ACADEMIA DE LAS CIENCIAS
Y LAS ARTES MILITARES

Comunicaciones académicas

Tratamiento integral de la Ciberseguridad y de la Protección de Datos de Carácter Personal en España

José Luis Goberna Caride
Academia de las Ciencias y Artes Militares
Sección de Futuro de las Operaciones Militares

21 de septiembre de 2022

El escenario global de la Transformación Digital

El Ciberespacio posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas. Es un nuevo ámbito que estimula el emprendimiento, potencia el progreso socioeconómico y ofrece cada día nuevas posibilidades en todos los sectores de actividad

El cambio que la actual transformación digital está provocando en los procesos productivos en todos los países, ya inmersos en la tercera década del siglo XXI, se manifiesta a escala global y a un ritmo vertiginoso y sin precedentes si la comparamos con la secuencia de las tres anteriores revoluciones industriales.

La Inteligencia Artificial, la Robótica, el Big Data, el Blockchain y el Internet de las Cosas son ya una realidad, si bien su verdadero potencial transformador está aún por descubrir. Las consecuencias de estas innovaciones van más allá de la dimensión tecnológica, pues se extienden hacia una profunda revisión de los actuales modelos sociales, de los usos y costumbres, de las relaciones personales, de la ética y de los propios derechos fundamentales de las personas.

La transformación digital de esta cuarta revolución industrial está remodelando también la seguridad a nivel planetario y presenta serios desafíos, dado que el ciberespacio se configura como un «campo de batalla» donde la información y la privacidad de los datos personales son activos de alto valor en un entorno de creciente competición geopolítica, reordenación del poder y también de un progresivo empoderamiento del individuo.

La creciente conectividad a través de variadas y complejas infraestructuras de alta capacidad (Fibras terrestres y submarinas, Satélites, Redes Móviles, etc.), y la mayor dependencia de las sociedades y del ser humano respecto a redes y sistemas, así como de sus componentes, objetos y dispositivos digitales, generan cada vez más no pocas vulnerabilidades y dificultan la adecuada protección de la información. De este modo, surgen múltiples riesgos para los Estados, para sus instituciones y organismos, para la sociedad civil de cada uno de ellos, y también para el propio individuo, al poder atentar contra su intimidad y privacidad.

Evolución del marco legal en España

Desde el Real Decreto 3/2010, de 8 de enero, a través del cual fue aprobada la primera versión del Esquema Nacional de Seguridad (ENS), con vocación de asegurar la información en el ámbito de la Administración Electrónica, se produjo su primera actualización con el Real Decreto 951/2015, de 23 de octubre, sobre la base de la experiencia adquirida, la situación de la Ciberseguridad en ese momento y los trascendentales cambios legales operados en la Administración, entre otros, con las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, del Régimen Jurídico del Sector Público; y con la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que considera a la Ciberseguridad como un ámbito de especial interés para la Seguridad Nacional.

En la misma línea de rápida evolución, las Estrategias de Seguridad Nacional de 2017 y 2021 han ido identificando el Ciberespacio como una nueva dimensión de conexión común de carácter global que supera los límites físicos de las fronteras físicas o políticas entre países y continentes, con apertura funcional y fácil accesibilidad. Al compás de las anteriores, la primera Estrategia de Ciberseguridad de 2013, y posteriormente la Estrategia Nacional de Ciberseguridad 2019 han ido incardinando una nueva concepción de la Ciberseguridad en el marco de la Política de Seguridad Nacional, donde el ENS está llamado a ser identificado como la herramienta fundamental a la hora de implantar las necesarias medidas de seguridad en redes y sistemas.

Por otro lado, la evolución de las amenazas y de las tecnologías en los últimos años también ha venido acompañada por las necesarias adaptaciones del marco jurídico a la normativa de la Unión Europea. En este sentido, la entrada en vigor del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 (conocida como Directiva NIS), ha supuesto un paso importante en la mejora de la Ciberseguridad en España, extendiendo el alcance de esta Directiva con el objetivo de mejorar la Ciberseguridad de todos los sectores estratégicos (infraestructuras críticas). En esta dirección, el reciente Real Decreto 43/2021, de 26 de enero, que lo desarrolla, ha fijado con un alcance estratégico e institucional las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, ligándolas al ENS.

