "Seguridad en Servicios Web en el ENS". (812).

Noviembre

- El CCN-CERT participa en en el primer ejercicio conjunto de ciberseguridad entre la UE y EEUU, **Cyber Atlantic 2011**. El encuentro fue auspiciado por ENISA y por el DHS estadounidense y contó con la participación de 20 Estados.

- Nueva versión de la Guía CCN-STIC: "Medidas de protección TEMPEST para instalaciones" (154).

Diciembre

- V Jornadas STIC CCN-CERT celebradas en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), en Madrid, inauguradas por la Secretaría General del CNI, Elena Sánchez Blanco.

- El CNI pasa a estar adscrito al Ministerio de la Presidencia.

- Publicación de los Informes de Amenazas CCN-CERT: Análisis de WhastApp (Android). Vulnerabilidades y "Bitcoin y la descentralización".

Elena Sánchez Blanco, secretaria general del CNI durante las V Jornadas STIC CCN-CERT de diciembre de 2011

CNI GENERAL SECRETARY DURING THE 5TH STIC CCN-CERT WORKSHOP DECEMBER 2011

- New version of MAGERIT (Risk Analysis and Management Methodology for Information Systems (MAGERIT v3), drawn up by the Higher Council for Electronic Administration (CSAE).
- New CCN-STIC guide: "Security in internet services in the NSF". (812).

NOVEMBER

- The CCN-CERT participated in the first joint cybersecurity exercise between the EU and the USA, Cyber Atlantic 2011. The meeting was brought about by ENISA and US DHS. 20 states participated.
- New version of CCN-STIC guide: "TEMPEST protection measures for facilities" (154)

DECEMBER

- 5th STIC CCN-CERT Workshop held at the National Defence Higher Studies Centre (CESEDEN), in Madrid, inaugurated by the CNI General Secretary, Elena Sánchez Blanco
- The CNI became part of the Ministry of the President's Office
- Publication of CCN-CERT Threat Reports: Analysis of WhatsApp (Android). Vulnerabilities and "Bitcoin and decentralisation".

2012

Enero

- Realización de auditorías de seguridad a los servicios Web de 17 organismos de la Administración General.
- Informe implantación ENS en la Administración General del Estado

Febrero

- Informe de Ciberamenazas 2011 y Tendencias 2012.
- IX Curso de Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC), con fase on-line y presencial.
- III Jornadas del Sistema de Alerta Temprana en Internet del CCN-CERT, en las dependencias del Centro Criptológico Nacional y con la asistencia de administraciones públicas y empresas estratégicas.
- Nuevas versiones de las Guías CCN-STIC: "Medidas de protección TEMPEST para instalaciones" (154), "Algoritmos y Parámetros de Firma Electrónica" (405) y "Seguridad en Windows 2008 Server. Servidor de Ficheros " (523)

Marzo

- Nueva versión de las Guías CCN-STIC: Seguridad de las TIC en la Administración (001) y Coordinación Criptológica (002).
- Se encarga al CCN la coordinación y elaboración, junto con otros organismos, de un borrador de la Estrategia Española de Ciberseguridad.

Abril

- Nueva Guía CCN-STIC "Indicadores y Métricas en el ENS" (815).
- Nueva versión de la Herramienta PILAR (5.2) que cuenta con unos módulos de cumplimiento del Esquema Nacional de Seguridad.
- Participación del CCN-CERT en el ejercicio de ciberdefensa Locked Shields 2012 del CCD COE (NATO Cooperative Cyber Defence Centre of Excellence) en Tallin Estonia.

8.2 2012

JANUARY

- Security audits were performed on internet services from 17 Central Administration organisations.
- Report on NSF implantation in the General State Administration

FABRUARY

- 2011 Cyber Threat and 2012 Trends report
- 3rd Workshop on the CCN-CERT Internet Early Warning System in National Cryptologic Centre dependencies, attended by public administrations and strategic companies.
- New versions of CCN-STIC Guides: "TEMPEST protection measures for facilities" (154), "Algorithms and Parameters for electronic signature" (405) and "Security in Windows 2008 Server. File Server" (523)

MARCH

- New version of CCN-STIC guides: ICT Security in Administration (001) and Cryptological Coordination (002).
- The CCN was commissioned to coordinate and draw up a draft of the Spanish Cybersecurity Strategy alongside other organisations.
- International Cyber Defence Exercise Locked Shields 2012

APRIL

- New CCN-STIC Guide "Indicators and Metrics in the NSF" (815)
- New version of the PILAR Tool (5.2) with compliance modules from the National Security Framework.

Mayo

- Encuentro Internacional del grupo de trabajo IICWG de Interoperabilidad entre Equipos de Cifra, organizado por el Centro Criptológico Nacional en Toledo, cuyo objetivo es definir las especificaciones del protocolo SCIP (Secure Communications Interoperability Protocol) para conseguir la interoperabilidad de la nueva generación de productos de cifra de la OTAN.

- III Cursos STIC de Herramienta PILAR (fase online y presencial).

Junio

- Nuevo portal web del Organismo de Certificación, del Centro Criptológico Nacional (www.oc.ccn.cni.es), en el que, entre otras novedades, se incluye un listado en continua actualización de todos los productos y sistemas certificados por el OC.

