El Centro Criptológico Nacional, CCN, hace pública las Guías CCN-STIC 455 y 454 de Seguridad en iPhone y iPad

Cómo utilizar de forma segura los dispositivos móviles de Apple

- **El CCN ofrece, en sendas Guías, recomendaciones de seguridad para la configuración de dispositivos móviles basados en el sistema operativo iOS (iPhone, iPad y iPod Touch), como forma de proteger el propio dispositivo, sus comunicaciones y la información y datos que gestionan y almacenan.**

- **Los documentos están disponibles en la parte pública del portal www.ccn-cert.cni.es, junto con más de 200 documentos de recomendaciones, normas y procedimientos en materia de ciberseguridad, incluyendo una Guía de Seguridad en Android (CCN-STIC 453).**

Madrid, 3 de septiembre de 2014.- El **CCN-CERT**, del Centro Criptológico Nacional, **CCN**, adscrito al Centro Nacional de Inteligencia, **CNI**, ha hecho pública las ***Guías CCN-STIC 454 de Seguridad en iPad y 455 Seguridad en iPhone (iOS 7)***, conscientes de que pese a que los dispositivos móviles se utilizan para comunicaciones personales y profesionales, privadas y relevantes, y para el almacenamiento de información sensible, el nivel de percepción de la amenaza de seguridad real existente no ha tenido trascendencia en los usuarios finales y en las organizaciones.

Las nuevas Guías publicadas realizan un análisis detallado de los mecanismos de configuración de seguridad recomendados para uno de los principales sistemas operativos empleados en la actualidad en este tipo de dispositivos, el iOS de Apple (empleado en los iPhone, iPad y iPod Touch), en concreto hasta la versión iOS 7.x con el objetivo de reducir su superficie de exposición frente a ciberataques.

Actualización del sistema operativo, la gestión empresarial de este tipo de dispositivos, el acceso físico, las restricciones en el proceso de activación o el cifrado de datos, son algunos de los aspectos abordados en estas guías.

Junto a ellos, la gestión de certificados digitales y credenciales, la eliminación de datos, los servicios de localización geográfica, las comunicaciones USB e inalámbricas (Wi-Fi, Bluetooth, GSM, etc) o las copias de seguridad, completan el extenso programa de estos documentos.

COMUNICADO CCN-CERT GUÍAS 454 Y 455

3 de septiembre de 2014

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del ENS.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es

LinkedIn

3 de septiembre de 2014