La seguridad en las TICs en las Administraciones Públicas

CCN-CERT pieza clave para garantizar el mantenimiento de la seguridad en las administraciones.

El **CCN-CERT, CERT Gubernamental (http:/www.ccn-cert.cni.es)**, perteneciente al Centro Criptológico Nacional, es el centro responsable de garantizar la seguridad de las Tecnologías de la Información y las Comunicaciones en la Administración, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.

Para dar cumplimiento a esta labor ha desarrollado diferentes servicios para prestar apoyo a las Administraciones Públicas:

- **Guías CCN-STIC – www.ccn-cert.cni.es/series**: a 31 de diciembre de 2012 existían **197 documentos** enmarcados en esta serie, con normas, procedimientos y directrices técnicas para optimizar la seguridad TIC.

- **Herramienta PILAR** (Procedimiento Informático Lógico para el Análisis de Riesgos) - **www.ccn-cert.cni.es**, cuya última versión, la 5.2, gratuita para el personal de la Administración, se presentó en 2012.

- **Formación en seguridad TIC:** en 2012 se desarrollaron 14 cursos presenciales, con 900 horas lectivas, asistiendo 500 alumnos de las distintas administraciones públicas. Además se ofrecieron seis cursos online, a través del portal www.ccn-cert.cni.es

	2010	2011	2012
Nº de alumnos inscritos	891	1.511	1.887
Nº de acceso a los cursos	5430	13.876	11.735

Ilustración 1. Evolución de los cursos online en seguridad TIC

También corresponde al **CCN-CERT, CERT Gubernamental,** la capacidad de prevención, detección, análisis, respuesta y coordinación ante las ciberamenazas sufridas por las Administraciones Públicas y los sistemas clasificados.

El Sistema de alerta temprana – SAT (www.ccn-cert.cni.es/sat) cuenta con dos opciones con un denominador común: la detección temprana de intrusiones y ciberataques.

- **SAT SARA.** Realiza la detección en tiempo real de ataques y amenazas llevada a cabo después del análisis y correlación del tráfico de red que circula entre las redes de los organismos de las Administraciones Públicas conectados a la red SARA. El servicio está desarrollado en colaboración con el Ministerio de Hacienda y Administraciones Públicas.
  Al término del año 2012, disponían de este servicio **51 organismos públicos** (incluyendo la totalidad de Ministerios, Comunidades Autónomas y otros organismos de la Administración). En total, en el año 2012 se notificaron **430 incidentes** mediante este sistema**,** frente a los 322 del ejercicio anterior.
- **SAT de INTERNET**. El SAT INET consiste en 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. A 31 de diciembre de 2012, 44 organismos públicos y algunas empresas estratégicas estaban adscritos al Sistema (entre ellos algunas Comunidades Autónomas). A través de este servicio se gestionaron en 2012 un total de **3.363 incidentes de ciberseguridad.**

Durante el año 2012, el CCN-CERT, a través de sus distintas fuentes de notificación (Servicios SAT, herramienta CARMEN, Portal Web…), gestionó **4.003 ciberincidentes** (frente a los 2.253 de 2011) con un grado de criticidad cada vez más elevado.

