



El CERT Gubernamental pone en marcha el Informe Nacional del Estado de la Seguridad, INES, accesible desde su portal [www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)

## Facilitar la adecuación al Esquema Nacional de Seguridad, objetivo del nuevo proyecto INES del CCN-CERT

- La nueva plataforma proporciona a las distintas Administraciones Públicas un conocimiento más rápido e intuitivo de su nivel de Adecuación al Esquema Nacional de Seguridad y del estado de seguridad de sus sistemas, tal y como recoge el artículo 35 del Real Decreto de regulación del ENS.
- El resultado de una primera fase piloto, que ha contado con la participación de 39 organismos, ha sido muy satisfactorio y permitirá la elaboración de un informe preliminar que será presentado en el recientemente creado Comité Ejecutivo de la Comisión de Estrategia TIC de la Administración General del Estado y sus Organismos Públicos.

Madrid, 13 de octubre de 2014.- El **CCN-CERT**, del Centro Criptológico Nacional, CCN, ha puesto en marcha, en colaboración con el Ministerio de Hacienda y Administraciones Públicas, un proyecto para facilitar la labor de todos los organismos de cara a conocer el estado de seguridad de sus sistemas y, por tanto, su adecuación al **Esquema Nacional de Seguridad, ENS**. Se trata del proyecto **INES (Informe Nacional del Estado de la Seguridad)**, una nueva plataforma telemática que proporciona un conocimiento más rápido e intuitivo del nivel de adecuación al ENS y de acceso directo a través del portal [www.ccn-cert.cni.es/ines](http://www.ccn-cert.cni.es/ines) (es preciso estar registrado para acceder a la herramienta).

"El Responsable de Seguridad de cada Organismo será el encargado de la interfaz con INES, proporcionando, validando y analizando la información"

El Real Decreto 3/2010, de 8 de enero, que lo regula, establece la obligación de evaluar periódicamente el estado de la seguridad de los sistemas por parte de las Administraciones Públicas. Así, su **artículo 35** señala: "El Comité Sectorial de Administración Electrónica articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente real decreto, de forma que permita

13 de octubre de 2014

[www.ccn.cni.es](http://www.ccn.cni.es)  
[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)  
[www.oc.ccn.cni.es](http://www.oc.ccn.cni.es)



elaborar un perfil general del estado de la seguridad en las Administraciones públicas". Asimismo, el ENS dispone la necesidad de establecer un sistema de medición de la seguridad del sistema estableciendo un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad, en los siguientes aspectos:

- a) Grado de implantación de las medidas de seguridad.
- b) Eficacia y eficiencia de las medidas de seguridad.
- c) Impacto de los incidentes de seguridad.

La plataforma INES, bajo gestión del CCN-CERT, permite la recogida de información organizada, delegada y supervisada. El **Responsable de la Seguridad** del organismo debe ser el encargado de la interfaz con INES, proporcionando, validando y analizando la información de seguridad propia de su organismo y consolidada a nivel de Administración Pública. Esta figura (art. 10 del RD) es la que determina las decisiones para satisfacer los requisitos de la seguridad de la información y de los servicios y es, además, el responsable de analizar los informes de auditoría regulares (que deben hacerse al menos cada dos años para verificar el cumplimiento de los requerimientos del ENS).



### Fase piloto exitosa

En un primero momento, se ha desarrollado una fase piloto en la que han participado **39 organismos**, tanto de la **Administración General del Estado (AGE)** como de las **Comunidades Autónomas**. Esta fase concluye este mes de octubre, momento en el que se presentará un informe preliminar al recientemente creado **Comité Ejecutivo de la Comisión de Estrategia TIC<sup>1</sup>** y en su caso al **Consejo de Ciberseguridad Nacional**. Posteriormente la plataforma se abrirá al resto de

<sup>1</sup> Órgano colegiado encargado de la definición y supervisión de la aplicación de la Estrategia sobre Tecnologías de la Información y las Comunicaciones de la Administración General del Estado y sus organismos públicos, adscrito al Ministerio de Hacienda y Administraciones Públicas a través de la Secretaría de Estado de Administraciones Públicas. (Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos).

13 de octubre de 2014

[www.ccn.cni.es](http://www.ccn.cni.es)  
[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)  
[www.oc.ccn.cni.es](http://www.oc.ccn.cni.es)



Administraciones Públicas (diputaciones, ayuntamientos, Universidades y otros organismos).

El piloto proporcionará un cuadro de mandos con el nivel de seguridad de los organismos comparado con la media de la AGE/CCAA y la media de todos los organismos que están incluidos en este proyecto preliminar.

### Sobre CCN-CERT

El CCN-CERT ([www.ccn-cert.cni.es](http://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](http://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

Argenta, 20. 28023 Madrid

[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)



[eventos@ccn-cert.cni.es](mailto:eventos@ccn-cert.cni.es)

[ines@ccn-cert.cni.es](mailto:ines@ccn-cert.cni.es)

13 de octubre de 2014

[www.ccn.cni.es](http://www.ccn.cni.es)  
[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)  
[www.oc.ccn.cni.es](http://www.oc.ccn.cni.es)