También desde el mismo marco legal europeo, la adopción del 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 sus datos personales y a la libre circulación de estos datos, a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), está generando un serio impacto en la sociedad, al reforzar la salvaguarda de los derechos fundamentales y libertades de las personas en el contexto de la referida transformación digital. La solución inmediata pasa por la implantación de las medidas previstas en el ENS (Disposición Adicional Primera).

De igual forma, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ha reiterado como solución la obligación de aplicar las medidas del ENS a los tratamientos de datos personales.

Con estos antecedentes, todo este diverso y multidisciplinar desarrollo legal ha venido a converger en la reciente versión del ENS del Real Decreto 311/2022, de 3 de mayo, respondiendo a una triple necesidad:

- Alinear el Esquema al marco normativo de la seguridad y de la protección de datos personales.
- Introducir la capacidad de ajustar el Esquema a la realidad de ciertos colectivos, racionalizando recursos bajo el concepto de «perfil de cumplimiento específico» del CCN del CNI.
- Facilitar una mejor respuesta a las tendencias de ciberseguridad, reduciendo vulnerabilidades y promoviendo la vigilancia continua con la revisión de los

principios básicos, los requisitos mínimos y las medidas de seguridad que constituyen el esqueleto del ENS.

Finalmente, la actualización del ENS se ha visto también ligada al Plan de Digitalización de las Administraciones Públicas 2021-2025 -como instrumento para el Plan de Recuperación, Transformación y Resiliencia (PRTR)-, al cumplimiento de la agenda España Digital 2025, y a la creación del Centro de Operaciones de Seguridad (COS/SOC) de la Administración General del Estado (AGE). Este deberá servir de referente para la más eficaz evolución de la seguridad en el sector público español y para el mejor cumplimiento del actualizado ENS.

Amenazas crecientes en constante ebullición

En este escenario de rápida evolución y consiguiente adaptación del marco legal, las ciberamenazas se definen como todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos y abarcan un amplio abanico de acciones caracterizado por su diversidad, tanto en lo que concierne a capacidades como a motivaciones del atacante.

Estas amenazas afectan a la práctica totalidad de los ámbitos de la Seguridad Nacional, como son la Defensa Nacional, la Seguridad Económica o la Protección de las infraestructuras críticas, entre otros, y como ya se ha mencionado no distinguen fronteras ni plazos temporales.

Entre las ciberamenazas podemos citar las enmarcadas en el ciberespionaje (amenazas persistentes avanzadas), el cibercrimen (ciberterrorismo, ciberdelito), el hacktivismo (ciberataques) o las amenazas híbridas (acciones militares, ciberataques y manipulación de la información / fake news) a partir de injerencias extranjeras de marcado signo político.

Por otra parte, las amenazas e infracciones al régimen de Protección de Datos no tienen por qué estar originadas solamente en escenarios tan beligerantes, pues ya forman parte de la vida social ordinaria, aunque difícilmente se producirán al margen de aquellas amenazas y de su impacto sobre redes y sistemas con altas vulnerabilidades.

En este sentido, resulta muy significativo mencionar que tanto en las tensiones originadas por crisis políticas y sociales, en la emergencia sanitaria del COVID-19 que padece el mundo, o en la actual guerra en Ucrania, la ciberseguridad y la protección de datos han sido y son actores de primera fila e incluso «armas de uso efectivo» en este último escenario, en un ambiente dominado por las redes sociales, las páginas web y apps en dispositivos móviles, datos en la nube, la geolocalización de usuarios y la gran actividad de los medios de comunicación asentados en múltiples soportes de telecomunicaciones.

Es evidente que la ciberseguridad posee un carácter transversal que exige que sea afrontada con una perspectiva integral que comprenda a las Administraciones Públicas, a las Fuerzas Armadas, a los Cuerpos y Fuerzas de Seguridad del Estado, a los sectores público y privado y a la sociedad en su conjunto, en tanto puede tener implicaciones simultáneas en aspectos tan diversos como la soberanía, la seguridad y defensa nacional, el orden público, los derechos fundamentales, la vida privada, la economía y el desarrollo tecnológico de la sociedad.

Con estos referentes, y sobre la base de cuatro principios, la Estrategia Nacional de Ciberseguridad de 2019 plantea como objetivo general, en línea con la anterior Estrategia de Seguridad Nacional de 2017 y ampliando el objetivo para la Ciberseguridad previsto en la misma, que España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico. Ello se completa a través de cinco objetivos específicos, siete líneas de acción y sesenta y cinco medidas. Entre los objetivos, destaca la consolidación de un marco nacional coherente e integrado que garantice la protección de la información y de los datos personales tratados por los sistemas y redes. De nuevo, se reclama un ENS integral, conciliando seguridad y respeto a los derechos fundamentales.

