Esquema Nacional de Seguridad

Última hora enero 2013

Nuevas incorporaciones de las Guías de Seguridad y otras novedades.

Se han incorporado nuevas guías CCN-STIC a la serie relativa al Esquema Nacional de Seguridad que, a la fecha, cuenta con las siguientes publicadas en el Portal de CCN-CERT: (datos 28 noviembre)

Guías CCN-STIC publicadas:

- 800 - Glosario de Términos y Abreviaturas del ENS
- 801 - Responsables y Funciones en el Esquema Nacional de Seguridad
- 802 - Auditoría del Esquema Nacional de Seguridad
- 803 - Valoración de sistemas en el Esquema Nacional de Seguridad
- 804 - Medidas de implantación del Esquema Nacional de Seguridad
- 805 - Política de Seguridad de la Información
- 806 - Plan de Adecuación del Esquema Nacional de Seguridad
- 807 - Criptología de empleo en el Esquema Nacional de Seguridad
- 808 - Verificación del cumplimiento de las medidas en el Esquema Nacional de Seguridad
- 809 - Declaración de Conformidad del Esquema Nacional de Seguridad
- 810 - Creación de un CERT / CSIRT
- 811 - Interconexión en el Esquema Nacional de Seguridad
- 812 - Seguridad en Entornos y Aplicaciones Web
- 813 - Componentes certificados en el ENS
- 814 - Seguridad en correo electrónico
- 815 - Métricas e Indicadores en el Esquema Nacional de Seguridad
- 817 - Criterios comunes para la Gestión de Incidentes de Seguridad
- 818 - Herramientas de Seguridad en el ENS
- 821 - Ejemplos de Normas de Seguridad
- 822 - Procedimientos de Seguridad en el ENS
- 824 - Informe del Estado de Seguridad

Se encuentran actualmente en desarrollo las siguientes guías:

- 819 – Contratación en el ENS
- 820 - Denegación de Servicio
- 823 - Cloud Computing en el ENS

Se ha publicado la versión 3 de MAGERIT, metodología de análisis y gestión de riesgos de los sistemas de información. Esta nueva versión mantiene en gran medida la estructura de la versión 2 y se ha actualizado para proporcionarle un mejor alineamiento con la normativa ISO. MAGERIT versión 3 persigue una integración de las tareas de análisis de riesgos dentro de un marco organizacional de gestión de riesgos dirigido desde los órganos de gobierno. También, a la luz de la experiencia de aplicación, se ha aligerado el

texto, se han eliminado partes poco importantes o poco usadas y se ha mejorado la normalización de las actividades.

También está disponible en el Portal de CCN-CERT una versión navegable del Esquema Nacional de Seguridad.

En cuanto a programas de Apoyo se dispone de los siguientes:

- Controles de aplicación en el Esquema Nacional de Seguridad según la categorización del sistema
- PILAR 5.1 – Windows – Unix - Mac
- µPILAR 5.1 – Windows – Unix - Mac

El Esquema Nacional de Seguridad y los ataques dirigidos (APT) protagonistas de las VI Jornadas STIC CCN-CERT

El CCN-CERT, en su calidad de CERT Gubernamental español, reunió en Madrid a los principales expertos en ciberseguridad del país, dentro de las VI Jornadas STIC CCN-CERT. El contenido de lo presentado, la afluencia de público y la calidad y conocimiento de los ponentes avalaron este encuentro celebrado el 11 y 12 de diciembre en el Auditorio de la Fábrica Nacional de la Moneda y Timbre e inauguradas por el Secretario de Estado-Director del CNI, Félix Sanz.

Las Jornadas centraron buena parte de su contenido en el Esquema Nacional de Seguridad (ENS), la proliferación de Ataques Dirigidos o APTs y el robo de información sensible. De hecho, el primer módulo del segundo día estuvo centrado en el Esquema y en él se abordaron las acciones realizadas para facilitar su aplicación y los indicadores en el ENS y su nivel de cumplimiento. La gestión de incidentes, los agentes implicados en el ciberespionaje, la persistencia de un APT, su funcionamiento y cómo reaccionar ante este tipo de amenazas que ponen en peligro la información más valiosa de las AAPP y de las empresas, fueron otros de los temas abordados en este encuentro celebrado los días 11 y 12 de diciembre, en el Auditorio de la Fábrica Nacional de la Moneda y Timbre, en Madrid, y cuyas ponencias pueden descargarse en el portal del CCN-CERT (www.ccn-cert.cni.es).

Durante los próximos meses de 2013, y dentro de este mismo ámbito, se contemplan las siguientes acciones:

- Seguimiento del progreso de la adecuación al Esquema Nacional de Seguridad (y al Esquema Nacional de Interoperabilidad), pues el plazo de adecuación para ambos vence el 30 de enero de 2014.
- Actualización del Real Decreto 3/2010 para adecuar ciertos aspectos del Real Decreto 3/2010 a la rápida evolución de las tecnologías de aplicación, a la experiencia derivada de la implantación del Esquema Nacional de Seguridad y al mejor cumplimiento de los preceptos indicados. Dichos aspectos se refieren a la mejora de la articulación de los procedimientos de recogida y consolidación de información para la

elaboración del informe del estado de la seguridad, a precisiones que aumentan la eficacia de las medidas de seguridad; más algún detalle de carácter editorial.

- Continuidad de los trabajos de elaboración de guías CCN-STIC y recomendaciones.
- Y el mantenimiento de la corresponsabilidad de todas las Administraciones Públicas mediante la continuidad de la dinámica de cooperación y colaboración permanente. En esta tarea desempeñan un papel clave la Comisión Permanente del Consejo Superior de Administración Electrónica, el Comité Sectorial de Administración Electrónica y su Comité de Seguridad, junto con sus respectivos grupos de trabajo.