Esta nueva *Guía CCN-STIC 453B* de dispositivos móviles se centra en la versión 4 del sistema operativo

Medidas de seguridad para Android, nueva Guía del CCN-CERT

- **Proporcionar una lista de recomendaciones de seguridad para la configuración de dispositivos móviles basados en Android con el fin de proteger el propio dispositivo, sus comunicaciones y la información y datos que gestiona y almacena, principales objetivos de este documento.**

- **De este modo, el CERT Gubernamental Nacional actualiza su Guía 453 de versiones anteriores de Android, el sistema operativo con más cuota de mercado en dispositivos móviles y también el más atacado.**

Madrid, 17 de abril de 2015.- El CCN-CERT ha hecho pública su **Guía CCN-STIC 453B Seguridad en Dispositivos Móviles: Android 4.x**, un completísimo documento en el que se proporciona una lista de recomendaciones de seguridad para la configuración de dispositivos móviles basado en Android 4.x, cuyo objetivo es proteger el propio dispositivo móvil, sus comunicaciones y la información y datos que gestiona y almacena. Todo ello, teniendo en cuenta que es uno de los principales sistemas operativos de dispositivos móviles utilizados en la actualidad y el que recibe un mayor número de ciberataques.

"La Guía aborda aspectos tales como la actualización del sistema operativo, modelo y arquitectura de seguridad, la gestión empresarial de dispositivos móviles, acceso físico al dispositivo móvil, cifrado de datos o APPS"

La Guía, elaborada por el **Centro Criptológico Nacional**, recoge los detalles específicos de la aplicación e implementación de las medidas de seguridad más adecuadas en este tipo de dispositivos móviles. El documento cuenta con un amplio capítulo sobre la *configuración de seguridad en Android* que, entre otros, aborda aspectos tales como la actualización del sistema operativo, modelo y arquitectura de seguridad, la gestión empresarial de dispositivos móviles, acceso físico al dispositivo móvil, múltiples perfiles de usuario, cifrado de datos, gestión de certificados digitales y credenciales o la eliminación de datos en Android.

Asimismo, la Guía recoge otros puntos como la localización o ubicación geográfica, las comunicaciones USB, NFC, Bluetooth y Wi-Fi; los mensajes de texto, las copias de seguridad, las aplicaciones móviles (APPS), su instalación y eliminación; el correo electrónico y Gmail, o las redes sociales.

17 de abril de 2015

Esta Guía se une a otras sobre dispositivos móviles del CCN-CERT (Android, iPad e iPhone) que son públicas y que pueden descargarse desde el portal del CCN-CERT (www.ccn-cert.cni.es).

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 Nacional** 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, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, a 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
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/
@CCNCERT

http://youtu.be/5XxS9mZZfKs

COMUNICADO CCN-CERT