

# El Rey FELIPE VI visita las multitudinarias XII Jornadas CCN-CERT, centradas en las capacidades de disuasión y la búsqueda de talento

Cómo rúbrica a una docena de ediciones de creciente interés, su Majestad el Rey, Felipe VI, tuvo a bien visitar las XII Jornadas CCN-CERT –organizadas a instancias del CNI–, convertidas ya en el mayor evento de ciberseguridad en España con más de 2.400 profesionales.

Durante dos días, bajo el lema “Ciberseguridad, hacia una respuesta y disuasión efectiva”, expertos de la administración, las empresas y la universidad, además de reconocidos *hackers*, analizaron la situación real de la ciberseguridad en España, sus normativas y los diferentes retos para 2019.

“Los profesionales de la ciberseguridad hacen que este mundo sea mejor”, destacó el director del CNI y Secretario de Estado **Félix Sanz** durante la inauguración, a la vez que recordó que “cada día el CNI se enfrenta a dos o tres ataques de peligrosidad muy alta”. El Subdirector General del **Centro Criptológico Nacional (CCN)**, **Luis Jiménez**,

destacó en la presentación que la sociedad “está enfrentándose a una de las mayores amenazas globales del siglo XXI, que afecta a nuestra intimidad, forma de vida, estabilidad del mercado y a la innovación”. Durante la sesión plenaria se celebró una mesa redonda en la que participaron expertos como **David Barroso**, CEO de **CounterCraft**, **José Mañas** –catedrático y creador de la herramienta PILAR– y **José Rosell**, de **S2 Grupo**.

Durante las jornadas, el Jefe del Departamento de Ciberseguridad del CCN-Cert, **Javier**



El Rey Felipe VI saluda a patrocinadores, organizadores y empresas de referencia. Como curiosidad fue obsequiado con un ‘Kit de seguridad digital’ para la princesa y la infanta

**Candau**, destacó que para hacer frente a las amenazas más peligrosas la clave es contar con capacidades para prevenir, detectar y responder, además de compartir información. Entre las novedades que dio a conocer destacó la puesta en marcha del SOC del **Ministerio de Justicia** el año pasado y el de la **Administración General del Estado (AGE)** en 2019. Además, el CCN-Cert también presentó nuevas herramientas para proteger a administraciones y empresas como sus SOC’s virtuales o la certificación de produc-

tos ciberseguros ‘Lince’ –más fácil de obtener que la **Common Criteria (CC)**– pero con un nivel básico aceptable.

Una de las novedades de esta edición fue la ‘Sala Rooted’, en la que participaron muchos de los apuntados a **Atenea**, la plataforma de retos de ciberseguridad del CCN-Cert, y cuyos primeros clasificados **Román Medina** y **Julián Menéndez** fueron galardonados. El CCN Cert también reconoció la trayectoria del CEO de **Dinosec**, **Raúl Siles**, con su “Premio CCN’ por “trayectoria en favor de la ciberseguridad” de 2019.

En esta edición participaron 43 empresas, entre ellas Revista SIC, y ocho entidades que han patrocinado el evento y han mostrado su tecnología. Entre las conferencias destacadas en un apretado programa de intervenciones, cabe destacar la del teniente coronel **Juan Sotomayor**, de Guardia Civil, la de **Fernando Sánchez**, del **CNPIC**, sobre la aplicación de la Directiva NIS y su futuro reglamento, la de **Alberto Cita**, de **Symantec**, sobre entrenamiento de inteligencia artificial o la de **Luis Salvador** y **Andrés Calvo**, de la **Agencia Española de Protección de Datos (AEPD)**, sobre la notificación de brechas de seguridad desde la aplicación del RGPD. Clausuraron esta edición el Secretario General de Administración Digital, **Fernando de Pablo Martín**, y la Directora de la AEPD, **Mar España**.

## Operador de servicio esencial y operador crítico: quién es quién y por qué

Durante las jornadas, tuvo lugar una interesante mesa redonda bajo la dirección de **José de la Peña**, Director de Revista SIC, en la que se ahondó en los pormenores de la transposición de la Directiva NIS a la legislación española. Su convergencia con algunas medidas ya contempladas en la Ley 8/2011 para la protección de las infraestructuras críticas, así como sus nuevos requisitos hacen que su desarrollo en España no esté exento de polémica. Una situación sobre la que debatieron representantes de la Administración Pública, como **Marcos Gómez** (Incibe), **Miguel A. Abad** (CNPIC) y **Carlos Córdoba** (CCN) junto a responsables de ciberseguridad de importantes proveedores de servicios como **Francisco Lázaro** (Renfe), **Juan Carlos Gómez** (Telefónica) y **Juan Luis Pozo** (Global Omnium).

El debate comenzó con una reflexión sobre la obligación que impone la Directiva NIS de identificar a los proveedores de servicios esenciales. Una tarea delicada donde los proveedores piden mayor claridad en su definición frente a los operadores de servicios críticos, ya que “se define como operador esencial al mismo que es crítico”. Esto hace que, para aquellos servicios que se quedan fuera, las inversiones que se realizan en ciberseguridad no tengan respaldo legal

y su repercusión sea complicada de justificar. También quedó patente que, aunque existe una mayor colaboración, “siguen existiendo claros oscuros, por enmiendas incorporadas sin la participación de todas las partes”.

El reconocimiento de la figura del responsable de seguridad de la información fue otro de los temas más debatidos. Los representantes de los operadores mostraron su preocupación por que no se desvirtúe o no tenga el peso adecuado para poder ejercer sus funciones correctamente –por ejemplo, dotándole de presencia en la alta dirección y de los recursos necesarios–.

Junto a todo ello, también quedó patente la necesidad de clarificar la notificación de incidentes “con baremos y tiempos precisos”, así como establecer un régimen sancionador que sea suficientemente ‘claro’ para que las empresas sean proactivas en el cumplimiento de la normativa.

