



Los responsables de seguridad de los sistemas tienen como límite el próximo 29 de enero de 2014 para adecuarse al Esquema

Cumplido el primer plazo para la adecuación de los sistemas de la Administración al Esquema Nacional de Seguridad

- **Así lo recoge la disposición transitoria del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.**
- **Para ayudar a la elaboración de este plan de adecuación el Centro Criptológico Nacional pone a disposición de todas las administraciones públicas la Guía CCN-STIC 806 disponible en el portal <http://www.ccn-cert.cni.es/ens>**

Madrid, 4 de febrero de 2011. La disposición transitoria del *Real Decreto 3/2010, de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*, publicado en el BOE el 29 de enero de 2010, articula el siguiente mecanismo escalonado para la adecuación a lo previsto en el Esquema Nacional de Seguridad: los sistemas de las administraciones deberán estar adecuados a este Esquema en el plazo de **doce meses**, aunque si hubiese circunstancias que impidan la plena aplicación, se dispondrá de un **plan de adecuación** que marque los plazos de ejecución, en ningún caso superiores a 48 meses desde la entrada en vigor. El primer plazo de 12 meses se cumplió el pasado 29 de enero de 2011 y el segundo plazo de 48 meses el 29 de enero de 2014.

El citado **plan de adecuación** será elaborado por el Responsable de Seguridad del sistema, deberá estar aprobado por los órganos superiores competentes y contendrá la siguiente información:

- La política de seguridad.
- Información que se maneja, con su valoración.
- Servicios que se prestan, con su valoración.
- Datos de carácter personal.
- Categoría del sistema.
- Declaración de aplicabilidad de las medidas del Anexo II del ENS.
- Análisis de riesgos.
- Insuficiencias del sistema.
- Plan de mejora de seguridad, incluyendo plazos estimados de ejecución.

Para ayudar a la elaboración de este plan de adecuación se dispone de la **Guía CCN-STIC 806 - Plan de Adecuación del Esquema Nacional de Seguridad**. Esta guía y otras que pueden ser de especial utilidad, tales como la *Guía 801 - Responsables y Funciones en el Esquema Nacional de Seguridad*, la *Guía 803 - Valoración de*

sistemas en el Esquema Nacional de Seguridad, la Guía 804 - Medidas de implantación del Esquema Nacional de Seguridad, Guía 805 - Política de Seguridad de la Información, junto con herramientas para la realización del análisis y gestión de riesgos, todo ello disponible en el portal <http://www.ccn-cert.cni.es/ens>.

Sobre CCN-CERT

El servicio de Respuesta ante Incidentes de Seguridad de la Información, CCN-CERT, fue creado en 2006 por el Centro Criptológico Nacional del Centro Nacional de Inteligencia, con el fin de contribuir a la mejora del nivel de seguridad de los sistemas de información de las administraciones públicas españolas (general, autonómica y local).

El CERT gubernamental español asesora a todas ellas en la implantación de medidas tecnológicas que mitiguen el riesgo de sufrir cualquier ataque, colabora en la resolución de cualquier incidente, facilita cursos de formación y proporciona información sobre vulnerabilidades, alertas y avisos de amenazas a los sistemas de información.

Para desempeñar de forma óptima estas funciones, el CCN-CERT cuenta con un portal en Internet (www.ccn-cert.cni.es), desde donde ofrece los servicios mencionados. Además, forma parte de prestigiosos organismos internacionales (como el Grupo EGC -European Government CERTs Group-, el FIRST -Forum of Incident Response and Security Team- o el Trusted Introducer), con quienes comparte objetivos, ideas e información relevante sobre seguridad informática.

MÁS INFORMACIÓN

Clara Baonza
cbaonza@tb-security.com
TB·Security
(+34) 91 301 34 95

Centro Criptológico Nacional
Avda. del Padre Huidobro, Km. 8,500
28023 Madrid
www.ccn-cert.cni.es
info@ccn-cert.cni.es