EL ESQUEMA NACIONAL DE SEGURIDAD, AL SERVICIO DE LA CIBERSEGURIDAD DEL SECTOR PÚBLICO

MIGUEL A. AMUTIO GÓMEZ

Ministerio de Política Territorial y Función Pública

El Esquema Nacional de Seguridad (ENS), disponible desde enero de 2010, proporciona al Sector Público en España un planteamiento común de seguridad para la protección de la información que maneja y los servicios que presta; impulsa la gestión continuada de la seguridad, imprescindible para la transformación digital en un contexto de ciberamenazas; a la vez que facilita la cooperación y proporciona un conjunto de requisitos uniforme a la Industria, constituyendo también un referente de buenas prácticas.

LA TRANSFORMACIÓN DIGITAL Y LA NECESIDAD DE CIBERSEGURIDAD

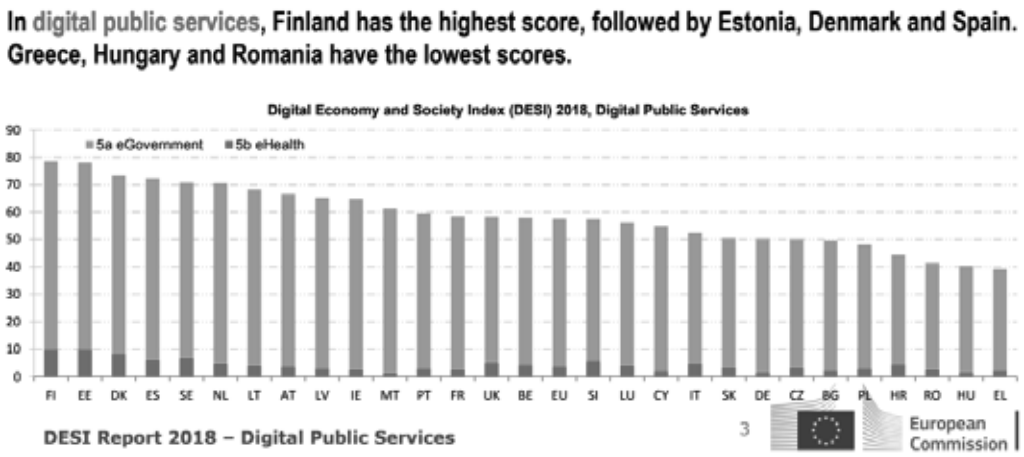
Las organizaciones y operadores económicos del Sector Privado, las empresas, interactúan con las entidades del Sector Público, particularmente con la Administración como sujetos obligados a relacionarse por medios electrónicos, a menudo con un volumen de transacciones considerable, y, por tanto, interesados en que se produzca en condiciones de seguridad; ofrecen servicios y soluciones de seguridad a las entidades del Sector Público; participan de forma creciente en la prestación de servicios de administración digital de diversa índole apoyando a las entidades del Sector Público, por ejemplo, a través de servicios en la nube; sin olvidar que también proporcionan servicios de valor añadido relativos a la conformidad, es decir, servicios de auditoría y certificación.

Como se apunta en la parte expositiva del Real Decreto 3/2010, *actualmente los sistemas de información de las administraciones públicas están fuertemente imbricados entre sí y con sistemas de información del Sector Privado: empresas y administrados. De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema.* Todo ello sin perder de vista la considerable dimensión del Sector Público en España, comentado más adelante.

En consecuencia, en este artículo, en primer lugar, nos ubicaremos en el contexto de la transformación digital y de la necesidad ineludible de ciberseguridad; seguidamente, veremos los aspectos principales del Esquema Nacional de Seguridad para hacernos con una comprensión global del mismo en cuanto a su alcance, potencial, características principales; posteriormente, trataremos de forma más pormenorizada las cuestiones de interés para las organizaciones y operadores económicos del Sector Privado; a continuación, el estado de situación de la implantación del ENS; y, finalmente, apuntaremos unas conclusiones y retos próximos.

Dice la «Estrategia para el Mercado Único Digital de Europa» que *la economía mundial se está convirtiendo*

FIGURA 1
DESI 2018, SERVICIOS PÚBLICOS DIGITALES



Fuente: Comisión Europea

rápidamente en digital. Las tecnologías de la información y la comunicación (TIC) ya no son un sector específico sino el fundamento de todos los sistemas económicos innovadores modernos. Y el Sector Público de España no es ajeno, no desde luego la Administración, a esta transformación digital inevitable e ineludible. En esa tarea nos encontramos, conscientes de que tiene un carácter continuo por la propia dinámica de lo digital y de su evolución permanente.

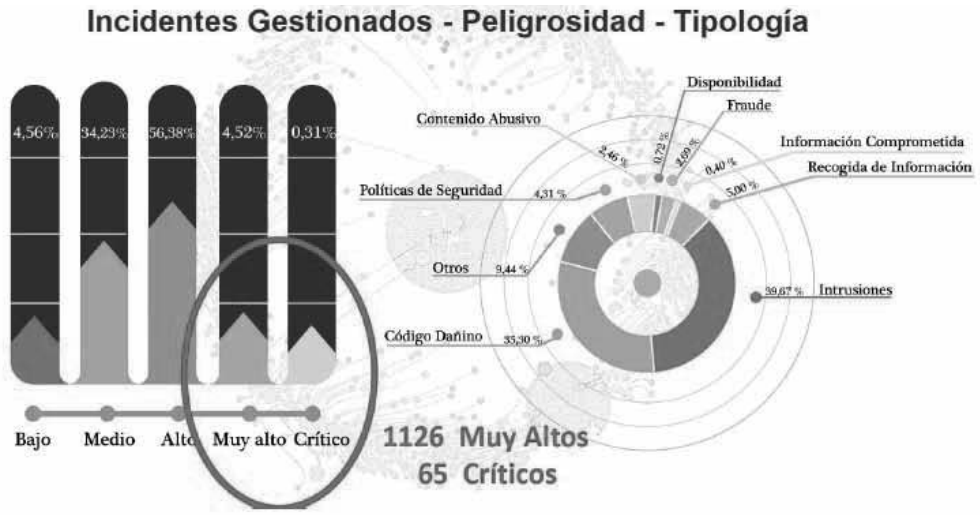
De hecho, según el «Índice de Economía y Sociedad Digital (DESI)» en su edición de 2018, índice compuesto que resume cinco indicadores del rendimiento digital de Europa (conectividad, capital humano, uso de internet, integración de la tecnología digital y servicios públicos digitales), y que permite un seguimiento de la evolución de los Estados miembros de la Unión Europea en la competitividad digital, España ocupa el puesto número 10 de los 28; puntuación que aumentó en 2018 debido a un mejor rendimiento en todas las dimensiones que mide DESI, destacando entre ellas la dimensión de los *Servicios Públicos Digitales* que es aquella en la que España obtiene mejores resultados, y según la cual figura en 4º lugar, tras Finlandia, Estonia y Dinamarca, habiéndose convertido nuestro país en un referente internacional.