Julio

- Nueva versión de la Guía CCN-STIC: "Norma de Seguridad de las Emanaciones TEMPEST" (210).

- Publicadas las nuevas Guías CCN-STIC: "Manual de la Herramienta de Análisis de Riesgos PILAR 5.2" (470E1), "Manual de la Herramienta de Análisis de Riesgos PILAR 5.2 Análisis del Impacto y Continuidad de Negocio" (470E2) y "Manual de la Herramienta de Análisis de Riesgos µPILAR 5.2" (473B).

Agosto

- La Junta de Extremadura primera autonomía en incorporarse al Servicio de Alerta Temprana (SAT) del CCN-CERT.

- Nueva versión de la Guía CCN-STIC: "Colocación de Etiquetas de Seguridad" (409).

- Publicadas las nuevasGuías CCN-STIC: "Gestión de Incidentes de Seguridad en el ENS" (817) y "Recomendaciones de Empleo de la Herramienta Nmap" (954).

MAY

- International meeting of the IICWG working group on Interoperability among Encryption Equipment, organised by the National Cryptologic Centre, aiming to define SCIP protocol specifications (Secure Communications Interoperability Protocol) to get interoperability for NATO's new generation of encryption products.
- 3rd STIC Courses on the PILAR Tool (online and classroom phase)

JUNE

- New Certification Body website from the National Cryptologic Centre (www.oc.ccn.cni.es), with important new features.
- The BOE published the Functional Certification of five new products (see page 48)

JULY

- New version of CCN-STIC guide: "TEMPEST Emanations Security Standard" (210).
- New CCN-STIC guides published: "Risk Analysis Tool Manual PILAR 5.2" (470E1), "Risk Analysis Tool Manual PILAR 5.2 Analysis of Impact and Business Continuity" (470E2) and "Risk Analysis Tool Manual µPILAR 5.2" (473B.August

AUGUST

- Extremadura Regional Government became the first region to include the CCN-CERT Early Warning Service (SAT).
- New version of CCN-STIC guide: "Placing Security Labels" (409).
- Publishing new CCN-STIC guides: "Security Incident Management in the NSF" (817) and "Nmap Tool Employment Recommendations"(954)

Septiembre

- El CCN-CERT abre un perfil en Linkedin, primera red social en el ámbito profesional.
- IX Cursos de Gestión STIC-Implantación del ENS.

Octubre

- Participación del CCN-CERT en el Ejercicio Paneuropeo de Ciberseguridad, Ciber Europe 2012, promovido y organizado por los Estados miembros de la Unión Europea y los países de la Asociación Europea de Libre Cambio (AELC).
- Publicada la nueva Guía CCN-STIC: "Ejemplos de Procedimientos de Seguridad" (821).
- Participación del CCN-CERT en el ejercicio de gestión de crisis de la OTAN CMX 2012 (Crisis Management exercise).
- Participación del CCN-CERT en el ejercicio de ciberdefensa de la OTAN Cyber Coaliittion 2012.

Noviembre

- Nueva versión de la Guía CCN-STIC: "Seguridad en Apache Traffic Server" (662).
- Publicada las nueva Guía CCN-STIC: "Informe del Estado de Seguridad" (824).

Diciembre

- Firma de un Memorándum de Entendimiento entre el CCN-CERT y el NATO Cyber Defence Management Board para la cooperación en ciberdefensa.

NCIRC
NATO
COMPUTER INCIDENT
RESPONSE CAPABILITY

- VI Jornadas STIC CCN-CERT inauguradas por el secretario de Estado director del CNI, Félix Sanz Roldán, en la Fábrica Nacional de la Moneda y Timbre. Las Jornadas contaron con la asistencia de 500 personas de la Administración Pública y empresas estratégicas.

SEPTIEMBRE

- The CCN-CERT set up a profile in Linkedin, top social network in the professional field.
- 9th STIC Management Courses - NSF Implantation

OCTOBER

- CCN-CERT participation in the Pan-European Cybersecurity Exercise, Cyber Europe 2012, promoted and organised by European Union member states and countries from the Free Change European Association (AELC).
- New CCN-STIC guide published: "Examples of Security Procedures" (821)

NOVEMBER

- New version of CCN-STIC guide: "Security in Apache Traffic Server" (662).
- New CCN-STIC guide is published: "State Security Report" (824)

DECEMBER

- Signing the Memorandum of Understanding between the CCN-CERT and NATO Cyber Defence Management Board for cooperation in cyber-defence
- 6th STIC CCN-CERT workshop inaugurated by the Secretary of State-CNI Director, Félix Sanz Roldán, at the National Mint. The Workshop was attended by 500 people from Public Administration and strategic companies.

VI Jornadas STIC CCN-CERT, diciembre 2012
VI JORNADAS STIC CCN-CERT

Edita: Centro Criptológico Nacional
Edit: National Cryptologic Centre

Diseño: Incita Security
Design: Incita Security

Fotografía: Centro Criptológico Nacional
Photography: National Cryptologic Centre

D.L. 198979 - 2013