# La cooperación entre países, eje de la lucha contra la ciberdelincuencia

## LA COLABORACIÓN ENTRE LOS DISTINTOS ORGANISMOS INTERNACIONALES ES ESENCIAL PARA RESPONDER DE FORMA EFICAZ A LAS AMENAZAS QUE AFECTAN A LOS SISTEMAS DE INFORMACIÓN DE TODO EL MUNDO

**CCN-CERT**
**Centro Criptológico Nacional**

En un mundo cada vez más globalizado, en el que los ataques cibernéticos se incrementan cada día y son más difíciles de detectar, la colaboración entre los distintos organismos internacionales es esencial para responder de forma eficaz a las amenazas que afectan a los sistemas de información de todo el mundo.

Según el último informe elaborado por la Organización para la Cooperación y el Desarrollo Económico (OCDE), las economías nacionales y su seguridad se enfrentan al cada vez más frecuente y complejo peligro del software dañino. Este fenómeno está provocando la pérdida de confianza de los usuarios en Internet y exige la actuación conjunta de los gobiernos en materia de seguridad.

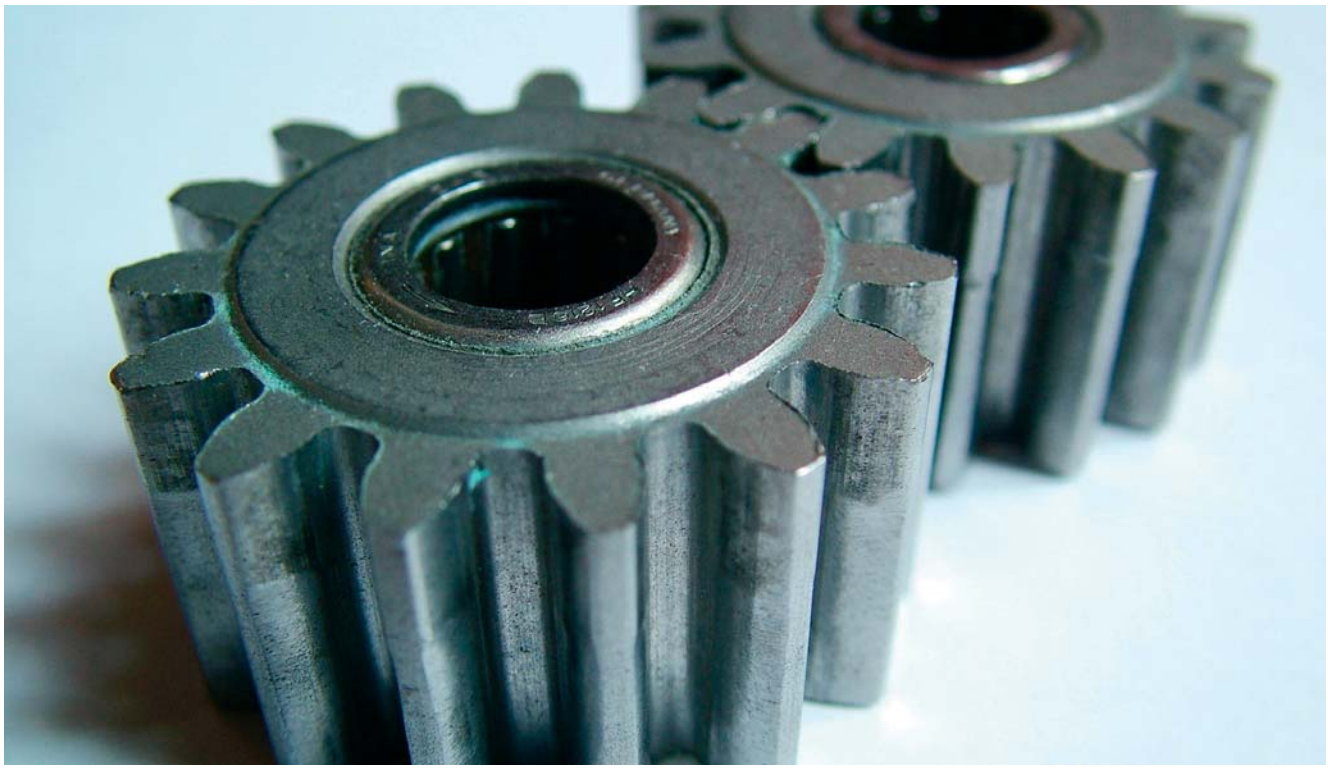
A lo largo del año pasado, este tipo de infecciones a ordenadores (el 93% de ellos de usuarios particulares) creció un 400%, dando lugar a una auténtica "industria" de servicios dañinos, habiendo supuesto un coste económico de 64.000 millones de euros en 2007 -el doble que en 2005-.

> Ante estas amenazas, los gobiernos de todo el mundo han ido adquiriendo una mayor conciencia sobre la necesidad de compartir defensas

La mayoría de las amenazas estuvieron relacionadas con el robo de credenciales, el envío de *spam*, el ataque *DDoS* y el *phishing*. Otros ataques también se realizaron por motivos políticos y se centraron en recaudar todo tipo de información sensible para dañar determinadas organizaciones o entidades gubernamentales.

Ante la proliferación de estas amenazas, los gobiernos de todo el mundo han ido adquiriendo una mayor conciencia sobre la necesidad de compartir objetivos, ideas e información sobre la seguridad de forma global.