En una línea similar, según el informe «UN eGovernment Survey 2018», España figura, como se subraya de forma explícita en el mismo, en la lista de *Top Performers* del índice de desarrollo de la administración electrónica (*E-Government Development Index* (EGDI)), junto con países tales como Dinamarca, Finlandia, República de Corea, Países Bajos, Australia, Japón, Nueva Zelanda, Reino Unido y Estados Unidos, manteniendo el puesto número 17 respecto a la edición de 2016, y el puesto número 10 en el ámbito de los países europeos.

Este posicionamiento de España se debe, en gran medida, a la interacción dinámica y evolución conjunta de tres pilares básicos, fruto de un esfuerzo colectivo, multidisciplinar y continuado a lo largo del tiempo. En primer lugar, un marco legal exhaustivo en las materias relativas a la administración digital, como queda testimoniado en el «Código de Administración Electrónica» publicado por el BOE, junto con el desarrollo normativo y la documentación de soporte que facilita su aplicación; adecuado todo ello a la realidad que impone la transformación digital, que proporciona seguridad jurídica y unas reglas de juego que facilitan la extensión a gran escala de la prestación y uso de los servicios públicos digitales. En segundo lugar, una dinámica de cooperación y gobernanza que contribuye a forjar una visión y una comprensión comunes de los retos a afrontar y de los caminos a emprender, a través de los órganos de gobernanza y cooperación en materia de administración electrónica. Y, en tercer lugar, el desarrollo de los servicios digitales que proporcionan la realidad práctica, particularmente, de aquellos servicios que resuelven necesidades comunes y que facilitan las economías de escala, de los cuales algunos ejemplos ilustrativos serían aquellos servicios relativos a la identidad electrónica (Cl@ve), la firma electrónica (@Firma), la Plataforma de Intermediación de Datos que facilita el derecho de los ciudadanos a no aportar datos que obran en poder de la Administración (véase el artículo 28 de la Ley 39/2015), etc.

Dicho lo anterior, la implantación de la administración digital ha de ir acompañada de medidas organizativas y técnicas de ciberseguridad proporcionadas a los riesgos. Los ciudadanos, incluyendo a las empresas, esperan que los servicios públicos digitales se presten en unas condiciones de confianza y seguridad equivalentes a las encontradas en un escenario de relación presencial. En particular, las empresas están obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo. Además, desde una perspectiva de conjunto, buena parte de la información y los servicios manejados por las administracio-

FIGURA 2
INCIDENTES GESTIONADOS – PELIGROSIDAD – TIPOLOGÍA



Fuente: CCN-CERT

nes constituirían, por acumulación, activos nacionales estratégicos.

En cualquier caso, la información y los servicios están sometidos a los riesgos provenientes de las acciones malintencionadas o ilícitas, los errores o fallos y los accidentes o desastres. En concreto, el Sector Público, por la naturaleza de la información que maneja y de los servicios que presta, está particularmente expuesto a los ciberataques, como de forma elocuente muestran las cifras crecientes de ciberincidentes ofrecidas por los informes anuales del CCN-CERT. Según el informe «CCN-CERT Ciberamenazas y Tendencias edición 2018», *durante el año 2017, el CCN-CERT, gestionó un total de 26.472 incidentes, frente a los 20. 807 del año 2016 (un 27,22% más) en los sistemas del Sector Público español y de empresas de interés estratégico para el país.* También apunta que *entre los principales ataques detectados en número, las intrusiones (ataques dirigidos a explotar vulnerabilidades e introducirse en el sistema) y el código dañino (troyanos, spyware) fueron los principales vectores de ataque.* Y que *también se registró un incremento importante de ataques de Denegación de Servicio.*

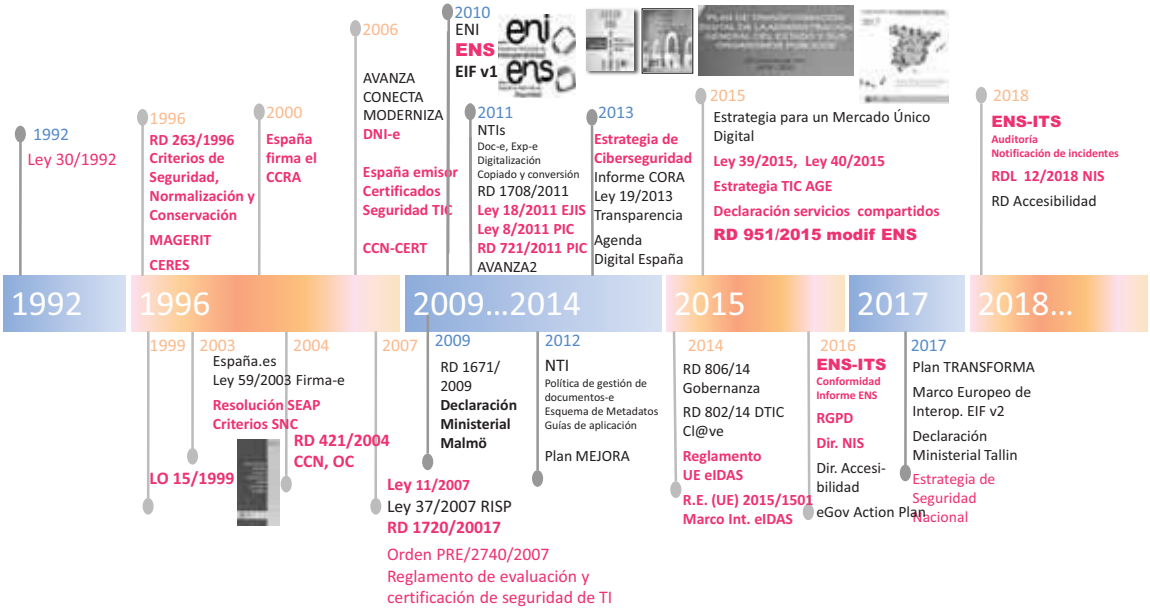
En concreto, las entidades del Sector Público están particularmente expuestas a los ataques orientados a la información, con sustracción bien con o sin revelación de la misma, alteración o destrucción, y a la denegación de servicio que afectaría al acceso a los propios servicios digitales y al derecho de acceso a la información. De hecho, según el citado informe «CCN-CERT Ciberamenazas y Tendencias edición 2018», *el 40% de los ataques web están dirigidos a la obtención de información, siendo las aplicaciones web patrocinadas por el sector público y el financiero las que mayor número de ataques han reportado en 2017*. Así que, al igual que ocurre con la transformación digital, nos encontramos ante un reto, el de la ciberseguridad, que requiere un esfuerzo global, conjunto, estable y continuado.

