DOCUMENTO INFORMATIVO DEL IEEE 08/2011

SEGURIDAD DE LA INFORMACIÓN

(MARZO DE 2011)

El Estado Mayor Conjunto y la Dirección General de Infraestructura, con el patrocinio de ISDEFE, organizaron las X Jornadas SID de Seguridad de la Información[1], del 21 al 24 de febrero del 2011, en el Centro Superior de Estudios de la Defensa Nacional. Aprovechando este evento se hizo mención de la aparición del Cuaderno de Estrategia del Instituto Español de Estudios Estratégicos nº 149 sobre **"Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio"[2],** editado en colaboración con el Instituto Universitario "General Gutiérrez Mellado".

Las X Jornadas SID, como en años anteriores, se han estructurado en dos bloques temáticos. El primer bloque, reservado para los profesionales de Defensa, trató todos estos aspectos en el entorno de Mando y Control. Se abordaron los siguientes temas: el ciberespacio como nuevo aspecto de la Defensa; aspectos legales de las operaciones en el ciberespacio; las redes militares como parte del ciberespacio; aspectos de seguridad de las redes presuntamente aisladas y protegidas; y sobre todo qué se está haciendo en las Fuerzas Armadas españolas al respecto; también se incluyó una mesa redonda sobre el nuevo concepto estratégico de la OTAN y las operaciones militares en el ciberespacio.

El segundo bloque planteó temas en los que el Ministerio está trabajando y colaborando como convenios con otras organizaciones, protección de infraestructuras críticas, normativa de seguridad de la información, seguridad industrial, II ejercicio de ciberdefensa de las FAS e iniciativas de pruebas, alertas y operaciones de seguridad. Se incluyeron también dos mesas redondas: la primera sobre los retos de la seguridad frente a los avances de la tecnología y la segunda sobre la convergencia de las seguridades.

Entre otros aspectos se presentaron los avances del GIPIC-grupo de trabajo informal sobre protección de infraestructuras críticas[3] impulsado por el CNPIC[4] – Centro Nacional de Protección de Infraestructuras Críticas de la Secretaría de Estado de Seguridad del Ministerio del Interior. Durante 2011 se desarrollarán Planes Operativos de Seguridad y Planes de Protección Específicos.

---

[1] https://www.jornadassid.ISDEFE.es/
[2] El cuaderno de estrategia nº 149 está disponible en el siguiente enlace: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf
[3] https://gipic.ISDEFE.es/
[4] http://www.cnpic-es.es/

Se abordó también la plataforma @firma[5] que lidera el Ministerio de Política Territorial y Administración Pública. @firma es una plataforma de validación y firma electrónica multi-PKI, que se pone a disposición de las Administraciones Públicas, proporcionando servicios para implementar la autenticación y firma electrónica avanzada de una forma rápida y efectiva. Es una solución de referencia para cumplir con las medidas de identificación y autentificación descritas en el Capítulo II de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP). Esta plataforma enlaza con el proyecto europeo STORK (*Secure idenTity acrOss boRders linKed*)[6], cuyo objetivo es conseguir el reconocimiento paneuropeo de las identidades electrónicas, y en concreto la aceptación del DNI electrónico e identificadores similares en Servicios de Administración Electrónica de otras administraciones europeas.

En la mesa redonda sobre los retos de la seguridad frente a los avances de la tecnología se planteó reemplazar el uso de productos COTS (productos comerciales) por productos certificados funcionalmente; la necesidad de evitar que los problemas de identificación y autenticación supongan un freno al avance de la seguridad TIC (Tecnologías de la Información); se recordaron los problemas que plantea la federación de redes y el reconocimiento de credenciales entre oficinas situadas en otros países; también se abordó la dificultad de la implantación de servicios en la nube en servicios de la administración y de defensa.

Durante el cuarto día se trataron los avances del Ministerio de Defensa en su normativa de seguridad de la información con la publicación de la OM 41/2010 julio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa. [7]

Se recordó el II Ejercicio de ciberdefensa de las FAS que tuvo lugar en octubre de 2010 organizado por el EMACON, a través de la Sección de Seguridad de la Información CIS y con la colaboración de ISDEFE, con participantes de distintos equipos pertenecientes al Ejército de Tierra, Armada, Ejército del Aire, Cuartel General del Estado Mayor de la Defensa (EMAD), Centro de Inteligencia de las Fuerzas Armadas (CIFAS), Centro Criptológico Nacional (CCN) y Guardia Civil. La capacidad inicial que se valoró en el I ejercicio ha mejorado respecto a este II ejercicio. En esta segunda ocasión la demanda de participación creció de manera considerable, lo que constituye una prueba de éxito. Esta edición, introdujo dos importantes mejoras en los escenarios de defensa y ataque, incluyendo sistemas SCADA y herramientas de análisis y correlación de eventos.

[5] http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=190

[6] https://www.eid-stork.eu/

[7] Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa. Orden DEF/54/2008, de 16 de enero, por la que se constituye la Comisión Ministerial de Administración Electrónica del Ministerio de Defensa, derogada por la Orden DEF/1159/2010, de 3 de mayo, por la que se regula la Comisión Ministerial de Administración Electrónica del Ministerio de Defensa.

La segunda mesa redonda abordó la convergencia de las seguridades. Este tema surgió en febrero de 2005, cuando dos asociaciones, ASIS e ISACA, la primera dedicada al sector *Seguridad* y la segunda, a la Seguridad de la Información, decidieron crear, ante la convergencia de las amenazas, la "Alianza para la Gestión del Riesgo Empresarial". La convergencia en seguridad es un proceso que persigue alcanzar una seguridad integrada con una planificación conjunta de los objetivos de seguridad, la integración de las tecnologías, la seguridad física y la seguridad lógica. La convergencia en seguridad es aplicar el enfoque integral a este ámbito para dar respuesta a las necesidades de Seguridad que tienen las organizaciones actuales. Es necesario superar el modelo tradicional de Seguridad porque no se puede trabajar aisladamente. El análisis de riesgos debe contemplar de una forma global tanto las amenazas físicas como las lógicas, y este modelo de convergencia está siendo ya aplicado en varias empresas y operadores española de gran tamaño.

M. J. Caro
Analista Principal del IEEE