En esta línea, y con motivo de la publicación del "Informe Anual 2007", el director general de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), Andrea Pirotti, invitó a los Estados miembros de la Unión Europea a aunar esfuerzos para reducir las amenazas de seguridad mediante una colaboración más estrecha para evitar un eventual "11-S digital". Además, insistió en la necesidad de crear CERTs (Centros de Respuesta a Incidentes de Seguridad) como piezas clave en la lucha contra el cibercrimen. En este sentido, conviene reseñar que en 2005, tan sólo ocho países de la UE disponían de CERTs gubernamentales, mientras que en 2008 el número ya se ha duplicado a 14 (entre ellos el CCN-CERT del Centro Criptológico Nacional), y se prevé que se constituyan 10 más en los próximos dos años.



Otro ejemplo de esta movilización se produjo el pasado 14 de mayo, cuando España y otros seis países de la OTAN (Alemania, Italia, Eslovaquia, Estonia, Letonia y Lituania) firmaron la creación formal del Centro de Excelencia de Cooperación en Ciberdefensa (COE) que tendrá su sede en la capital de Estonia, Tallín. El centro (cuya apertura está prevista para finales de este año) se encargará de desarrollar programas de investigación y formación en materia de "guerra digital" e incluirá una plantilla de cerca de 30 profesionales.

La lucha contra las amenazas cibernéticas también se está extendiendo a los países del Tercer Mundo. Así, en la última Cumbre de Ciberseguridad Mundial (World Cyber Security Summit, WCSS) celebrada en Kuala Lumpur (Malasia), el Instituto SANS anunció la donación de un millón de dólares para llevar a cabo un proyecto conjunto con la Asociación Internacional Multilateral

La lucha contra las amenazas cibernéticas también se está extendiendo a los países del Tercer Mundo

contra el Ciber-Terrorismo (International Multilateral Partnership Against Cyber-Terrorism, IMPACT) que ayude a aumentar la capacidad de defensa de los países en vías de desarrollo.

## Intensa proyección internacional del CCN-CERT

España no se ha mantenido al margen de esta problemática. En 2004, y sobre la base del conocimiento que sobre amenazas, vulnerabilidades y riesgos en los sistemas de información y comunicaciones había ido adquiriendo el CNI a lo largo de su historia, se creó en España el Centro Criptológico Nacional (CCN), como Organismo responsable de garantizar la seguridad de las TIC en el ámbito de la Administración, siguiendo la línea trazada en materia de seguridad por los países avanzados y por las organizaciones internacionales OTAN y Unión Europea.

Desde entonces, el CCN ha participado en organismos y programas internacionales, ha firmado convenios de colaboración para impulsar aspectos de seguridad y ha intercambiado información sobre vulnerabilidades y ataques a nivel global.

Posteriormente, a principios de 2007, se constituyó el Equipo de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN-CERT, en aras de incrementar y mejorar el nivel de seguridad de los sistemas

de información de las administraciones públicas (central, autonómica y local).

Desde su creación, y con el fin de ofrecer una respuesta lo más rápida y eficaz posible, el CCN-CERT -CERT gubernamental español- ha apostado por mantener un contacto directo con otros equipos del resto del mundo con los que compartir información y, en caso de ataque, conocer las fuentes fiables para atajar el incidente.

En este sentido, el CCN-CERT ingresó en junio de 2007 en el Forum de Respuesta a Incidentes y Equipos de Seguridad Informática (FIRST), el foro más importante del mundo, con más de 180 miembros de Europa, América, Asia y Oceanía, procedentes del ámbito gubernamental, económico, educativo, empresarial y financiero.

En febrero de 2008, fue admitido en Trusted Introducer, el principal foro de CERTs europeos que forma parte de TERENA (Asociación Transeuropea de Investigación y Educación de Redes).

El CCN-CERT también está integrado en el *AntiPhishing Working Group* (APWG), un programa del Consejo de Europa enfocado a eliminar todo tipo de fraude y robo de identidad, y trabaja en estrecha colaboración con el Grupo de CERTs Gubernamentales Europeos (EGC), en el que se incluyen los países nórdicos, Francia, Alemania, Hungría, Holanda y Reino Unido.

## Participación en eventos internacionales

Asimismo, el CCN-CERT ha participado activamente en los grupos de trabajo de la citada ENISA (el último, el IX encuentro de CERTs europeos promovido por este Organismo y celebrado el pasado 29 de mayo en Atenas) y en las reuniones del NCIRC de la OTAN (NATO Computer Incident Response Capability), en las que los distintos CERTs de los países miembros de la Alianza Atlántica analizan y comparten información sobre seguridad de la información.

De hecho, fue el anfitrión del último encuentro sobre Ciberdefensa del NCIRC, celebrado el pasado mes de abril en Barcelona, al que asistieron más de 180 representantes de los 26 países miembros.

**El CCN-CERT ingresó en junio de 2007 en el Forum de Respuesta a Incidentes y Equipos de Seguridad Informática (FIRST), el foro más importante del mundo**

En mayo, el personal especializado del CCN-CERT acudió a un encuentro sobre delincuencia informática y ciberterrorismo organizado en Bogotá por la Organización de Estados Americanos (OEA), que reunió a delegados de más de siete países sudamericanos (Bolivia, Chile, Ecuador, Paraguay, Perú, República Dominicana y Colombia) y a especialistas del sector provenientes de Argentina, Brasil y Estados Unidos.

Por último, a finales de junio, el CCN-CERT estuvo presente en la Vigésima Conferencia Anual del Forum de Respuesta a Incidentes y Equipos de Seguridad Informática (FIRST) en Vancouver (Canadá), cuyo tema de debate giró en torno a la necesidad de crear una fuerza de seguridad a nivel mundial.