SEGURIDAD DE
LA INFORMACIÓN

Certificación del Esquema Nacional de Seguridad

La finalidad del Esquema Nacional de Seguridad (ENS) es crear las condiciones necesarias para generar la confianza de los ciudadanos en el uso de los servicios electrónicos ofrecidos por las Administraciones Públicas. Por ello, sus sistemas de información deberán estar adecuados al ENS antes de noviembre de 2017; y en todo este proceso la certificación de conformidad en el cumplimiento de este esquema y su mantenimiento juegan un papel determinante. En la actualidad, AENOR ha emitido más de diez certificaciones ENS a distintas entidades públicas.

Redacción

Para que la comunicación a través de medios electrónicos entre los ciudadanos y las Administraciones Públicas sea efectiva y esté basada en la confianza es necesario que se proteja la información, y que los sistemas que gestionan dicha información presten sus servicios sin interrupciones, modificaciones o accesos no deseados. Con esta finalidad se ha desarrollado el Esquema Nacional de Seguridad (ENS), definido en el RD 3/2010 y modificado posteriormente con el RD 951/2015, que propone unos principios básicos y unos requisitos mínimos que se alcanzan aplicando a los sistemas de información un conjunto de medidas de seguridad.

El ámbito de aplicación del ENS se establece en el artículo 2 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos. Para generar y acreditar esa confianza en los ciudadanos, el propio ENS define unos mecanismos de verificación y transparencia. El mecanismo de verificación es la auditoría de seguridad descrita en el artículo 34 y Anexo III. Concretamente, el punto 4 de este artículo dice *En la realización de esta auditoría se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información*. Asimismo, en la disposición transitoria del Real Decreto 3/2010 se articula un mecanismo escalonado para la adecuación a lo previsto en el ENS. Por ello, los sistemas de información de las Administraciones Públicas deberán estar adecuados al ENS antes de noviembre de 2017; y en todo este proceso la certificación de conformidad en el cumplimiento de este esquema

y su mantenimiento juegan un papel determinante.

Para explicar la situación actual de la implantación del ENS en la Administración Pública, así como ofrecer las herramientas necesarias para llevar a cabo la adecuación de los sistemas de seguridad de la información según los requisitos legales y en el plazo establecido, se celebró en AENOR el 28 de junio la jornada *Certificación Esquema Nacional de Seguridad*. Dirigida a responsables de seguridad de entidades públicas y profesionales con competencias en la administración electrónica, contó con la participación de expertos de Start Up, Centro Cripotológico Nacional (CCN-CERT) y AENOR. La apertura y presentación corrió a cargo de Luis Gómez, Director de Start Up, quien afirmó que "el ENS es un recurso muy útil para las Administraciones Públicas y para quienes tienen la responsabilidad de los sistemas informáticos. Sin duda, la certificación contribuirá al éxito de este esquema y a mejorar su grado de cumplimiento".

Implantación

Nora Pacheco y Pablo López, expertos del Departamento de Ciberseguridad del Centro Criptológico Nacional (CCN), participaron en esta jornada hablando sobre el estado de implantación del ENS y la conformidad con este esquema. Nora Pacheco hizo un repaso de los principios básicos, requisitos mínimos y las medidas de seguridad que incluye el ENS para llevar a cabo una protección adecuada de la información. El CCN es el organismo encargado de articular los procedimientos necesarios para la recogida y tratamiento de la información en relación con las variables de seguridad del ENS. "Por este motivo, vimos la necesidad de crear una herramienta que favoreciera toda esta recogida de información. De esta forma surgió INES (Informe Nacional del Esquema de Seguridad)" explicó Pacheco. Se trata de una plataforma *on line* que facilita a las distintas Administraciones Públicas un conocimiento más rápido e intuitivo de su nivel de adecuación al ENS y del estado de seguridad de sus sistemas.

Por su parte, Pablo López explicó los puntos básicos para alcanzar la conformidad con el ENS. Señaló varios aspectos que hay que tener en cuenta para lograr esta adecuación, como preparar y aprobar la política de seguridad, definir roles, categorizar los sistemas o realizar el análisis de riesgos. En este sentido, los dos procedimientos de verificación establecidos para alcanzar la conformidad con el esquema son la autoevaluación, realizada por el mismo personal que administra el sistema de información o aquel otro en quién se haya delegados; este procedimiento está reservado para sistemas de categoría básica e implica una Declaración de Conformidad. Y la auditoría formal, con las garantías metodológicas y de independencia profesional y adecuación requeridas que supone una Certificación de Conformidad, y está destinada a los sistemas de categoría media y alta. Este certificado de conformidad debe ser emitido por una entidad acreditada por la Entidad Nacional de Acreditación (ENAC), como es el caso de AENOR.

Pablo López destacó que el ENS es un marco regulatorio que permitirá

SEGURIDAD DE LA INFORMACIÓN

disponer de una Administración Pública aún más segura. "El ENS debe contribuir a formar una comunidad concienciada con la ciberamenaza que comparta soluciones a problemas comunes en las Administraciones Públicas", subrayó López.

Adecuación al ENS

El Director Técnico de Start Up, Pedro Pablo Fernández, explicó en profundidad los pasos que las entidades deben seguir para alcanzar con éxito la certificación en el ENS. Así, dividió el proceso en ocho pasos: política de seguridad; categorización de sistemas; análisis de riesgos; declaración de aplicabilidad; plan de mejora de seguridad e insuficiencias del sistema; desarrollo de normativa y procedimientos con la consiguiente implantación; mejora continua y auditoría de certificación.

