Adecuación al Esquema Nacional de Seguridad

Instrumentos para la seguridad en la administración electrónica

Han transcurrido más de dos años desde la entrada en vigor del ***Real Decreto 3/2010**, de 8 de Enero de 2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica* que desarrolla lo previsto en el artículo 42 de la Ley 11/2007. El **Esquema Nacional de Seguridad (ENS)**, elaborado con la participación de todas las Administraciones Públicas, está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información y su objeto es establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la citada Ley.

Transcurrido este tiempo, la seguridad de la información manejada y los servicios prestados por las Administraciones Públicas sigue siendo un aspecto de carácter estratégico para la realización de la administración electrónica y, de hecho, se contempla en la **Estrategia Española de Ciberseguridad**, en elaboración, de manera que constituye uno de sus objetivos y se desarrolla en una de sus líneas de acción orientada a asegurar la plena implantación del Esquema Nacional de Seguridad.

La adecuación ordenada al Esquema Nacional de Seguridad requiere el tratamiento de las siguientes cuestiones básicas:

- Preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades.
- Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados.
- Realizar el análisis de riesgos, que incluye la valoración de las medidas de seguridad existentes.

- Preparar y aprobar la Declaración de Aplicabilidad de las medidas del Anexo II del ENS.
- Elaborar un plan de adecuación para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución.
- Implantar operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad.
- A los dos años, realizar la auditoría de la seguridad, de la cual pueden derivar las acciones de mejora de la seguridad correspondientes.

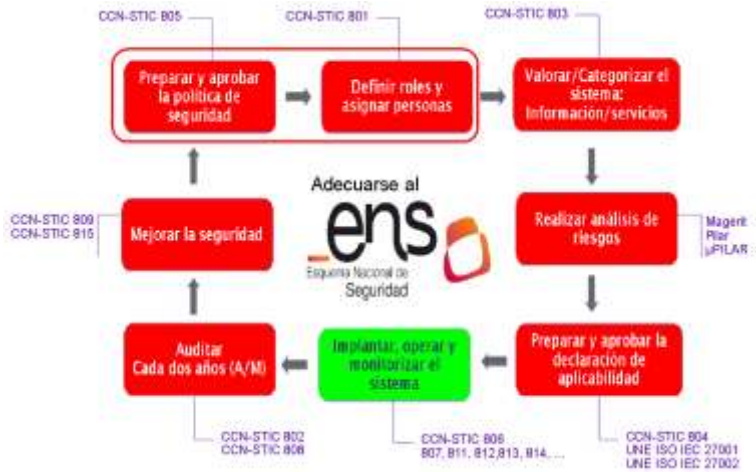

Figura: Acciones claves de la adecuación al Esquema Nacional de Seguridad.

En cualquier caso, a la hora de emprender la adecuación al ENS será **de gran ayuda servirse de lo siguiente**:

- Usar guías e instrumentos específicos.
- Usar las infraestructuras y servicios comunes.
- Usar la normalización.
- Comunicar incidentes de seguridad.
- Usar productos certificados.
- Preguntar.

- Formarse.

En estos dos años se viene desarrollando una intensa y continua actividad de desarrollo de **instrumentos de apoyo para la adecuación al ENS**. Destaca la colección de **guías CCN-STIC** previstas en el artículo 29 del Real Decreto 3/2010 y disponibles en el Portal del CCN-CERT[i], elaboradas por el Centro Criptológico Nacional con apoyo del Ministerio de Hacienda y Administraciones Públicas (MINHAP). Se han publicado las guías CCN-STIC siguientes:

- 800 - Glosario de Términos y Abreviaturas del ENS.
- 801 - Responsables y Funciones en el ENS.
- 802 - Auditoría del ENS.
- 803 - Valoración de sistemas en el ENS.
- 804 - Medidas de implantación del ENS.
- 805 - Política de Seguridad de la Información.
- 806 - Plan de Adecuación del ENS.
- 807 - Criptología de empleo en el ENS.
- 808 - Verificación del cumplimiento de las medidas en el ENS.
- 809 - Declaración de Conformidad del ENS.
- 810 - Guía de Creación de un CERT/CSIRT.
- 812 - Seguridad en Entornos y Aplicaciones Web.
- 813 - Componentes certificados.
- 814 - Seguridad en correo electrónico.
- 815 - Indicadores y Métricas en el ENS.
- 817 - Criterios para la Gestión de Incidentes de Seguridad en el ENS.

Se trabaja para incorporar **nuevas guías** que orienten en cuestiones tales como los procedimientos operativos de seguridad, la denegación de servicio y la computación en la nube, entre otras cuestiones. Otra línea de trabajo en curso contempla la

identificación **medidas del ENS de alto impacto y de bajo coste** al objeto de proporcionar orientación que ayude a agilizar la mejora de la seguridad.

Estas guías se acompañan de herramientas para la realización del análisis y gestión de riesgos, como la metodología MAGERIT v2 (cuya versión 3 ya elaborada se publicará próximamente) y las herramientas PILAR y μPILAR que incluyen el perfil de protección del Esquema Nacional de Seguridad.

Adicionalmente, de acuerdo con lo previsto en los artículos 36 y 37 del citado Real Decreto 3/2010, están disponibles los **servicios de respuesta ante incidentes de seguridad CCN-CERT**; complementados con los **Servicios de Alerta Temprana en la Red SARA**.

Por otra parte se encuentran los servicios del **Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información**[ii] relativos a la acreditación de laboratorios y a la certificación de productos de seguridad de las tecnologías de la información.

Además, se viene perfeccionando progresivamente la colección de **'preguntas frecuentes' relativas al ENS** sobre la base de la resolución de dudas suscitadas acerca de la aplicación del mismo.

Finalmente, todo lo anterior se completa con la **formación** en seguridad de las tecnologías de la información y las comunicaciones, **presencial**, a través de los **cursos STIC** que imparte CCN en colaboración con el MINHAP y el INAP; así como **en línea** mediante el curso de iniciación al ENS (20 horas) y el curso introductorio a la herramienta PILAR (10 horas) en las partes públicas y privadas del Portal del CCN-CERT.

[i] https://www.ccn-cert.cni.es/ , https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2420&Itemid=211&lang=es

[ii] http://www.oc.ccn.cni.es/