CyberCamp 2015. Los días 26, 27, 28 y 29 de noviembre se celebrará en Madrid la segunda edición de CyberCamp (**https://cybercamp.es**), el salón que organiza INCIBE al objetivo de "identificar, atraer, gestionar y ayudar a la generación de talento en ciberseguridad que sea trasladable al sector privado, en sintonía con sus demandas". No es este un evento al que se le pueda buscar fácilmente un paralelo fuera de nuestras fronteras. Tampoco es un evento de concepción sencilla, porque sus objetivos tienen un punto de heterogeneidad no desdeñable; a saber: identificar trayectorias profesionales de los jóvenes talentos; llegar a las familias, a través de actividades técnicas, de concienciación y difusión de la ciberseguridad para padres, educadores e hijos; y detectar y promocionar el talento en ciberseguridad mediante talleres y retos técnicos.

En los predios del sector dominados por el furor "tequi" y en aquellos otros en los que se rinde culto a la gestión organizativa y técnica, no se entendió mayoritariamente CyberCamp. Sin embargo, conviene reflexionar y comprender que es una acción que favorece el uso responsable de las TIC por la gente en lo que toca a la ciberseguridad y la ciberprivacidad, que sirve para que los chavales puedan enjuiciar con algún conocimiento de causa dedicarse (o no) a estas disciplinas, y que, además, intenta canalizar con mayor o menor tino el talento en este mundo empresarial tan cerrado.

CyberCamp merece el apoyo inteligente del ramo de la Ciberseguridad, aunque ello requiera curarse de la epidemia de cortoplacismo que casi todos padecemos.

IX Jornadas STIC CCN-CERT (**www.ccn-cert.cni.es**). Los días 10 y 11 de diciembre tendrán lugar en Madrid las Jornadas STIC, organizadas por el CCN-CERT, a las que se ha asociado en su novena edición la leyenda genérica "Detección e intercambio, factores clave", que es una sutil vuelta de tuerca a la idea de colaboración, porque define en qué dirección debe ir esta para obtener mejores resultados que hasta ahora. Carga las tintas hoy el Cert del Centro Criptológico Nacional –cuyos principales ámbitos competenciales actuales en este terreno son las administraciones públicas y las compañías estratégicas para España–, en la detección (por encima de la prevención y la respuesta) y el intercambio de información. Hay que apoyar esta iniciativa.

Esta revista organizó el pasado octubre un nuevo evento, dedicado al *malware* y la ingeniería social, bajo la cabecera de Tendencias SIC, que se tituló "Ciberataques: por dónde van los tiros". Allí quedó patente el hecho de que la industria privada anti-*malware* dedica ingentes cantidades de dinero y talento a ir sabiendo qué pasa, intentando, en paralelo, encontrarle sitio a ese verso suelto que es la ingeniería social. En dicho evento, en el que participó el CCN-CERT, quedó patente que con los actuales derroteros TIC de la sociedad digital, la "industria del *malware* y del engaño" (individuos y grupos criminales –trabajando para sí o para terceros– y estados) la detección deja mucho que desear, porque los 0-day son la base de una floreciente economía. Del intercambio solo puede decirse que la industria privada anti-*malware* (que no está regulada específicamente) se debe a sus clientes, entre los que están particulares, compañías usuarias, MSSPs, administraciones públicas y estructuras oficiales de ciberseguridad de estados. Con eso queda dicho todo.

"Puerto Seguro" (**www.agpd.es**). El 6 de octubre se hizo pública la sentencia en virtud de la cual el TJUE invalidó el denominado Acuerdo de Puerto Seguro, mantenido por la UE con EE.UU. en lo que toca a la transferencia internacional de datos personales. A finales de enero de 2016, según la postura manifestada por el "Grupo de Trabajo del artículo 29", se debería haber encontrado una solución con EE.UU. a los problemas que plantea la aplicación de esta sentencia. El reto es que dicha solución debe ser respetuosa con los derechos fundamentales objeto de protección. Si no hay fumata blanca, las autoridades de control europeas de los estados miembros actuarían en consecuencia. La verdad es que la tesitura abre un camino a todas las partes implicadas para explorar fórmulas y herramientas de transferencia tan legales como novedosas. ●

Edita: Ediciones CODA, S.L. Goya, 39. 28001 Madrid (España) Tels.: 91 575 83 24 / 25 Fax: 91 577 70 47 **Correo-e:** info@revistasic.com www.revistasic.com **Editor:** Luis Fernández Delgado **Director:** José de la Peña Muñoz **Redacción:** Carlos Losada Redondo **Sección Laboratorio SIC:** Javier Areitio Bertolín **Colaboran en este número:** David Acosta, Ignacio Alamillo, Xavier Aparicio, Carlos Cabañas, Joan Corominas, Jorge Dávila, Francisco J. Diéguez, Miguel López, Juan López-Rubio, Alfonso Martín, Ricard Martínez, Manuel Orellana, Rafael Ortega, Alberto Partida, Florentino Pérez, Paco Pérez, Borja Roux, Luis Saiz, José Luis Serrano, Lluis Sintes, Francisco Valencia **Departamento de Marketing/Publicidad:** Rafael Armisén Gil, Fernando Revilla Guijarro **Administración y suscripciones:** Susana Montero, Maite Montero, Mercedes Casares **Fotografía:** Jesús A. de Lucas **Producción, diseño y maquetación:** MSGráfica **Imprime:** Monterreina **ISSN:** 1136-0623