QUÉ ES EL ESQUEMA NACIONAL DE SEGURIDAD (ENS)

Como no se puede entender la implantación de la administración digital sin el acompañamiento de las adecuadas medidas organizativas y técnicas de seguridad, se ha considerado necesario proporcionar un planteamiento común de principios, requisitos, medidas y mecanismos de conformidad para la seguridad, ceñido a las necesidades y requisitos del Sector Público, según una concepción de que la seguridad no es una cuestión exclusivamente técnica, sino que afecta a todas las personas que utilizan los medios electrónicos que las entidades ponen a su disposición para el desarrollo de su actividad y a sus responsables jerárquicos, responsables a la postre de la información manejada y de los servicios prestados. Resulta ilustrativo de este enfoque el hecho de que el título III de la denominada «E-Government Act» de 2002 del gobierno de los Estados Unidos, incluyera a su vez la «Federal Information Security Management Act», conocida popularmente como «FISMA», referente principal del ENS en el momento de su concepción.

La figura del Esquema Nacional de Seguridad apareció en la Ley 11/2007. El motivo es obvio, en aquél momento pareció ineludible acompañar el impulso de la administración electrónica con las adecuadas medidas que aporten seguridad a la información manejada y los servicios prestados. Se materializó mediante el «Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica», que se ocupa esencialmente de establecer la política de seguridad en la utilización de medios electrónicos a través de los principios básicos y requisitos mínimos que garanticen adecuadamente

FIGURA 3
CONTEXTO DE ACTUACIONES EN MATERIA DE SEGURIDAD A LO LARGO DEL TIEMPO



Fuente: elaboración propia

la seguridad de la información tratada, coletilla que introduce la noción de proporcionalidad. Fue elaborado en su día con la participación de todas las administraciones públicas y con aportaciones del Sector Privado a través de las asociaciones principales de la Industria del Sector TIC que contribuyeron al perfeccionamiento del proyecto y que partían de una valoración muy positiva del mismo al vislumbrar el potencial que ofrecía la armonización de los requisitos de un gran sector y el rigor con el que se afrontaba.

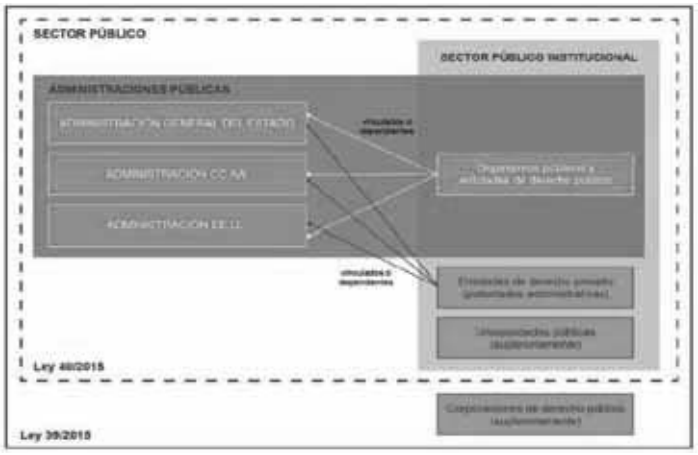
Posteriormente, el ENS fue modificado en 2015 (por el Real Decreto 951/2015) a la luz de la experiencia obtenida de su implantación desde su publicación en enero de 2010, de los resultados del informe del estado de la seguridad previsto en su artículo 35; de la evolución de la tecnología y las ciberamenazas y del contexto regulatorio internacional y europeo, especialmente, por razón del «Reglamento (UE) nº 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…».

Las leyes 39/2015 y 40/2015 han recogido el testigo. La primera, la «Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas», establece entre los derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo «*a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas*»; realiza, además, diversas menciones específicas al cumplimiento de las garantías y medidas de seguridad al referirse a cuestiones tales como registros, archivo de documentos y copias.

Mientras que la segunda, la «Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público», incluye la seguridad entre los principios de actuación de las administraciones públicas, así como la garantía de la protección de los datos personales, al señalar en su artículo 3 los principios generales relativos a las relaciones de las administraciones por medios electrónicos. También realiza diversas menciones concretas a la seguridad en apartados relativos a la sede electrónica, el archivo electrónico de documentos, los intercambios electrónicos en entornos cerrados de comunicaciones y las transmisiones de datos entre Administraciones Públicas. Y, sobre todo, en el artículo 156 se recoge el Esquema Nacional de Seguridad *que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada*.

La figura de *Contexto de actuaciones en materia de seguridad a lo largo del tiempo* facilita la comprensión del ENS dentro de un esfuerzo más global que incluye antecedentes tales como los «Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades», la firma del Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de la Tecnología de la Información, la creación del Centro Criptológico Nacional y del Organismo de Certificación, el lanzamiento del CCN-CERT, entre otros.

