El Esquema Nacional de Seguridad, cinco retos próximos

Transcurridos cinco años desde la publicación del Esquema Nacional de Seguridad (ENS) en enero de 2010, se plantean retos en cuanto a conocer e informar acerca del estado de la seguridad de las administraciones públicas; asegurar la plena implantación del Esquema; implantar servicios comunes que favorezcan la seguridad del conjunto y reduzcan el esfuerzo individual; actualizar el ENS a la luz de la experiencia y de la evolución del contexto tecnológico y regulatorio en la Unión Europea; y, finalmente, publicar la conformidad como manifestación expresa de cumplimiento con el ENS.

MIGUEL ÁNGEL AMUTIO
Subdirector Adjunto de Coordinación de Unidades TIC Dirección de Tecnologías de la Información y las Comunicaciones

Transcurridos cinco años desde la publicación del Esquema Nacional de Seguridad (Real Decreto 3/2010) en enero de 2010, las administraciones públicas manejamos un planteamiento común de principios, requisitos y medidas para la seguridad de los sistemas de información que impulsa la gestión continuada de la misma, imprescindible en un escenario de prestación de servicios 24 x 7 y de transformación digital, a la vez que un tratamiento homogéneo de la seguridad que facilita la cooperación interadministrativa, constituye un referente de buenas prácticas y configura un escenario uniforme de cara a la provisión de servicios por parte de la Industria. Nos hemos dotado también de una exhaustiva colección de instrumentos como guías (serie CCN-STIC 800), así como de herramientas y servicios de respuesta ante incidentes disponibles en el Portal CCN-CERT **(1)**.

Esta senda ha recibido el respaldo de la Estrategia Española de Ciberseguridad que en su Objetivo I se refiere a "Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia" y que incluye una línea de acción al respecto con referencia a la implantación del ENS. Por otra parte, en un contexto más general de transformación digital, las recientes Recomendaciones de la OCDE para el desarrollo de Estrategias de Administración Digital **(2)** se refieren a "Establecer un marco de gestión de riesgos para garantizar la seguridad digital y la preservación de la privacidad, así como adoptar medidas de seguridad efectivas".