Integración de la Ciberseguridad y la Protección de Datos Personales en un marco legal actualizado

Reconocido el desarrollo legal efectuado durante más de una década y el auge de las ciberamenzas en una sociedad inmersa en plena transformación digital, llegó el momento de revisar el ENS, dotándolo de pragmatismo y flexibilidad y, a la vez, de un articulado que garantice derechos fundamentales como la protección de datos personales o el secreto de las telecomunicaciones, constitucionalmente reconocidos.

En este proceso integrador, ha jugado un papel fundamental la Agencia Española de Protección de Datos (AEPD), a la hora de diferenciar los ámbitos de la seguridad de la información y el propio de la protección de datos de carácter personal. Respecto a este último, resulta significativo el cambio de un modelo pasivo de «lista de cumplimiento» a otro de «responsabilidad activa», basado en un análisis de riesgos e impacto propio para los datos personales, donde el Delegado de Protección de Datos (DPD) adquiere un papel protagonista.

Asumiendo esta singularidad, el nuevo ENS 2022 ha recogido en sus artículos 3 y 12.1.f), y en el apartado 5.7.1 del Anexo II todas las novedades legales mencionadas en relación a la protección de datos personales, y el reconocimiento de los criterios que puedan establecer la AEPD o las Agencias Autonómicas de Protección de Datos, todo ello sin perjuicio de los requisitos del propio ENS, pero dando prevalencia a las medidas a implantar como consecuencia de los análisis de riesgos y evaluaciones de impacto específicos para los datos personales.

En la misma línea integradora, a través del artículo 24 del ENS en su tercera versión, dedicado a Registro de Actividad y detección de Código dañino, la AEPD ha introducido referencias explícitas a las garantías de derechos al honor, intimidad personal y familiar, y a la propia imagen de los afectados, junto al registro de las actividades de los usuarios autorizados, que deben respetar los principios de necesidad y proporcionalidad, limitación de la finalidad, minimización de datos o la limitación del plazo de conservación. Un mandato explícito para el equilibrio entre la seguridad de la información y el respeto a los derechos fundamentales, que ahora afecta también a la información clasificada, a la que el nuevo ENS amplía su ámbito de actuación respecto a las dos versiones anteriores.

Desarrollo y limitaciones de competencias a nivel nacional

Frente a este nuevo escenario, el mínimo nivel de Ciberseguridad en España marcado por el ENS 2022, con toda la flexibilidad que aporta y siempre supervisado por el Centro Criptológico Nacional (CCN) del CNI, debe contar también en lo

relativo a la Protección de Datos de carácter personal con los órganos de control como la Agencia Española de Protección de Datos (AEPD) y sus homólogas vasca y catalana, especialmente para la certificación y acreditación del cumplimiento del ENS y de la LOPDGDD a nivel nacional en todo el conjunto del territorio nacional.

En todo caso, no se debe perder de vista lo establecido en la sentencia del Tribunal Constitucional 142/2018, que analizó la distribución de competencias entre el Estado y las Comunidades Autónomas en materia de Ciberseguridad, en la que establece que *La Ciberseguridad como sinónimo de la seguridad en la red, es una actividad que se integra en la seguridad pública, así como en las telecomunicaciones*, como competencias exclusivas del Estado, de acuerdo con lo previsto en los artículos 149.1.21ª y 149.1.29ª de la Constitución. Este criterio ha sido ratificado por el preceptivo informe del Consejo de Estado en el proceso normativo del nuevo ENS, frenando cualquier interpretación de competencias compartidas o transferidas desde el nivel estatal.

Retos inmediatos de carácter tecnológico e industrial

Hasta ahora, la falta de implantación de infraestructuras de seguridad y protección de datos, tanto en el sector público como en el privado, ha venido motivado por tres factores:

- Falta de planeamiento integral y recursos económicos muy limitados.
- Escasez de personal tecnológicamente capacitado.
- Carencia de experiencia en un deseable marco normalizado.

Para resolver estas carencias y lograr una mayor implantación del nuevo ENS y de la normativa LOPDGDD, resultaría más práctico y eficiente plantear una nueva Estrategia Conjunta (ESN & LOPDGDD).