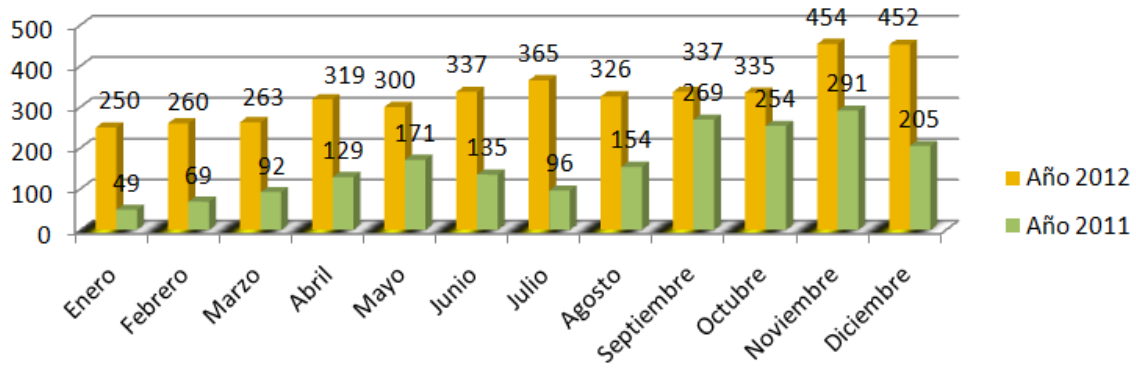

Ilustración 2. Número de incidentes gestionados por el CCN-CERT

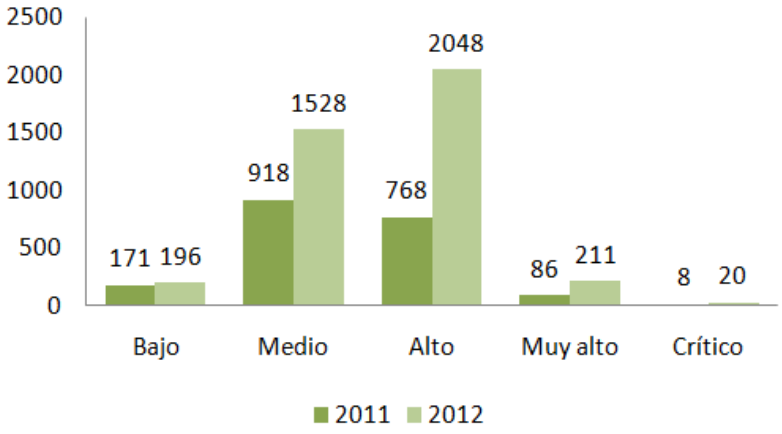

Ilustración 3 Nivel de Criticidad de los incidentes 2011-2012

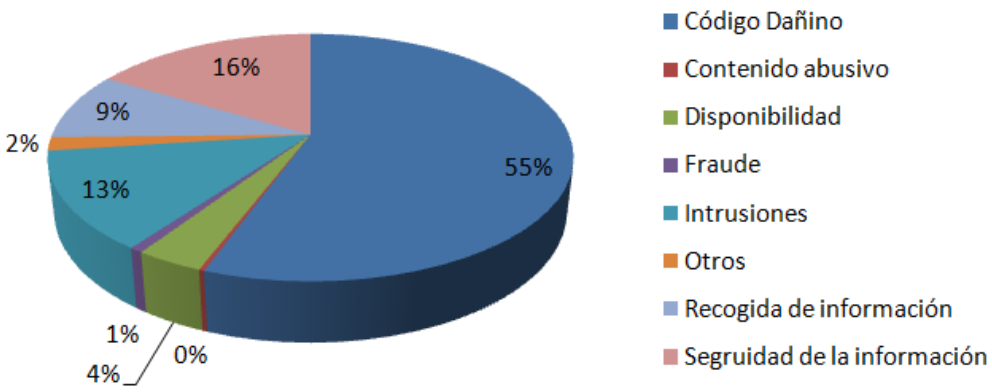

Ilustración 4 Tipología de los incidentes detectados por el CCN-CERT en 2012

Otro de los ejes de actividad es estudiar las tecnologías de seguridad utilizadas. Mediante el formulario "Situación y necesidades de los Organismos pertenecientes a las AAPP y empresas estratégicas en el marco de colaboración con el CCN-CERT (este informe no es público)", el CERT Gubernamental obtuvo una visión general de las tecnologías de seguridad utilizadas por las distintas Administraciones Públicas y empresas estratégicas que, de un modo u otro, colaboran o se encuentran adscritas a cualquiera de los proyectos que actualmente ofrece el CCN-CERT. Estos son algunos datos de ese informe.

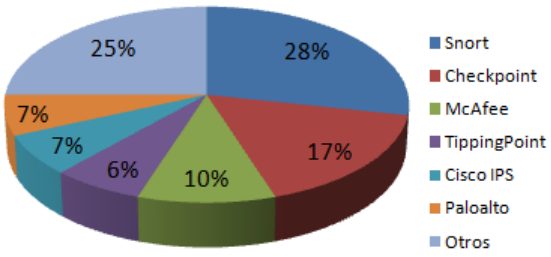

Ilustración 5 Tecnología en IDS/IPS

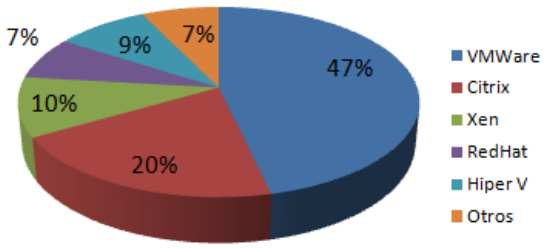

Ilustración 6 Plataforma de virtualización

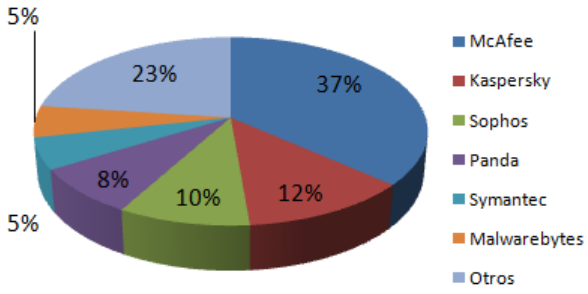

Ilustración 7 Antivirus empleados

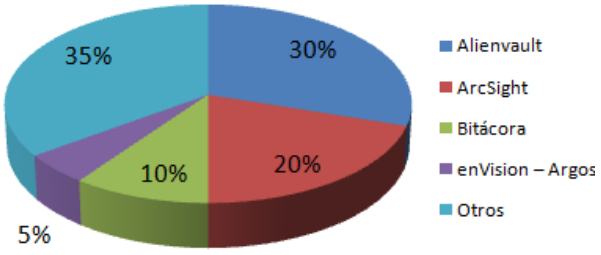

Ilustración 8 SIEM/SEM

Por último, es importante recordar que el 30 de enero de 2014 concluye el plazo de 48 meses fijado por el RD 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. Para establecer aspectos y metodologías comunes relativos a la seguridad en la implantación y utilización de los medios electrónicos, el CCN y la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica de la Secretaría de Estado de Administraciones Públicas, publicaron en 2012, 22 guías de la serie 800.