Hizo especial hincapié en el mantenimiento del ENS, esto es, el paso relativo a la mejora continua. "La gestión de la seguridad de la información es un proceso sujeto a cambios constantes, por ello es necesario implantar un proceso de actualización permanente", explicó Pedro Pablo Fernández. Así, el proceso de actualización debe incluir una revisión de la política de seguridad de la información, así como de los servicios e información y su categorización, entre otros aspectos. En definitiva, se trata de aplicar un ciclo de mejora continua (Planificar-Hacer-Verificar-Actuar) partiendo del trabajo realizado.

Similitudes con la ISO 27001

La jornada concluyó con la intervención de Carlos Manuel Fernández y Boris Delgado, Gerente y Coordinador de TIC de AENOR, respectivamente, quienes explicaron la interrelación de la certificación UNE-ISO/IEC 27001 y la certificación de conformidad ENS. "La certificación ISO 27001 ayuda a cubrir el 75 % de los requisitos del ENS", afirmó Carlos Manuel Fernández. Y es que, la *Guía de Seguridad CCN-STIC 825 del Esquema Nacional de Seguridad* reconoce la certificación UNE-ISO/IEC 27001 como soporte de cumplimiento del ENS, ya que este esquema contempla y exige la gestión continuada de la seguridad, para lo que debe aplicar un sistema de gestión de seguridad de la información. Además, las organizaciones que hayan certificado sus servicios o sistemas de acuerdo con la Norma UNE-ISO/IEC 27001 están muy cerca de asegurar el cumplimiento del ENS, cuya conformidad debe alcanzarse siguiendo la metodología descrita en los Anexos I, II y II del Real Decreto 3/2010.

El certificado de conformidad en el cumplimiento del Esquena Nacional de Seguridad debe ser emitido por una entidad acreditada por ENAC, como es el caso de AENOR

En este sentido, el Anexo II del mencionado Real Decreto establece 75 medidas de seguridad para el ENS y el Anexo A de la Norma UNE-ISO/IEC 27001 incluye 114 controles. Por tanto, la interrelación del ENS con la norma internacional es amplia. Estableciendo paralelismos, un sistema de gestión define una política, unos objetivos y el modo de conseguirlos. En el caso del SGSI hablaríamos de política de seguridad de la información, requisitos u objetivos de seguridad de la información y la aplicación de un conjunto de controles técnicos y organizativos para conseguirlos. En el ENS, la definición de la política de seguridad de la información es un requisito exigido. Los niveles de seguridad que hay que lograr se derivan de la categorización de los sistemas (Anexo I) y en función de ésta el Anexo II define

Más de 50 profesionales asistieron a la jornada "Certificación ENS", organizada por AENOR

las medidas de seguridad (controles que hay que implantar).

Tanto el SGSI como el ENS formalizan en el documento *Declaración de Aplicabilidad* la relación de controles/medidas de seguridad que hay que implantar. Ante la posibilidad de disparidad o diferencia entre los controles propuestos por la Norma UNE-ISO/IEC 27001 y las medidas de seguridad identificadas en el Anexo II del ENS, la propia norma elimina esta posible barrera que aparece en el párrafo 6.1.3 *Tratamiento de los riesgos de seguridad de la información*, en su punto b, que dice: *Determinar todos los controles que sean necesarios para poner en práctica la opción de tratamiento de riesgos de seguridad de la información elegida. NOTA: Las organizaciones pueden diseñar controles según sea necesario, o identificarlos a partir de cualquier fuente*. Si la fuente utilizada para implantar los controles es el Anexo II del ENS, la superposición es completa.

La selección de controles para realizar las pruebas de cumplimiento en el caso de auditorías conjuntas con la UNE-EN ISO/27001 y el ENS se realizan de acuerdo con la categorización establecida para cada sistema o servicio. La revisión se realiza de forma integrada en aquellos controles comunes con objetivos comunes de acuerdo con la declaración de aplicabilidad; y de forma específica sobre aquellos controles del ENS no contemplados en la UNE-ISO/IEC 27001. Por lo tanto AENOR está en condiciones de emitir certificados de conformidad ENS según la nueva reglamentación. De hecho, ya son más de diez los que ha concedido. ◗

CURSOS Y PUBLICACIONES DE AENOR RELACIONADAS

- **Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001**
- **Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad**

OPINIÓN

Luis Gómez
Director
Start Up

Recurso útil

La certificación del Esquema Nacional de Seguridad (ENS) es una garantía para los ciudadanos que, de esta manera, pueden confiar aún más en la administración electrónica en España. Tanto el Ministerio de Hacienda y Administraciones Públicas como el Centro Criptológico Nacional han realizado un magnífico trabajo para generar un sistema de ayuda dirigido a las Administraciones Públicas para que puedan adecuar sus sistemas de información al ENS en los plazos previstos. No sólo las Administraciones Públicas, y todo lo que depende y gira en torno a ellas, están obligadas a cumplir con el ENS, sino también las empresas privadas que sean proveedores de tecnología y de servicios informáticos. Pero lo más importante es que el ENS no sólo es una obligación; es algo bueno que sitúa a la Administración Pública española en un lugar muy destacado en este ámbito en Europa y el resto del mundo. En España podemos estar muy orgullosos de nuestros servicios públicos y Administración Pública.

AENOR tiene una amplísima experiencia de certificación en el ámbito TIC, en particular con la ISO 27001, por lo que tiene mucho terreno avanzado para jugar un papel importante en el proceso la certificación de conformidad en el cumplimiento del ENS. La certificación *pone en valor* el trabajo de quienes han hecho *los deberes*, le da visibilidad al cumplimiento del ENS y aporta valor. Por su parte, en Start Up también contamos con gran experiencia y hemos llevado a cabo más de 120 implantaciones del ENS en diferentes instituciones y organismos.