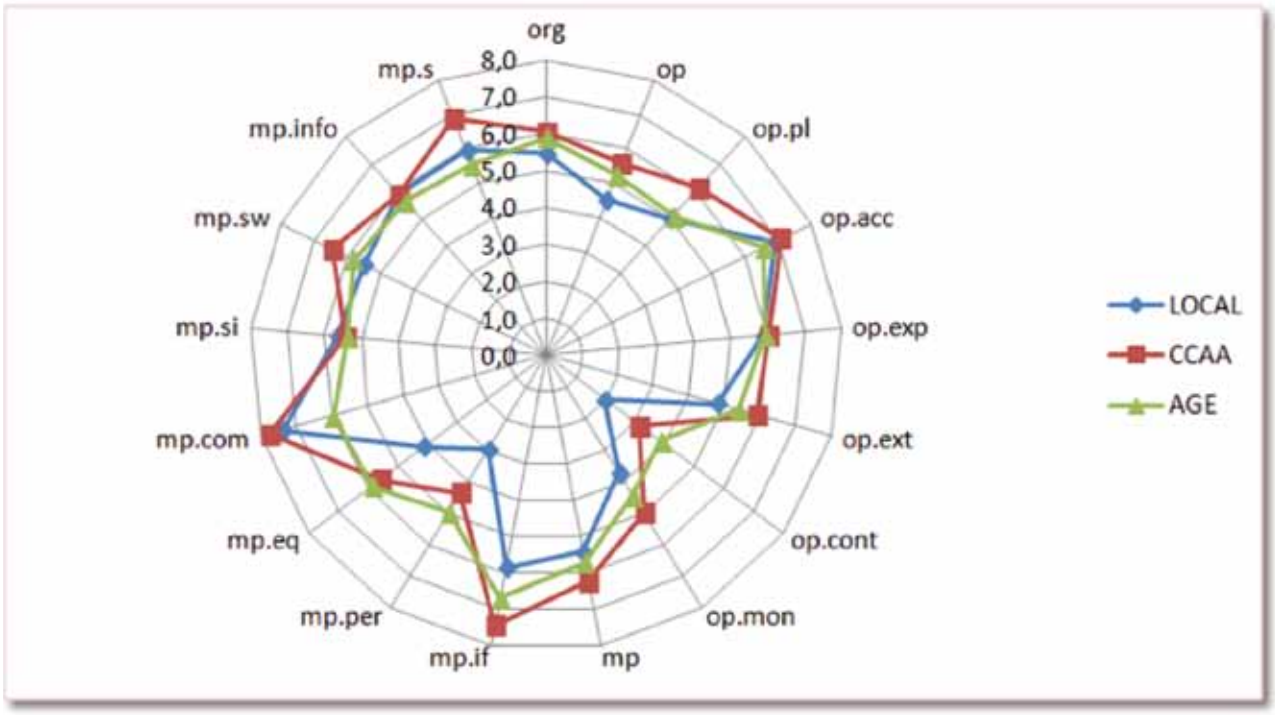

FIGURA 1. Situación en Diciembre 2014. Fuente INES

Es momento de preguntarse dónde estamos, hacia dónde vamos y de recapitular los retos que se presentan por delante, en concreto los cinco retos que se exponen a continuación.

Reto 1: Conocer e informar del estado de la seguridad

Saber dónde estamos es relevante. Los datos son necesarios para estimar la eficacia y la eficiencia de las actuaciones en materia de la seguridad TIC; para estimar el esfuerzo humano y económico dedicado a la misma; así como para argumentar mejores alternativas. Previendo esta necesidad, el ENS exige, mediante lo establecido en su artículo 35, conocer regularmente el estado general de la seguridad en las administraciones públicas, para lo cual es preciso, en primer lugar, llevar a cabo la medición de la seguridad (véase la medida 4.6.2 Monitorización del sistema [op.mon.2]), a través la implementación de indicadores que permitan medir el desempeño real del sistema en términos del grado de implantación de las medidas de seguridad, de la eficacia y eficiencia de las mismas, así como del impacto de los incidentes de seguridad; y, en segundo lugar, consolidar y difundir dichos datos mediante el informe correspondiente. Esta información es de interés para el conjunto, pero también para cada actor en particular, en la medida en la que permite contrastar cada situación individual frente a la general de los demás.

Desplegada en 2014, la herramienta INES (Informe Nacional del Estado de la Seguridad) **(3)** facilita la recogida y consolidación de información para el Informe del Estado de la Seguridad, previsto en el citado artículo 35 del Real Decreto 3/2010, así como en la línea de acción 2 de la Estrategia de Ciberseguridad Nacional **(4)** . La dinámica ya está puesta en marcha, si bien toca asentarla, principalmente, promoviendo el incremento del nivel de participación de todas las AA.PP., especialmente de CC.AA. y EE.LL., y mejorando los indicadores relativos a los recursos humanos y económicos dedicados a la seguridad.

Ahora bien, la medición requiere manejar dos facetas de la implantación de las medidas de seguridad. Estas dos facetas son, por un lado, el índice de cumplimiento, para evaluar la satisfacción de las medidas que se exigen en función de los niveles de seguridad o de la categoría del sistema; y, por otro lado, el índice de madurez de las medidas implantadas en la organización. Para esta segunda faceta, la orientación proporcionada a través de las guías CCN-STIC 815 Métricas e indicadores y 824 Informe del estado de seguridad **(5)** se basa en establecer un nivel de madurez de referencia para cada medida

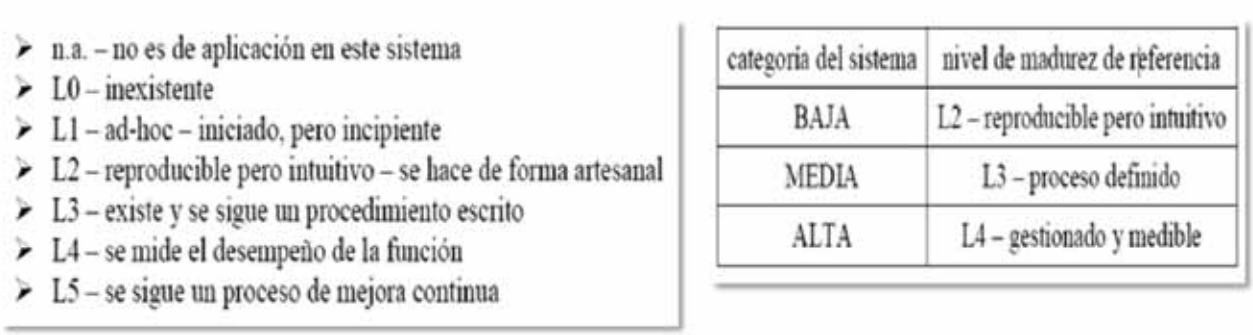

FIGURA 2. Correspondencia entre la categorización de los sistemas y los niveles de madurez. Fuente: Guía CCN-STIC 815 Métricas e indicadores.

de protección del Anexo II del ENS mediante una regla simple de correspondencia entre la categorización de los sistemas y los niveles de madurez, según se muestra ilustrativamente en la FIGURA 2.

