Avance del ENS y medidas de seguridad previstas en el Plan de Transformación Digital

Para abordar el tema de la seguridad en la Administración habría que comenzar preguntándose qué tenemos ahora que antes no teníamos y qué sabemos ahora y que antes no sabíamos. En primer lugar, el Esquema Nacional de Seguridad (ENS) nos proporciona un planteamiento común de principios, requisitos y medidas de seguridad para la protección de la información y de los servicios de la Administración, actualizado recientemente a la luz de la experiencia adquirida y del entorno regulatorio comunitario, imprescindible en un escenario de transformación digital, acompañado de la serie 800 de guías CCN-STIC y de la colección de servicios de detección, análisis, auditoría e intercambio que proporciona CCN-CERT. Acompaña la realización de lo previsto por las leyes 39/2015 y 40/2015 en cuanto a la seguridad se refiere.

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

En segundo lugar, el ENS ha permitido implantar una dinámica de captación regular de información, de la que no se disponía en otro tiempo, y que permite conocer dónde estamos, a través del Informe nacional del estado de la seguridad y su herramienta de soporte, conocida como INES. El informe más reciente, que cuenta con una participación exhaustiva de la AGE y de las CC.AA., así como de una muestra significativa de las EE.LL. y universidades invitadas, nos muestra que, en términos de cumplimiento del ENS, nos encontramos a medio camino y que es necesario un renovado esfuerzo para cumplir con los requisitos previstos. Las citadas leyes y el Plan de transformación digital de la AGE y sus OO.PP. han de ayudar en dicho esfuerzo.

Algunos aspectos, a la luz del informe reciente, que requieren especial atención son la gestión de cambios, el mantenimiento, la configuración y su gestión, la monitorización de la actividad del sistema, la gestión de incidentes, la continuidad del servicio, así como la concienciación y la formación. Las principales recomendaciones se refieren a promover la conformidad con el ENS; que los datos aportados a INES se basen en una auditoría o una autoevaluación, según proceda; ampliar el alcance del informe a más entidades, e impulsar medidas de seguridad horizontales disponibles a través de plataformas en la nube.

Responsabilidad de todos

Hay que tener presente que, como ilustra el Informe de ciberamenazas 2015/tendencias 2016 de CCN-CERT, los incidentes se van a

incrementar en número, tipología y gravedad por, entre otras razones, la ubicuidad y omnipresencia de la tecnología. De hecho, el CCN-CERT gestionó durante 2015 un total de 18.232 incidentes detectados en las Administraciones Públicas y en empresas de interés estratégico, cifra que representa un incremento del 41,45% con respecto al año 2014.

Por ello, hemos de trabajar de forma conjunta aplicando el ENS así como los servicios y herramientas de CCN-CERT para afrontar las amenazas, las vulnerabilidades y los ataques y constituir un objetivo resistente con capacidad de prevención, reacción y recuperación.

Todos nos tenemos que aplicar, no solo desde el lado de la prestación de los servicios, sino también como usuarios que adoptan buenos hábitos de seguridad, en el día a día de nuestro trabajo en la Administración y fuera del mismo.

Los ciudadanos también tenemos nuestra parte de responsabilidad en la ciberseguridad y en calidad de tales contamos con los servicios de la Oficina de Seguridad del Internauta (OSI) de INCIBE.

Un CISO en la AGE

Al hablar de asentar en la AGE la responsabilidad de la seguridad de la información y de la posible figura de un CISO (*ChiefInformation Security Officer)*, que genéricamente velaría por la seguridad de la información manejada y de los servicios prestados en sintonía con los objetivos y obligaciones de la organización, hay que tener en cuenta nuestro contexto. Tengamos en cuenta que la AGE es extensa, diversa y compleja y que vienen asentándose la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) y el nuevo modelo de gobernanza, junto con los servicios comunes y compartidos. Cabe pensar, en consecuencia, en una figura cuya atención se centraría en la protección de los servicios comunes y compartidos, en colaboración con una red de responsables de seguridad en los Departamentos ministeriales y ubicado en la DTIC, en la posición óptima que le permita llevar a cabo el desempeño de sus funciones. ✱