Esta Estrategia, respetando los contextos jurídico y organizativo de cada norma, compartiría las mismas medidas de seguridad mínimas (de carácter tecnológico) para neutralizar los riesgos que padezcan las redes y sistemas, y los que resulten cuando se vean comprometidos los datos de carácter personal.

Ya que con un nuevo marco jurídico integrado y contando con la necesaria financiación, habrá que tener en cuenta que la seguridad de las redes y sistemas de información requiere potenciar medidas concretas de prevención, detección y respuesta, fomentando la "seguridad por diseño y por defecto", que debe estar incorporada tanto en el desarrollo de productos y servicios tecnológicos como en su normal funcionamiento o en su actualización.

Desde un punto de vista tecnológico y en el ámbito de la Protección de Datos, permitiría implantar de forma racional a nivel nacional las denominadas Privacy Enhancing Technologies (PETs), conjunto organizado y coherente de soluciones TIC que reducen los riesgos que afectan a la privacidad, implementando las estrategias y patrones definidos anteriormente. Estas aparecen en la red IPEN, Red de Ingeniería de Privacidad en Internet (Internet Privacy Engineering Network) del Supervisor Europeo de Protección de Datos (EDPS), para dar soporte a los desarrolladores en el empleo de patrones de diseño y otros bloques reutilizables orientados a proteger y mejorar la privacidad de manera eficiente y efectiva.

La ENISA (European Union Agency for Cybersecurity) ha publicado informes sobre la evolución de las tecnologías de privacidad mejorada para comparar los niveles de madurez. La Agencia trabaja también en el establecimiento de una plataforma como repositorio centralizado de consulta pública donde obtener información sobre soluciones para que los desarrolladores las ajusten como mejor se adapten a los objetivos de privacidad que persiguen en cada caso.

Combinar las herramientas y productos de Ciberseguridad homologados por el CCN del CNI con las PET fomentadas por la AEPD abre un panorama de innovación al que no se le ha prestado la debida atención hasta la fecha. Ello permitiría elevar a medio plazo el nivel de Ciberseguridad y Protección de Datos a escala nacional, encarando ambos retos a la vez de forma coordinada e integral desde la perspectiva tecnológica.

Tomar la iniciativa en la implantación de medidas, productos y lograr la certificación de los niveles de Ciberseguridad y Protección de Datos en el sector público e incluso privado de las Pequeñas y Medianas Empresas (PyMEs) es un campo

innovador que hasta la fecha ha progresado de manera muy limitada. Ello abre amplias posibilidades si se lleva a cabo de forma planificada y gradual con el concurso de la industria nacional. En esta línea, las Compras Públicas Innovadoras o los Acuerdos de Colaboración Público-Privados surgen como instrumentos que pueden favorecer una más rápida implantación de las medidas de seguridad mínimas previstas en el ENS 2022.

Establecer acuerdos previos desde ciertas empresas españolas especializadas en el sector de las Tecnologías de la Información y las Telecomunicaciones con el CCN y con la AEPD en este nuevo escenario, parece también lo más recomendable ante este desafío de carácter estratégico para nuestra Ciberseguridad, a escala nacional e internacional.

Con estas oportunidades, la reciente publicación del renovado Esquema Nacional, con un enfoque más pragmático y adaptado a las necesidades de las redes y sistemas de los diversos organismos; y, sobre todo, su efectiva y rápida implantación supone un paso necesario e ineludible, que ya no permite mayores retrasos en la Ciberseguridad que demanda la transformación digital de la sociedad española.

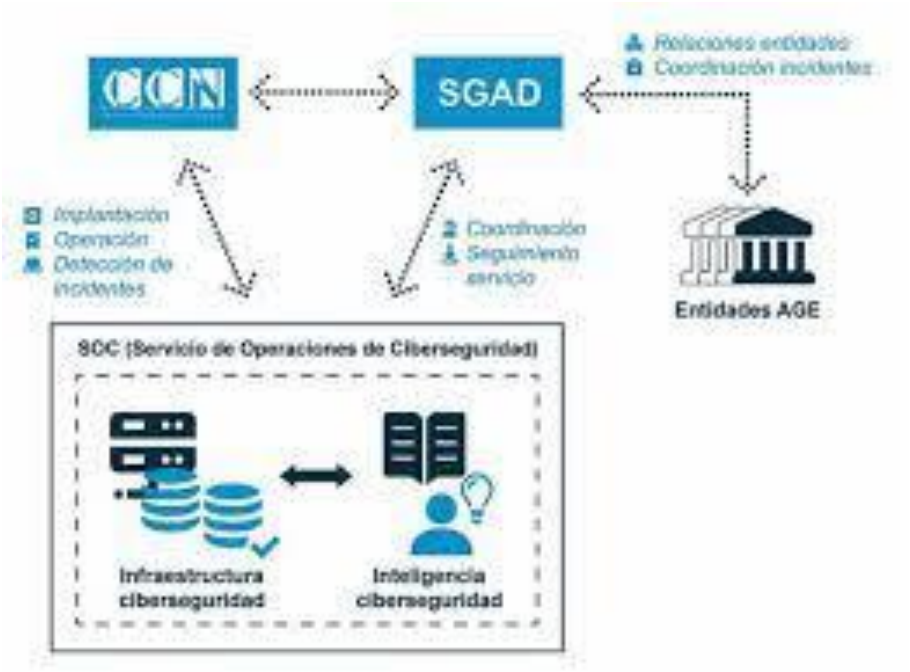
Aportación del Centro de Operaciones de Ciberseguridad (COS/SOC) de la AGE.