Reto 2: Asegurar la plena implantación del ENS

Los datos consolidados a finales de 2014 y obtenidos de INÉS a partir de la información aportada por unas 120 entidades de la AGE, CC.AA. y EE.LL. (FIGURA 1), permiten constatar, tanto el esfuerzo realizado en estos años desde la publicación del ENS, como el que queda por delante (en términos de implantación de las medidas y de la madurez de las mismas), a la vez que identifican aspectos que demandan una atención especial.

Consciente de que el logro de unos niveles óptimos de seguridad requiere continuidad, la Estrategia de Ciberseguridad Nacional incluye en su línea de acción 2, titulada "Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas", la medida relativa a "Asegurar la plena implantación del Esquema Nacional de Seguridad y articular los procedimientos necesarios para conocer regularmente el estado de las principales variables de seguridad de los sistemas afectados".

Por otra parte, aunque, a la fecha, el ámbito de aplicación del ENS se ciñe a los previsto en el artículo 2 de la Ley 11/2007, estando excluidos los sistemas que manejan información clasificada, la seguridad requiere contemplar y tratar adecuadamente el escenario global de riesgos, con independencia de si existe o no relación electrónica con ciudadanos u otras entidades y de si tal relación tiene lugar utilizando medios tecnológicos o procedimientos manuales. El siguiente paso lógico parece, por tanto, extender la aplicación del ENS a aquellos otros sistemas no contemplados originariamente en su ámbito de aplicación, con el objetivo de que la protección de la generalidad de los sistemas de información de las AA.PP. se ampare en un mismo enfoque de principios, requisitos y medidas de seguridad.

Reto 3: Implantar servicios comunes.

Ciertas medidas de seguridad se pueden implementar mediante servicios prestados de forma centralizada, servicios que ofrecen oportunidades para aumentar de forma notable la seguridad de los sistemas de información y comunicaciones del conjunto, a la vez que reducen el esfuerzo individual de las entidades integradas en los mismos, dando lugar en términos económicos, a una consolidación, frente al coste de las acciones individuales.

Adicionalmente, las infraestructuras y servicios comunes también ofrecen oportunidades en materia de seguridad, tales como la reducción del perímetro físico que aligera la carga en medidas de protección de las instalaciones e infraestructuras [mp.if] para las entidades usuarias; la reducción del perímetro lógico que aligera la carga para las entidades usuarias en medidas de explotación [mp.exp], de protección de las aplicaciones informáticas [mp.sw], de protección de los servicios [mp.s] y de monitorización del sistema [op.mon]; la reducción de la carga de gestión de incidentes [op.exp7]; la mejora de la elasticidad para hacer frente a picos de actividad o a ataques de denegación de servicio [mp.s.8]; o la mejora de la conformidad con estándares para facilitar la recuperación, integración, interoperabilidad, portabilidad, e integración con herramientas de seguridad (medidas varias de tipo [op]).

Reto 4: Actualizar el ENS

Además de lo establecido en el artículo 42 'Actualización permanente' del Real Decreto 3/2010, justifican la actualización del ENS razones tales como la experiencia obtenida a partir de la implantación del mismo en las AA.PP. desde su publicación en

Saber dónde estamos es relevante. Los datos son necesarios para estimar la eficacia y la eficiencia de las actuaciones en materia de la seguridad TIC; para estimar el esfuerzo humano y económico dedicado a la misma; así como para argumentar mejores alternativas

enero de 2010; los comentarios recibidos por diversas vías, tanto formales como informales, en el curso de los trabajos relativos al seguimiento del progreso de la adecuación al ENS realizados en 2013 y 2014 y al informe del estado de la seguridad; la evolución de la tecnología y las ciberamenazas; y el contexto regulatorio europeo, especialmente por razón de la publicación en agosto de 2014 del Reglamento nffl 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE **(6)** que afecta a varias medidas del seguridad recogidas en el anexo II del ENS.

Los aspectos principales de la actualización del ENS, de forma muy resumida, son los que siguen:

• Se enfatiza que la política de seguridad 'articule la gestión continuada de la seguridad' (art.11).

• Se introduce la noción de 'profesionales cualificados' (art.15).

• En relación con la adquisición de productos certificados, se introduce la noción de la proporcionalidad a la categoría del sistema y nivel de seguridad determinados y a los riesgos (art. 18).

• La relación de medidas seleccionadas del anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de seguridad (art. 27).

• Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (art. 27).