FIGURA 4
ÁMBITO DE APLICACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD



Fuente: Guía CCN-STIC 830

¿Cuál es *el* ámbito de aplicación *del ENS?* Pues el Sector Público, según lo establecido en el artículo 2 de las leyes 39/2015 y 40/2015 sobre el ámbito subjetivo y lo indicado sobre el sector público institucional. Es un ámbito no carente de complejidad, como se puede vislumbrar en la visión panorámica que ofrece la figura «Ámbito de aplicación del Esquema Nacional de Seguridad» procedente de la «Guía CCN-STIC 830 Ámbito de aplicación del ENS», guía que desarrolla en detalle los ámbitos subjetivo y objetivo de aplicación del Esquema Nacional de Seguridad.

El Sector Público en España tiene una dimensión considerable que alcanzaría un orden de magnitud de más de 30.000 entidades, contando, por un lado, administraciones públicas con unas 13.000 entidades (incluyendo entidades locales menores) y, por otro lado, el sector público institucional con más de 18.000 entidades, según fuentes tales como el INVENTE gestionado por la IGAE y el Directorio Común de Unidades Orgánicas y Oficinas (DIR3) gestionado por la Secretaría General de Administración Digital.

Por otra parte, cabe precisar que están excluidos del ámbito de aplicación del ENS los sistemas que tratan información clasificada regulada por la Ley 9/1968 de 5 de abril, de Secretos Oficiales y sus normas de desarrollo.

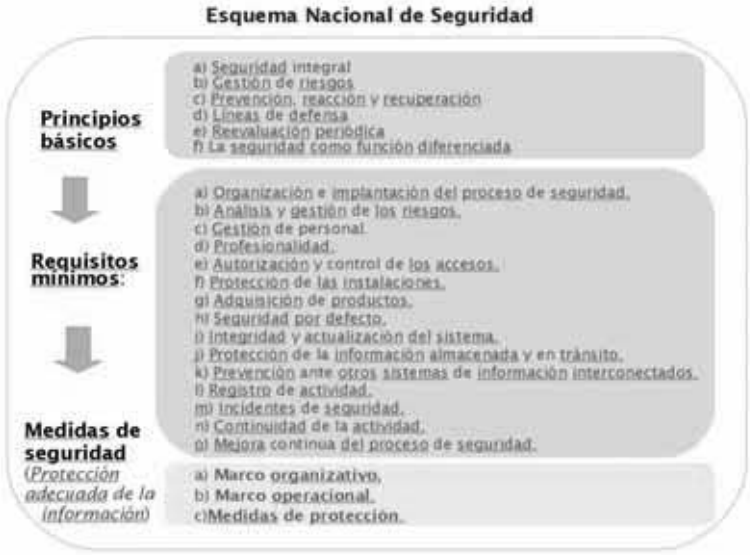
¿Qué objetivos persigue? El principal es crear las condiciones necesarias de seguridad en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permitan el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Otros objetivos, importantes también, aunque pueda tener un carácter más instrumental, son promover la gestión continuada de la seguridad, al margen de impulsos puntuales, o de su ausencia; promover la prevención, detección y corrección para una mejor resiliencia en el escenario de ciberamenazas y ciberataques; promover un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios públicos digitales cuando participan diversas entidades, que se consigue esencialmente gracias a los elementos y el lenguaje comunes que han de guiar la actuación de las entidades del Sector Público, así como facilitar la comunicación de los requisitos de seguridad de la información a la Industria; y, por qué no, servir también de modelo de buenas prácticas, es decir, predicar con el ejemplo, como se apunta en las recomendaciones de la OCDE, «Digital Security Risk Management for Economic and Social Prosperity - OECD Recommendation and Companion Document».

El mandato principal del Esquema Nacional de Seguridad, establecido en su artículo 11 sobre requisitos mínimos de seguridad, es que todos los órganos superiores de las Administraciones públicas, extendido hoy en día a las todas las entidades del Sector Público, *deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente*, que se establecerá en base a los principios básicos y que se desarrollará aplicando los requisitos mínimos.

Los citados principios básicos (6) orientan en las decisiones en materia de seguridad. Mientras que la aplicación de los requisitos mínimos (15) permite una protección adecuada de la información manejada y de los servicios prestados.

Además, el mecanismo de categorización sirve para lograr el cumplimiento de los principios básicos y de los requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información y los servicios a proteger. Esta categorización de los sistemas contempla tres categorías, BÁSICA, MEDIA y ALTA, en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la in-

FIGURA 5
PANORÁMICA DE PRINCIPIOS BÁSICOS, REQUISITOS MÍNIMOS Y MEDIDAS DE SEGURIDAD



Fuente: elaboración propia

FIGURA 6
PANORÁMICA DE LAS MEDIDAS DE SEGURIDAD

Fuente: elaboración propia

formación o de los servicios a proteger con perjuicio para las dimensiones de seguridad (disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad), que a su vez se valoran en tres escalones BAJO, MEDIO y ALTO. En la valoración del impacto sobre estas dimensiones cabe tener en cuenta aspectos como la repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, así como el respeto de la legalidad y de los derechos de los ciudadanos. Se trata de modular el equilibrio entre la importancia de la información que se maneja y de los servicios que se prestan, por un lado, y el esfuerzo de seguridad requerido, en función de los riesgos a los que se está expuesto, bajo el criterio del principio de proporcionalidad, por otro lado.

Las medidas de seguridad (75) se encuentran estructuradas en tres grupos: *marco organizativo*, constituido por medidas relacionadas con la organización global de la seguridad; *marco operacional,* constituido por las medidas para proteger la operación del sistema como conjunto integral de componentes para un fin; y *medidas de protección*, que protegen activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad. La relación de medidas seleccionadas se formaliza en un documento denominado *Declaración de Aplicabilidad;* y las medidas de seguridad referenciadas en el Anexo II del ENS *podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos y los requisitos mínimos*.