Después de tres años tras el anuncio de su creación, en febrero de 2019, el Gobierno aprobó el 29 de marzo de 2022 el Plan Nacional de Ciberseguridad en el que se prevé la puesta en marcha del Centro de Operaciones de Ciberseguridad (COS/SOC) de la AGE y sus Organismos Públicos.

El COS/SOC de la AGE operará de manera centralizada sobre el Servicio Unificado de Comunicaciones de la Administración General, y sobre aquellas entidades con conexión a la Red de Sistemas de Aplicaciones y Redes para las Administraciones (Red SARA). Su finalidad es la prestación de servicios horizontales de ciberseguridad que aumenten la capacidad de vigilancia y detección de amenazas en las operaciones diarias de los sistemas de información y telecomunicaciones de la Administración, así como la mejora de su capacidad de respuesta ante cualquier ciberataque.

Precisamente, por su carácter centralizado, la creación del COS/SOC de la AGE facilitará la implantación de las herramientas y tecnologías más adecuadas en cada momento, así como las medidas de seguridad previstas en el ENS, eliminando duplicidades y facilitando la especialización. El hecho de que sea el CCN-CERT (Computer Emergency Response Team) del CNI, en su calidad de CERT

Gubernamental Nacional, quien implante y opere el nuevo COS/SOC, bajo la dirección técnica y estratégica de la División de Planificación y Coordinación de Ciberseguridad de la Secretaria General de Administración Digital (SGAD) del Ministerio de Asuntos Económicos y Transformación Digital, ofrece una gran oportunidad para la efectiva implantación del nuevo Esquema Nacional de una manera planificada, ordenada, directa y expedita.



Nuevo escenario con la implantación del ENS 2022 y la creación del COS/SOC de la AGE.

La reciente publicación y entrada en vigor de la tercera versión del ENS ha supuesto la culminación de un largo esfuerzo de actualización de la norma más relevante para la Ciberseguridad en España, aprovechando la experiencia adquirida durante más de una década en la lucha contra los crecientes ciberamenazas, la necesidad de adaptarse a la normativa de la Unión Europea en lo relativo a la seguridad de redes y sistemas y a la protección de datos personales, y el aprovechamiento de los avances tecnológicos que caracterizan a la transformación de la era digital.

En este trabajo conjunto se debe destacar el protagonismo del Centro Criptológico Nacional (CCN) del CNI y de la Agencia Española de Protección de Datos (AEPD), con sus expertos y acreditados colaboradores en el ámbito académico de nuestra nación, al haber logrado conciliar la seguridad de redes y sistemas con el respeto al derecho fundamental de la protección de datos personales. El papel del CCN cobra una doble relevancia, pues al compás de la puesta en marcha del nuevo ENS hay que añadir la creación del COS/SOC de la AGE, que servirá para implantar la

nueva normativa, con un enfoque realista y práctico, y para crear un modelo que sirva de referencia efectiva para la Ciberseguridad en España desde la propia Administración estatal.

Pero estas dos iniciativas no hay que entenderlas solamente como las respuestas a unas necesidades inexcusables en el orden técnico o jurídico, sino también como una oportunidad para la integración de tecnologías, para la innovación en el marco de la transformación digital que vive la sociedad española, incrementando la confianza en unos sistemas y servicios, que ya forman parte del día a día del ciudadano, y que, por tanto, también afectan a su seguridad, a su bienestar, y por ende a la Defensa Nacional.