• Se introducen las 'instrucciones técnicas de seguridad' para señalar el modo común de actuar en ciertos aspectos (art. 29), tales como: Informe del estado de la seguridad, Notificación de incidentes de seguridad, Auditoría de la seguridad, Conformidad con el Esquema Nacional de Seguridad, Adquisición de productos de seguridad, Criptología de empleo en el Esquema Nacional de Seguridad, Interconexión en el Esquema Nacional de Seguridad, Requisitos de seguridad en entornos externalizados

• Se mejoran los mecanismos para obtener un conocimiento regular del estado de la seguridad en las AA.PP. (art. 35).

• Se introduce la notificación de incidentes de seguridad (art. 36); la figura de la notificación de los hechos que tengan un impacto significativo en la seguridad es una tendencia en proyectos normativos de la Unión Europea.

• Se precisan los elementos necesarios para la investigación de incidentes de seguridad (art. 37) para que se puedan tener en cuenta evidencias tales como informes de auditoría, registros de auditoría, configuraciones, así como los soportes informáticos.

• Se mejora la eficacia de ciertas medidas de seguridad (Anexo II). Cabe destacar ciertas medidas afectadas por el Reglamento 910/2014 como 4.2.1 Identificación [op.acc.1], 4.2.5. Mecanismo de autenticación [op.acc.5], 5.7.4. Firma electrónica [mp.info.4] o 5.8.2. Protección de servicios y aplicaciones web [mp.s.2]; las medidas relacionadas con 4.1.5 Componentes certificados [op.pl.5]; u otras, entre las que cabe destacar 3.4 Proceso de autorización [org.4], 4.1.2. Arquitectura de seguridad [op.pl.2], 4.3.8. Registro de la actividad de los usuarios [op.exp.8], 4.6.1. Detección de intrusión [op.mon.1], 4.6.2. Sistema de métricas [op.mon.2], 5.5.5. Borrado y destrucción [mp.si.5], 5.6.1. Desarrollo de aplicaciones [mp.sw.1] y 5.7.7. Copias de seguridad [mp.info.9].

Reto 5: Publicar la conformidad con el ENS

Es el cierre del círculo; la publicación de la conformidad con el ENS, prevista en su artículo 41, es la manifestación expresa de que el sistema cumple lo establecido en el mismo y se materializaría mediante las correspondientes declaraciones en las sedes electrónicas, en su caso, junto con otros distintivos de seguridad. Se hizo un planteamiento razonablemente abierto para esta cuestión, sin embargo, hoy en día ya se pone de manifiesto la necesidad de configurar un escenario más concreto y claro sobre la forma de obtener y publicar la conformidad.

Algunas conclusiones

El Esquema Nacional de Seguridad, de aplicación a todas las administraciones públicas, persigue la creación de condiciones adecuadas de seguridad para el ejercicio de derechos y cumplimiento de deberes por medios electrónicos, impulsa la gestión continuada de la seguridad imprescindible en un escenario de prestación de servicios 24 x 7 y de transformación digital, a la vez que un tratamiento homogéneo de la seguridad que facilite la cooperación, proporcionando principios requisitos y medidas de seguridad comunes.

Tras el recorrido realizado desde 2010, se plantean retos en cuanto a conocer e informar acerca el estado de la seguridad de las administraciones públicas; asegurar la plena implantación del Esquema; implantar servicios comunes que favorezcan la seguridad del conjunto y reduzcan el esfuerzo individual; actualizar el ENS a la luz de la experiencia y de la evolución del contexto tecnológico y regulatorio en la Unión Europea; y, finalmente, publicar la conformidad como manifestación expresa de cumplimiento con el ENS.

Siempre hay que recordar que se trata de un esfuerzo colectivo de todas las administraciones públicas (AGE, CC.AA., EE.LL. (FEMP), Universidades (CRUE), ámbito de Justicia (EJIS), coordinado por el MINHAP y el CCN, más las aportaciones de la Industria sector TIC, en el contexto del convencimiento común de la necesidad de la seguridad de los sistemas de información adaptada al quehacer de la Administración, cuestión en la que los profesionales TIC desempeñan un papel esencial. ✱

NOTAS

(1) *https://www.ccn-cert.cni.es/*

(2) *http://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2014/Agosto/Noticia-2014-08-12-Recomendaciones-OCDE-estrategias-Adigital.html*

(3) *https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=3741&Itemid=210&lang=es*

(4) *http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf*

(5) *Disponibles en el portal CCN-CERT, https://www.ccn-cert.cni.es/ , en la sección del ENS, junto con las demás guías de la serie 800.*

(6) *http://www.boe.es/doue/2014/257/L00073-00114.pdf*

El Esquema Nacional de Seguridad, de aplicación a todas las administraciones públicas, persigue la creación de condiciones adecuadas de seguridad para el ejercicio de derechos y cumplimiento de deberes por medios electrónicos