La respuesta ante incidentes de seguridad resulta esencial en el escenario de ciberamenazas y ciberataques. Se recoge en los artículos 36 y 37 del ENS como *capacidad de respuesta a los incidentes de seguridad* de los sistemas en las administraciones públicas, la estructura CCN-CERT del Centro Criptológico Nacional (CCN) que ha de actuar sin perjuicio de las capacidades de respuesta que pueda tener cada administración pública, y de su función como coordinador a nivel nacional e internacional. Sus funciones incluyen el soporte y coordinación para el

tratamiento de vulnerabilidades y la resolución de incidentes de seguridad o de agresiones recibidas por las entidades del Sector Público; la investigación y divulgación de las mejores prácticas sobre seguridad de la información; la formación destinada al personal especialista en el campo de la seguridad de las tecnologías de la información; la información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias; el apoyo a las Administraciones públicas para que desarrollen sus propias capacidades de respuesta a incidentes de seguridad. También se contempla en el ENS la notificación al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados y según los detalles que se han concretado en una Instrucción Técnica de Seguridad específica sobre esta cuestión.

El uso de productos certificados contribuye a aportar mayor confianza, especialmente cuando la categorización de los sistemas es ALTA. El ENS también destaca la importancia de la certificación a la hora de adquirir productos de seguridad, particularmente a través de lo establecido en su artículo 18 sobre *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

La auditoría de la seguridad es necesaria para verificar el cumplimiento del Esquema Nacional de Seguridad; es así mismo relevante para la aportación de información al informe anual del estado de la seguridad y esencial para la certificación de la conformidad de sistemas que caigan en las categorías MEDIA y ALTA. Se reconoce que son de aplicación los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicable a la misma.

En relación con la conformidad, se contempla la publicación en las sedes electrónicas de la conformidad con el ENS y de otros distintivos de los que se pueda ser acreedor según lo establecido en la correspondiente Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, cuestión desarrollada más adelante.

La formación y la concienciación son necesarias para garantizar el conocimiento del ENS por parte del personal del Sector Público; y hay que añadir que así también como por parte del personal de las organizaciones y operadores económicos del Sector Privado que prestan servicios y soluciones de diversa naturaleza a las entidades del Sector Público.

Finalmente, las instrucciones técnicas de seguridad facilitan una implantación adecuada y homogénea de los requisitos y medidas recogidos en el ENS; particularmente, para indicar el modo común de actuar en aspectos concretos tales como el informe del Estado de la Seguridad; la notificación de incidentes de Seguridad; la auditoría de la Seguridad; la conformidad con el ENS; la adquisición de Productos de Seguridad; la criptología de empleo en el ENS; la interconexión en el ENS; y los requisitos de seguridad en entornos externalizados. Todo lo anterior sin perjuicio de nuevas instrucciones que pudieran adoptarse. Las cuatro primeras ya están publicadas en el BOE y continúan los trabajos preparatorios de las demás.

El ENS va acompañado, además, de una exhaustiva colección de guías, la serie CCN-STIC 800, así como de una serie de herramientas y servicios disponibles en el Portal CCN-CERT.

LA CONFORMIDAD CON EL ENS Y LAS EMPRESAS PROVEEDORAS DE SERVICIOS Y SOLUCIONES TECNOLÓGICAS

La publicación de la conformidad con el ENS es el cierre del círculo; constituye la manifestación expresa de que se cumple con lo establecido en el mismo. En efecto, el artículo 41 del ENS sobre 'Publicación de conformidad' señala que los órganos y Entidades de Derecho Público *darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del ENS*. Formulación escueta, pero de gran calado y potencial, que afecta a todas las entidades del Sector Público en España tras la entrada en vigor de las leyes 39/2015 y 40/2015, así como a los operadores del Sector Privado que les prestan soluciones y servicios, no solo de seguridad, o que estén interesadas en la certificación de la conformidad con el ENS.

La «Instrucción Técnica de Seguridad de Conformidad con el ENS» establece los criterios y procedimientos para la determinación de la conformidad, así como para la publicidad de dicha conformidad. Precisa los mecanismos de obtención y publicidad de las declaraciones de conformidad y de los distintivos de seguridad obtenidos respecto al cumplimiento del ENS. Según la categoría del sistema, se distingue entre la *Declaración de Conformidad*, de aplicación a sistemas de información de categoría BÁSICA, para la que bastaría con una autoevaluación; y la *Certificación de Conformidad*, de aplicación obligatoria a sistemas de información de categoría MEDIA o ALTA y voluntaria en el caso de sistemas de información de categoría BÁSICA, para la que se requiere una auditoría independiente.

Además, dicha Instrucción precisa los requisitos de las entidades certificadoras, que quieran certificar el cumplimiento con el ENS, siendo ENAC la encargada de acreditar a las entidades de certificación que realizan las preceptivas auditorías de conformidad con el ENS, acreditación que se realiza conforme a la norma «UNE-EN ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios».

FIGURA 7
DECLARACIÓN DE CONFORMIDAD, CERTIFICACIÓN DE CONFORMIDAD Y DISTINTIVOS ASOCIADOS

Fuente: ITS de Conformidad con el ENS

Sobre esta base, las entidades co-responsables del ENS, la Secretaría General de Administración Digital (Ministerio de Política Territorial y Función Pública) y el Centro Criptológico Nacional, han colaborado con la Entidad Nacional de Acreditación (ENAC), para desplegar el esquema de certificación de la conformidad con el ENS, hoy ya una realidad práctica que cuenta, por un lado, con una colección de entidades de certificación ya acreditadas o en proceso, y, por otro lado, con una colección creciente de entidades certificadas frente al ENS tanto del Sector Público como del Sector Privado. ENAC ha ayudado a precisar aquellos aspectos que han permitido la puesta en práctica de la certificación de la conformidad con el ENS, particularmente, los requisitos de las entidades certificadoras, así como a desplegar el esquema de acreditación de estas entidades.

La creación de distintivos relativos a la conformidad con el ENS ha perseguido dar respuesta tanto a la exigencia de publicidad recogida en el Real Decreto 3/2010, como incentivar a las entidades, públicas o privadas, que hubiesen alcanzado la conformidad con la implantación del ENS en alguno de sus sistemas de información. La certificación del cumplimiento con el ENS mediante entidades de certificación acreditadas aporta confianza a las entidades del Sector Público, así como a las del Sector Privado afectadas o interesadas, en cuanto a determinar la conformidad con los principios y requisitos del ENS y a que se cuenta con un servicio competente para la protección adecuada de la información manejada y los servicios prestados.

