víctimas del cibercrimen en todo el mundo, con unas pérdidas de hasta 750.000 millones. Sólo por robos vinculados a transacciones con tarjeta de crédito, se pierden 1.500 millones de euros al año en la UE. Robos y estafas tras los que se encuentran, según la compañía Kaspersky, entre 1.500 y 3.000 mafias, desarrollando códigos maliciosos o virus (malware).

SOMOS MÁS VULNERABLES

Una situación crítica porque, a los tradicionales ataques a los PC, se han sumado los realizados contra móviles y tablets, de los que es más fácil obtener datos y beneficios económicos por su bajo nivel de seguridad. De hecho, el Centro Criptológico Nacional (CCN), dependiente del CNI, acaba de recordar que, para este año, "se espera un crecimiento del malware para dispositivos móviles, así como ataques de ingeniería social y el uso económico de las redes sociales". Fruto de su trabajo, tiene 'guardados' más de 140.000 tipos distintos de software maligno.

"No somos consciente de la dependencia que tenemos de la tecnología. Si cayera Internet, estaríamos al borde de la extinción porque no somos capaces de hacer frente a los nuevos retos sin tecnología", explica el director del Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC), teniente coronel de la Guardia Civil Fernando Sánchez Gómez.

En España, el número de amenazas cibernéticas se ha multiplicado exponencialmente en los últimos cuatro años, pasándose de amenazas conocidas, puntuales y dispersas, a otras muy sofisticadas persistentes y con objetivos muy claros, explican desde el CCN, organismo del CNI, encargado de velar por la seguridad de las redes de la Administración y de

FOTO: GUARDIA CIVIL

La Administración dispone de sondas en Internet para detectar la llegada de ciberataques.

LOS GUARDIANES DE LA CIBERSEGURIDAD EN ESPAÑA

En España, las competencias en este campo se reparten entre casi una decena de organismos oficiales. Por supuesto, en su trabajo colaboran con otras entidades privadas como el Centro Nacional de Excelencia de Ciberseguridad, el Centro de Ciberseguridad Industrial o la Asociación Española para el Fomento de la Seguridad de la Información.

El Centro Criptológico Nacional (CCN) Integrado en el Centro Nacional de Inteligencia (CNI) es el organismo español de referencia. Entre sus misiones está la gestión de la seguridad del ciberespacio utilizado por las administraciones estatales, autonómicas y locales, así como detectar y actuar ante cualquier amenaza que pueda afectar a la Seguridad Nacional. Para ello cuenta con el CCN-CERT (Capacidad de Respuesta ante Incidentes de Seguridad), el centro de alerta ante ciberamenazas de la Administración, además de proteger la información nacional clasificada. Inf: 91 372 50 00/ www.ccn.cni.es

El Instituto Nacional de Tecnologías de la Comunicación (INTECO). Dependiente del Ministerio de Industria, Turismo y Comercio, con sede en León, es el responsable de gestionar, a través de su Centro de Alerta Temprana (CERT), la defensa del ciberespacio que utilizan la PYMES españolas y los usuarios. Inf: 987 877 189 / www.inteco.es

Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Depende del Ministerio de Interior y es el encargado de proteger todas las infraestructuras de este tipo en España, de las que un 80% son privadas. Su reto es impulsar y coordinar los mecanismos necesarios para garantizar su seguridad, ya que de ellas dependen los servicios básicos de la sociedad –electricidad, finanzas. tráfico, etc.-. Inf: 91 537 25 57 / www.cnpic-es.es

Grupo de Delitos Telemáticos de la Guardia Civil y **Unidad de Investigación de Delincuencia en Tecnologías de la Información de la Policía Nacional.** Se trata de dos cuerpos, que dependen de Inte-