Entre ellas, destacan cinco guías de acceso público destinadas a la implantación del Esquema Nacional de Seguridad

El CCN elabora y actualiza 17 nuevas Guías para la ciberseguridad de los sistemas de las Administraciones Públicas

- **Los nuevos documentos forman parte de las más de 170 Guías CCN-STIC, que ofrecen normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de la información y las comunicaciones de las distintas administraciones, incluyendo una amplio capítulo de dispositivos móviles.**

- **Las guías, junto con el resto de servicios puestos a disposición del personal de la Administración, pueden descargarse desde el portal www.ccn-cert.cni.es**

Madrid, 17 de septiembre de 2012.- El Centro Criptológico Nacional (CCN) ha puesto a disposición de las distintas administraciones públicas 17 nuevas guías, incluidas en sus Series CCN-STIC, con las que mejorar los requisitos de ciberseguridad exigibles en los sistemas de información y comunicaciones de la Administración. Estos documentos, algunos de los cuales son revisiones y actualizaciones de guías ya existentes, se centran en diversos campos: políticas (Serie 000), procedimientos (Serie 100), normas (Serie 200), instrucciones técnicas (Serie 300), guías generales (Serie 400), guías entornos Windows (Serie 500), guías otros entornos (Serie 600), **implantación del Esquema Nacional de Seguridad, ENS** (Serie 800) e informes técnicos (Serie 900).

En concreto, y dentro del capítulo de implantación del ENS, las nuevas guías elaboradas por el personal del CCN y que son de acceso público, abordan aspectos tales como la ***Gestión de Incidentes de Seguridad en el ENS*** (CCN-STIC 817), ***Responsabilidades y Funciones en el ENS*** (CCN-STIC 802), ***Componentes Certificados en el ENS*** (CCN-STIC 813) o ***Guía de Interconexión en el ENS*** (CCN-STIC 811).

Asimismo, el CCN ha elaborado una serie de guías sobre dispositivos móviles: ***Seguridad en Android 2.1*** (CCN-STIC 453***), Seguridad en iPad*** (CCN-STIC 454) y

Seguridad en iPhone (CCN-STIC 455), así como de la nueva versión de la Herramienta PILAR: ***Manual de la Herramienta de Análisis de Riesgos PILAR 5.2*** (CCN-STIC 470E1) y ***Manual de la Herramienta de Análisis de Riesgos PILAR 5.2. Análisis de Impacto y Continuidad de Negocio*** (CCN-STIC470E2).

Todas las Guías (tanto las de acceso público, como las restringidas al personal de seguridad de las distintas administraciones públicas españolas), están disponibles el portal del CCN-CERT www.ccn-cert.cni.es.

Sobre CCN-CERT

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del **Centro Criptológico Nacional**, CCN (www.ccn-cert.cni.es). Este servicio se creó a finales del año 2006 como **CERT gubernamental/nacional**, y sus funciones quedan recogidas, tanto en el RD 421/2004 de regulación del CCN, como en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad. De acuerdo a este RD, el CCN-CERT, tiene responsabilidades en ciberataques sobre sistemas clasificados, sistemas de la Administración y, de acuerdo con la Ley 11/2002, sobre sistemas de empresas de sectores estratégicos.

MÁS INFORMACIÓN

Centro Criptológico Nacional
Argentona, 20
28023 Madrid
www.ccn-cert.cni.es
eventos@ccn-cert.cni.es

17 de septiembre de 2012