Se ha perseguido, en consecuencia, establecer unas reglas de juego que ofrezcan la adecuada independencia y confianza esperada y demandada por los actores interesados, públicos y privados; escenario que solo puede pasar por la certificación acreditada, máxime en España, donde hay una larga trayectoria en estos servicios de valor añadido, y, por tanto, hay quien sabe certificar y hay quien sabe acreditar la competencia de quien desea certificar.

¿Por qué interesa la certificación de la conformidad con el ENS a los operadores del *Sector Privado?* Más allá de la prestación específica de servicios o soluciones de seguridad es creciente la participación de operadores del Sector Privado en la provisión de servicios de administración digital, por ejemplo, basados en servicios 'en nube' (*cloud computing*). Estos servicios deben cumplir el ENS según la categoría que tengan los sistemas de las entidades a las que dan servicio. La citada Instrucción Técnica de Seguridad de Conformidad con el ENS así lo indica en su apartado VII sobre soluciones y servicios prestados por el Sector Privado al establecer en su párrafo 1 que *Cuando los operadores del Sector Privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas.*

En consecuencia, cualquier entidad privada puede certificar la conformidad con el ENS de sus servicios o soluciones; certificación que, además de representar un valor añadido, le otorga una ventaja competitiva para ofrecerlos a las entidades del Sector Público, especialmente, en concursos públicos, pues según el párrafo VII.2 de la instrucción en cuestión *Es responsabilidad de las entidades públicas contratantes notificar a los operadores del Sector Privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad...*

Certificaciones para las que les son de aplicación los mismos procedimientos y documentos relativos a la conformidad con el ENS que para las entidades del

Sector Público según lo indicado en el párrafo *VII.3* en cuanto a que *Cuando la provisión de las soluciones o la prestación de los servicios sujetos al cumplimiento del Esquema Nacional de Seguridad sean realizados por operadores del Sector Privado, estos utilizarán los mismos modelos documentales utilizados para las Declaraciones, las Certificaciones o los Distintivos de Conformidad ...*

Cabe añadir aquí que el ENS responde de una forma más amplia, exhaustiva y precisa a los requisitos de seguridad de las entidades del Sector Público que la que pueda aportar la conformidad con la norma ISO 27001. No obstante, la guía «CCN-STIC-825 Esquema Nacional de Seguridad. Certificaciones 27001» explica la aplicación y en su caso certificación 27001 como soporte de cumplimiento del ENS, a la vez que ayuda a determinar qué controles del Anexo A de la norma ISO 27001, desarrollados en la norma ISO 27002, son necesarios para cumplimiento de cada medida del Anexo II del ENS y, en su caso, qué elementos adicionales son requeridos.

La Comisión Europea acepta la legislación nacional como una alternativa a la certificación en ISO 27001, tal como queda reflejado en el artículo 10 del «Reglamento de Ejecución (UE) 2015/1501 de 8 de septiembre de 2015 sobre el marco de interoperabilidad relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior», según el cual *Los operadores de nodos que proporcionen autenticación demostrarán que, con respecto a los nodos participantes en el marco de interoperabilidad, el nodo cumple los requisitos de la norma ISO/CEI 27001 por medio de certificación, o por métodos de evaluación equivalentes, o mediante el cumplimiento de la legislación nacional*. Este enfoque habrá de propagarse y extenderse a otras disposiciones y dominios del ámbito comunitario, como enfoque natural. Por lo demás, el estudio de la entidad European Cybersecurity Organisation (ECS) titulado «Overview of existing Cybersecurity standards and certification schemes» incluye al ENS en el apartado 5.6 *Standards and schemes for public services / eGovernment / digital citizenship.*

LA ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y LA CONTRATACIÓN DE SERVICIOS DE SEGURIDAD

En relación con los productos de seguridad de las tecnologías de la información y comunicaciones, es de interés lo indicado en el artículo 18 del ENS en términos de que *se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.*

El ENS cita al Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC (el Centro Criptológico Nacional) como aquel encargado de determinar el criterio a cumplir en función del uso previsto del producto, en relación con el nivel de evaluación, otras certificaciones de seguridad que se requieran adicionales, así como en aquellos casos en los que no existan productos certificados. Asimismo, en diversas ocasiones, el ENS señala la recomendación y, o bien, obligación de utilizar algoritmos certificados por el Centro Criptológico Nacional a la hora de utilizar diferentes productos o características de los sistemas, como en el caso de la utilización de dispositivos físicos (*tokens*), la protección de claves criptográficas, la protección de la confidencialidad, la autenticidad e integridad o los medios utilizados en la firma electrónica.

En particular, según la medida *Componentes certificados [op.pl.5]*, aplicable a la categoría ALTA, *se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas*. Diversas otras medidas se refieren a esta cuestión del uso de componentes certificados, tales como *protección de claves criptográficas, protección de la confidencialidad, protección de la autenticidad e integridad, criptografía, borrado y destrucción, firma electrónica, sellos de tiempo*; y el Anexo V del ENS incluye un modelo de cláusula administrativa particular para la adquisición de este tipo de productos. Para desarrollar esta cuestión en detalle, se ha previsto una Instrucción Técnica de Seguridad de Adquisición de Productos de Seguridad, que se encuentra en preparación a la fecha de redacción de este artículo.

Mientras tanto, se avanza mediante fórmulas como, por ejemplo, la que se incluye en el «Pliego de prescripciones técnicas que rige la celebración del acuerdo marco a través del procedimiento especial de adopción de tipo para el suministro de sistemas, equipos y software de comunicaciones (AM 10/2018)», que se remite al citado artículo 18 del ENS. En dicho acuerdo marco se dice que *Para cada producto, el cumplimiento de los requisitos funcionales de seguridad exigidos por el ENS podrá ser acreditado por su inclusión en el «Catálogo de productos STIC (Seguridad de las Tecnologías de la Información y la Comunicación)» del CCN (Centro Criptológico Nacional). Dicho Catálogo recogido en la Guía CCN-STIC 105 ofrece un listado de productos supervisados por el CCN que incluye los Productos Aprobados para el manejo de información clasificada y los Productos Cualificados para el manejo de información sensible, para que sirvan de referencia a la Administración Pública*.

