GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA

centro nacional de inteligencia
centro criptológico nacional

CCN-CERT
centro criptológico nacional

La Guía CCN-STIC 596 está disponible en la parte restringida del portal

Protección de sistemas con el control de aplicaciones AppLocker, nueva Guía CCN-STIC

- ***La Guía detalla la funcionalidad existente con AppLocker y cómo ayuda a proteger contra la ejecución de código dañino o aplicaciones no controladas por la organización.***

- ***El documento forman parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Microsoft (CCN-STIC 500), siendo de aplicación para la Administración y de obligado cumplimiento para los Sistemas que manejan información clasificada Nacional.***

Madrid, 19 de febrero de 2016.- El Centro Criptológico Nacional (CCN) ha publicado en la parte privada del portal del CCN-CERT su ***Guía CCN-STIC 596 Protección de sistemas con AppLocker.*** El documento se ha elaborado para proporcionar información sobre cómo implementar este control de aplicaciones en una configuración restrictiva de seguridad. Se incluyen, además, operaciones básicas de configuraciones adicionales, desactivación del componente, entre otros aspectos, además de aquellas acciones que deben ser llevadas a cabo para el adecuado mantenimiento del servicio.

La Guía incluye también una descripción sobre las características de AppLocker y cómo ayuda a proteger contra la ejecución de código dañino o aplicaciones no controladas por la organización, así como los riesgos de la ejecución de aplicaciones.

Directivas de AppLocker, un paso a paso en infraestructuras de dominio, mantenimiento, procedimientos de aplicación en clientes y servidores independientes, así como una lista de comprobación para verificar el grado de cumplimiento de un servidor o puesto de trabajo con respecto a las condiciones de seguridad que se establecen en la guía, son otros de los aspectos abordados en el documento.

La Guía forman parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Microsoft (CCN-STIC 500), siendo de aplicación para la Administración y de obligado cumplimiento para los Sistemas que manejan información clasificada Nacional.

19 de febrero de 2016

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 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, 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

https://www.youtube.com/watch?v=5XxS9mZZfKs