

Organizada por el CCN-CERT

El ENS y las claves para afrontar los riesgos emergentes en las AA.PP., eje central de la IV Jornada STIC

El Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) celebró el pasado 14 de diciembre, en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), la **IV Jornada STIC**, con el objetivo de ofrecer al personal de las diferentes administraciones públicas españolas (general, autonómica y local), información y herramientas con que afrontar las amenazas que se ciernen sobre sus sistemas, compartiendo el conocimiento y los recursos disponibles.

El evento –al que asistieron más de 300 profesionales y en el que participó la revista SIC en tanto que entidad copatrocinadora– fue inaugurado por el Secretario de Estado Director del CNI, **Félix Sanz Roldán**, quien ofreció un breve resumen de los más recientes servicios incorporados por el CERT guber-



Félix Sanz Roldán

namental español durante el año 2010, y puestos a disposición del personal de la administración en su portal www.ccn-cert.cni.es.

Dichos servicios son: una sección del Esquema Nacional de Seguridad (ENS) con nueve guías de implantación, programas de apoyo y documentación sobre el mismo; las series CCN-STIC, con 145 guías que recogen normas, instrucciones y recomendaciones; cursos STIC; cursos on-line de seguridad de la información; el sistema *MultiAnti-virus* o la herramienta *Pilar*.

Tras el acto inaugural, representantes del CCN-CERT expusieron los principales incidentes y amenazas detectados por este equipo gracias a sus Sistemas de Alerta Temprana, los cuales posibilitan la detección rápida

de eventos sospechosos y anomalías dentro del ámbito de la Administración, tanto dentro de la red SARA como en los accesos a Internet de los organismos suscritos al servicio.

En el transcurso de la jornada, reconocidos expertos en seguridad TIC abordaron en sus ponencias aspectos como el Esquema Nacional de Seguridad (**José de la Peña**, director de SIC, moderó al respecto del mismo una mesa redonda en esta Jornada), el *malware* para dispositivos móviles *Zeus MITMO* (*Man in the Mobile*), los ataques informáticos y su gestión en un operador de servicio, la inseguridad en los dispositivos móviles, el panorama actual de las redes robot, la herramienta *Pilar*, la inseguridad en las redes inalámbricas, o los ataques sobre las infraestructuras críticas.



actual de las redes robot, la herramienta *Pilar*, la inseguridad en las redes inalámbricas, o los ataques sobre las infraestructuras críticas.

El MPTyAP, con la colaboración de INDRA, avanza en el proyecto europeo STORK

La multinacional española **Indra** colabora actualmente con el **Ministerio de Política Territorial y Administración Pública de España** (MPTyAP) en el proyecto de ámbito europeo **Stork**, cuyo objetivo es facilitar la interoperabilidad de las identidades electrónicas, garantizando el acceso seguro e integrado a servicios de gobierno-e, conforme a unas especificaciones de interoperabilidad comunes.

El proyecto *Stork* –de cuyo arranque ya informara SIC en números anteriores– se desarrolla bajo la iniciativa *i2010 –A European Society for growth and employment*, lanzada por la **Comisión Europea** en junio del 2005. Esta iniciativa, cuyo desarrollo definitivo finaliza en mayo de este año, promueve una economía digital abierta y competitiva con acento en las TIC como motor de inclusión y calidad de vida. Su plan de acción destaca la necesidad de aceptar las identidades electrónicas nacionales en otros países, propiciando un acceso seguro, integrado y sin fisuras a los servicios de Gobierno electrónico de los diferentes países por parte de ciudadanos comunitarios que residen temporal o permanentemente en otro estado miembro.

Para dar cumplimiento a este objetivo, 32 entidades de 14 países: 13 de la Unión Europea (Alemania, Austria, Bélgica, Eslovenia, España, Estonia, Francia, Italia, Luxemburgo, Países Bajos, Portugal, Reino Unido y Suecia), además de Islandia, se han unido en el consorcio **Secure Identity AcrOss BoRders LinkEd** (Stork), cofinanciado por la Comisión Europea dentro de la estrategia comunitaria de crear servicios paneuropeos de administración electrónica.

Gracias a esta iniciativa, el DNIe y otras identidades electrónicas comunes en España serán aceptados por las administraciones-e de Francia, Austria, Alemania,

Portugal y otros países participantes. La Administración española, por su parte, también podrá aceptar las identidades electrónicas procedentes de otros países. Además, a diferencia de otros sistemas de gestión de identidades, los datos de identidad suministrados por la plataforma *Stork* son garantizados por los gobiernos de los países donde las credenciales han sido emitidas, asegurando la transparencia, seguridad y fiabilidad de los datos. Toda la información se recoge en una plataforma que podrá gestionar las identidades de 400 millones de ciudadanos europeos, permitiéndoles el acceso, actualmente, a unos 40 portales.

Indra es responsable, junto al MPTyAP, del diseño, desarrollo e implantación de esta plataforma. Para ello, se están coordinando los trabajos de definición y desarrollo por parte de los participantes sobre los modelos de confianza y protocolos de intercambio de identificadores nacionales, así como los datos adicionales de identidad que permiten realizar un proceso de autenticación completo a través de las identidades electrónicas existentes en cada país.

El desarrollo de la plataforma europea de identificación transfronteriza y su implantación en los 14 estados miembros del consorcio ha tenido una duración de dos años. En la actualidad, se está verificando la validez de la solución en unos pilotos reales basados en seis servicios de Administración electrónica que ya soportan las identidades electrónicas de otros países: una plataforma de autenticación transfronteriza para servicios electrónicos *SafeChat* que pretende proteger a los menores en comunicaciones interactivas; Movilidad de Estudiantes; Entrega electrónica transfronteriza de notificaciones oficiales; un piloto de

Cambio de Domicilio; y un dispositivo con la Comisión Europea para que los empleados públicos puedan acceder a sus aplicaciones corporativas a través de sus identidades nacionales. De ellos, dos pilotos tienen participación española: el de Cambio de Domicilio, que es un servicio que ofrece el MPTyAP para comunicar a las administraciones públicas la nueva dirección de residencia; y el de Movilidad de Estudiantes, liderado por la Conferencia de Rectores de la Universidades Españolas (CRUE).

Proyecto Gobierno de Asturias

Por otra parte, la compañía española también ha resultado adjudicataria de un concurso del **Gobierno de Asturias** para la dotación de los sistemas informáticos del nuevo **Hospital Universitario Central de Asturias (HUCA)**, el cual alojará el Centro de Proceso de Datos (CPD) de Respaldo del Principado, de cuya creación se responsabilizará Indra, por un montante de 11,7 millones de euros.

El Gobierno del Principado de Asturias ya disponía de un CPD, que se inauguró el pasado julio tras la migración de todos los sistemas desde su anterior ubicación; y este CPD de Respaldo abarcará hasta 31 servicios identificados como críticos a través de la elaboración previa de un análisis de impacto en el negocio.

La firma **PricewaterhouseCoopers** se encargará de prestar apoyo a la dirección del proyecto en lo que se refiere a la coordinación, seguimiento y control, en tanto que adjudicataria, por 1,5 millones de euros, del sexto y último lote del concurso, correspondiente a la Oficina Técnica.