Efectivamente, la «Guía CCN-STIC-105 Catálogo de productos STIC» recoge en su versión más reciente seis categorías de productos (Control de Acceso, Seguridad en la Explotación, Monitorización de la Seguridad, Protección de las Comunicaciones, Protección de las Información y Soportes de Información, Protección de equipos y servicios) y 33 familias, como sistemas operativos, herramientas *anti-spam*, tarjetas inteligentes, dispositivos

FIGURA 8
EVOLUCIÓN DE LA PARTICIPACIÓN EN EL INFORME NACIONAL DEL ESTADO DE LA SEGURIDAD

Fuente: CCN-CERT

biométricos o sistemas *Honeypot*. Para cada producto incluido en la guía se indican cuestiones tales como la clasificación de la información que puede manejar (Difusión Limitada, Confidencial, Reservado, Secreto), sus características de seguridad, la categoría del sistema de información en la que puede emplearse según lo definido en el ENS (ALTA, MEDIA, BÁSICA), las certificaciones aportadas o el entorno donde se vaya a emplear. Esta guía evolucionará en su estructura de contenidos y en la colección de productos recogidos.

Finalmente, también interesa que para la contratación de servicios de seguridad, los operadores del Sector Privado han de tener en cuenta lo previsto en el artículo 15 'Profesionalidad' del ENS en cuanto a que *las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados*.

ESTADO DE SITUACIÓN DE LA IMPLANTACIÓN DEL ENS

El ENS contempla, en su artículo 35 'Informe del estado de la seguridad', la recogida de información que permita conocer regularmente el estado general de la seguridad en el Sector Público y su plasmación, con periodicidad anual, en el Informe del estado de la seguridad. La información recogida en este informe es de interés para el conjunto, pues viene proporcionando datos, ya tras cuatro ediciones, y de los que antes se carecía, que permiten elaborar un perfil general del estado de la seguridad. También es de interés para cada actor en particular, en la medida en la que permite contrastar cada situación individual frente a la general de los demás.

La herramienta INÉS, desplegada en 2014, facilita la recogida y consolidación de información para la elaboración de este Informe del Estado de la Seguridad, según las condiciones indicadas en la Instrucción Técnica de Seguridad correspondiente. Permite la recopilación de la información de seguridad de las entidades del Sector Público para poder elaborar el informe, y evaluar regularmente el estado de la seguridad y su adecuación al ENS. Sobre la base de toda la información recogida se produce un informe general y cuatro informes específicos, para la Administración General del Estado, las Comunidades Autónomas, las Entidades Locales y las Universidades Públicas (CRUE). Hasta la fecha se han realizado cuatro ediciones del informe, desde 2014 a 2017, y como se puede ver en la figura *Evolución de la participación en el Informe Nacional del Estado de la Seguridad,* la participación presenta una tendencia de crecimiento notable.

Atendiendo a los resultados generales, a la luz de los datos recogidos en la edición más reciente del «Informe Nacional del Estado de la Seguridad», el publicado en 2018 sobre la base de la campaña de 2017, la conclusión es que, en general, el nivel de adecuación al ENS en las entidades públicas, es mejorable, encontrándose a medio camino, por lo que es necesario continuar con un esfuerzo importante en los próximos años para alcanzar los requisitos mínimos exigidos.

RETOS Y CONCLUSIONES

Como hemos visto, el Esquema Nacional de Seguridad proporciona al Sector Público en España un planteamiento común de seguridad para la protección de la información que maneja y los servicios que presta, imprescindible para la transformación digital en un contexto de ciberamenazas, a la vez que facilita la cooperación y proporciona un conjunto de requisitos uniforme a la Industria.

La Industria no solo ofrece servicios y soluciones de seguridad a las entidades del Sector Público, sino que también participa, de forma creciente, en la prestación de servicios de administración digital de diversa índole; más los servicios de valor añadido que ofrece relativos a la conformidad, es decir, auditoría y certificación. En consecuencia, los proveedores de soluciones o servicios deben estar en condiciones de exhibir la correspondiente *Declaración de Conformidad* con el ENS, en el caso de sistemas de categoría BÁSICA, o la *Certificación de*

FIGURA 9
RESULTADOS GENERALES INES 2017

	Índice de Madurez	Índice de Cumplimiento
AGE	60,7	72,2
CC.AA.	59,2	69,3
EE.LL.	46,6	57,1
UNIV.	51,2	61,8
GLOBAL	52,2	63,8

Figura 57.- Resultados de los índices de madurez y cumplimiento por ámbito

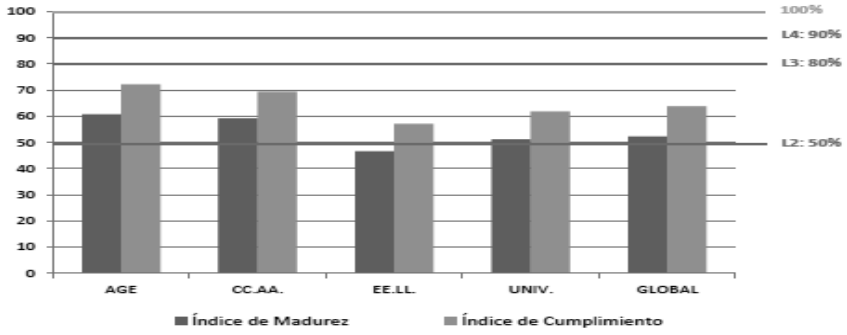


Figura 58.- Resultados de los índices de madurez y cumplimiento por ámbito

Fuente: CCN-CERT

Conformidad, en el caso de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos para las entidades del Sector Público. Por tanto, cualquier entidad privada puede certificar la conformidad con el ENS de sus servicios o soluciones, certificación que le otorga una ventaja competitiva para ofrecerlos a las entidades del Sector Público.

En el caso específico de los productos, el cumplimiento de los requisitos funcionales de seguridad exigidos por el ENS podrá ser acreditado por su inclusión en el «Catálogo de productos STIC » del CCN, recogido en la Guía CCN-STIC 105 que ofrece un listado de productos supervisados por el CCN. Más el hecho de que las entidades del Sector Público pueden exigir que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

En relación con la evolución y desarrollo del propio Esquema Nacional de Seguridad, el reto principal procede de su aplicación en un entorno cambiante por la rápida evolución de las tecnologías, la experiencia adquirida en la implementación del ENS, y la evolución del contexto regulatorio europeo y nacional recientemente reforzado en materias de protección de datos de carácter personal y de seguridad de la información y las redes.

