El Esquema Nacional de Seguridad

Tras un largo periodo de trabajo y consultas, el 8 de enero de 2010 veía la luz el RD 3/2010, que regula el Esquema Nacional de Seguridad. El ENS es una guía de qué hacer y cómo hacerlo. Un conjunto de principios básicos para que podamos sentirnos razonablemente seguros y, a la vez, generar confianza en la ciudadanía en torno a la Administración electrónica. El Centro Criptológico Nacional ha participado en su elaboración y está involucrado en su implantación. Seguidamente se presenta esta importante herramienta normativa, con especial hincapié en los objetivos por ella perseguidos y en los aspectos más relevantes de su contenido.

POR CARLOS BELSO

El ENS persigue el establecimiento de las condiciones necesarias de confianza en el uso de los medios electrónicos, que permitan a los ciudadanos y a las Administraciones Públicas utilizarlos para el ejercicio de derechos y el cumplimiento de deberes. Asimismo, el ENS contribuye a la introducción de los elementos comunes que han de guiar la actuación de las Administraciones públicas en materia de seguridad TIC, y aporta un lenguaje común para facilitar, tanto la interacción entre las Administraciones públicas, como la comunicación de los requisitos de seguridad TIC a la Industria.

El ámbito de aplicación del ENS coincide con el de la Ley de acceso electrónico de los ciudadanos a los Servicios Públicos: las diversas Administraciones -Central, Autonómica y Local- y los ciudadanos -en sentido amplio-. Se aplicará, tanto en las relaciones de los ciudadanos con las Administraciones Públicas, como en las relaciones entre las distintas Administraciones.

Considerando el amplio conocimiento y experiencia del CCN sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el ENS le ha encomendado una doble tarea: por un lado, la elaboración y difusión de las guías CCN-STIC y, por otro, la coordinación de la respuesta ante los incidentes de seguridad, por medio de su Equipo de Respuesta ante Incidentes (CCN-CERT)

Las guías CCN-STIC constituyen un conjunto de normas, instrucciones, guías y recomendaciones elaboradas para establecer un marco de referencia que garantice la seguridad de los sistemas TIC de las Administraciones y para servir de apoyo a su personal responsable de la seguridad TIC. Estas guías están divididas en series: aquéllas numeradas desde el 000 al 300 (Políticas, Procedimientos, Normas e Instrucciones Técnicas) son de obligado cumplimiento; mientras que, las numeradas entre el 400 y el 900 (Guías de carácter general, entorno Windows, otros entornos e Informes Técnicos) tienen carácter orientativo.

La publicación del ENS no representa el final del camino, sino el inicio de la senda de su implantación:

* Las Administraciones deben aplicar lo establecido en el ENS a cualquier sistema nuevo y adecuar al mismo los sistemas existentes, en un plazo de entre 12 y 48 meses, desde la entrada en vigor del decreto.

* En lo referente a las guías STIC, el CCN está trabajando actualmente

en una serie dedicada específicamente al ENS, que se ya se encuentra en fase de recepción de comentarios de las distintas administraciones.

* El CCN, el CCN-CERT en particular, para cumplir lo establecido acerca de la prestación de servicios a la comunidad, precisa de un redimensionamiento de sus estructuras, de cara a afrontar los nuevos requerimientos planteados. En la situación económica actual parece utópico pensar que ello pueda suceder a corto plazo, por lo que la mayoría de los esfuerzos probablemente se centrarán en las actividades de formación relativas al ENS, en colaboración con el INAP. En esa línea, el VII Curso STIC, incluido entre los cursos informativos y de concienciación en Seguridad del presente año, ya ha estado enfocado al ENS.

* En otro orden de cosas, la implantación del ENS, además de apoyar el desarrollo del tejido industrial de la alta tecnología, pretende colaborar con la racionalización del gasto: la aplicación racional del Esquema y de las guías de acompañamiento debe reducir el gasto en consultorías y productos innecesarios.

* Por último, la puesta en marcha del ENS contribuirá a la concienciación de la Sociedad acerca de la importancia del concepto de la seguridad, en particular, la seguridad TIC.

El éxito en la aplicación del esquema va a depender de la concienciación de todos los participantes en la gestión de la seguridad y, sobre todo, de la del responsable jerárquico de la Organización.

Quizá el punto más débil de la implantación del ENS resida en la condición de autoevaluación de las auditorías de seguridad requeridas. Se debe confiar en los responsables de definir las políticas, implantar las medidas y gestionar los sistemas, pero es conveniente afianzar esta confianza proporcionando a los responsables de la organización instrumentos para comprobar el nivel de cumplimiento, así como recordándoles el riesgo que conlleva el incumplimiento del ENS, en forma de posibles responsabilidades: administrativa (nulidad o invalidez de los actos), disciplinaria, patrimonial de la administración o del funcionario, e, incluso, penal.

Lo más adecuado será certificar el sistema usando la metodología Margerit, de análisis y gestión de riesgos, y su herramienta complementaria, PILAR. Ambos son el resultado de sendos desarrollos patrocinados por la Administración española y están ampliamente extendidos, dentro y fuera de España.

Adicionalmente, el ENS impulsa la gestión continuada de la seguridad, mediante actuaciones formalizadas, permitiendo auditorías basadas en estándares internacionales que suscitan consenso y refuerzan la confianza, como la ISO 27000. En cualquier caso, hay que tener en cuenta que los controles incluidos en dicha norma no coinciden exactamente con las medidas propuestas por el ENS, aunque existe un alto grado de solapamiento entre ambos. Por tanto, un sistema certificado bajo la ISO 27000 tendría gran parte del camino recorrido, pero no todo.

El ENS también hace referencia a posibles distintivos de cumplimiento, que implican la existencia de auditores externos que los certifiquen. Estos sellos dotarán de un status de excelencia a los organismos que los posean, en relación con su seguridad TIC. Y ello será motivo de confianza en sus servicios electrónicos.

Carlos Belso
Jefe de los Equipos de Acreditación
Centro Criptológico Nacional