En relación con esta última cuestión un emergente de calado es el «Reglamento General de Protección de Datos». En su documento «El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Publicas» la Agencia Española de Protección de Datos se refiere en el punto 11 a la necesidad de revisar las medidas de seguridad que se aplican a los tratamientos a la luz de los resultados del análisis de riesgo de los mismos; y, en ese mismo punto, señala que *la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad*. De esta forma se aprovecha el esfuerzo general de protección de la información y los servicios para la protección específica de los datos de carácter personal.

Además, la «Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales», en su Disposición adicional primera sobre *Medidas de seguridad en el ámbito del sector público* indica que *El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos de carácter personal, para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679*. Se trataría de incorporar al ENS aquellos aspectos específicos de la protección de datos de carácter personal previstos en el Reglamento y en la Ley Orgánica para completar el Esquema. El siguiente paso, aprovechando la experiencia relativa a la conformidad con el ENS, sería una evolución para que con un solo esfuerzo las entidades pudieran obtener y demostrar la conformidad con ambos, con el ENS y con el Reglamento, lo cual daría lugar a sinergias y economías de escala de alto impacto. El hecho de que el Reglamento se refiera en relación con la conformidad a la norma ISO 17065 habría de facilitar este planteamiento.

Por otra parte, en el «Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información» se recoge el papel del ENS en el ámbito sectorial que le corresponde, en cuestiones tales como las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales y en la obligación de notificar.

El desarrollo de las Instrucciones Técnicas de Seguridad ha de continuar con aquellas pendientes de publicación en el BOE que son a la fecha las relativas a la *criptología de empleo en el ENS*, la *interconexión en el ENS*, la *adquisición de Productos de Seguridad* y los *requisitos de seguridad en entornos externalizados*; siendo de especial interés estas dos últimas para los proveedores de soluciones y servicios.

Para las entidades afectadas por el ENS, el reto principal es el de la plena implantación, cuestión sobre la que las ediciones del Informe nacional del estado de la seguridad van mostrando la evolución y los aspectos que requieren especial atención, como el refuerzo de la capacidad de prevención, monitorización, vigilancia y respuesta a ciberataques y ciberamenazas. Para las empresas que prestan soluciones y servicios a las entidades del Sector Público, no solo de seguridad, la certificación de la conformidad con el ENS es un valor añadido que otorga una ventaja competitiva para ofrecerlos a las entidades del Sector Público.

BIBLIOGRAFÍA

COMISIÓN EUROPEA. *Estrategia para el Mercado Único Digital de Europa*. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52015DC0192

COMISIÓN EUROPEA. Índice de Economía y Sociedad Digital (DESI). Disponible en: https://ec.europa.eu/digital-single-market/en/desi

NACIONES UNIDAS. *UN eGovernment Survey 2018*. Disponible en: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018

CENTRO CRIPTOLÓGICO NACIONAL. *Informe CCN-CERT Ciberamenazas y Tendencias edición 2018.* Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html

US GOVERNMENT.*E-Government Act*. Disponible en:https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html

US GOVERNMENT. *Federal Information Security Management Act*. Disponible en: https://www.dhs.gov/fisma

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330

Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2015-11881

BOLETÍN OFICIAL DEL ESTADO. *Código de Administración Electrónica*. 7 de febrero de 2018. Disponible en:https://www.boe.es/legislacion/codigos/codigo.php?id=029_Codigo_de_Administracion_Electronica

CENTRO CRIPTOLÓGICO NACIONAL. *Guía CCN-STIC-830* Ámbito de aplicación del Esquema Nacional de Seguridad. 2016. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1674-ccn-stic-830-ambito-aplicacion-ens/file.html

IGAE. INVENTE. Disponible en: http://www.pap.hacienda.gob.es/Invente/pagBuscadorEntes.aspx?V8dle/a+VI7G69aCoVquzG3r4TQDypP8EAj5+3DsFF1YHgCpRnTPIKlbdQ0AaUVZu0LD8Q3KCjKcKlse04ipnw==#tab-1

Directorio Común de Unidades Orgánicas y Oficinas (DIR3). Disponle en: https://administracionelectronica.gob.es/ctt/dir3

OECD. Digital Security Risk Management for Economic and Social Prosperity - OECD Recommendation and Companion Document.2015. Disponible en: http://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm

MINISTERIO DE ADMINISTRACIONES PÚBLICAS. *Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades*. 2004. 212 páginas. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:56967857-2b54-40a5-8c67-99104dfd9e23/2004-Criterios-de-seguridad-normalizacion-NIPO-326-04-044-9.pdf

REGLAMENTO (UE) nº 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 la que se deroga la Directiva 1999/93/CE. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32014R0910

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *El impacto del Reglamento general de protección de datos sobre la actividad de las administraciones públicas*. Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf

Portal CCN-CERT. *Empresas certificadas en el ENS*. Disponible en: https://www.ccn-cert.cni.es/ens/empresas-certificadas.html

CENTRO CRIPTOLÓGICO NACIONAL. *Guía CCN-STIC-809 Declaración de conformidad con el ENS*. 2018. Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/1279-ccn-stic-809-declaracion-de-conformidad-con-el-ens/file.html

ECS. *Overview of existing Cybersecurity standards and certification schemes*. Disponible en: http://www.ecs-org.eu

CENTRO CRIPTOLÓGICO NACIONAL. *Guía CCN-STIC-825 Esquema Nacional de Seguridad. Certificaciones 27001.* 2013. Disponible en:https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.html

Reglamento de Ejecución (UE) 2015/1501 de 8 de septiembre de 2015 sobre el marco de interoperabilidad relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2015-81816

CENTRO CRIPTOLÓGICO NACIONAL. *Guía CCN-STIC-105*Catálogo de productos STIC (Seguridad de las Tecnologías de la Información y la Comunicación). Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de

estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en https://www.boe.es/diario_boe/txt.php?id=-BOE-A-2018-16673

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Disponible en: https://www.boe.es/boe/dias/2018/09/08/pdfs/BOE-A-2018-12257.pdf

Portal CCN-CERT. Disponible en: https://www.ccn-cert.cni.es/