LA CIBERSEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN EN EL ÁMBITO DE LA ASISTENCIA SANITARIA

Carlos
Galán Cordero

Profesor de la Universidad Carlos III de Madrid
Departamento de Derecho Público del Estado. Área de Derecho Administrativo
Agencia de Tecnología Legal

SUMARIO

RESUMEN

En la era digital, donde la interconexión y la inmediatez en la gestión de la información prevalecen, los sistemas de información se han convertido en activos esenciales para diversas instituciones, y entre ellas, destaca el sistema sanitario. En España, este sistema almacena una ingente cantidad de datos sensibles que van desde historiales clínicos hasta investigaciones biomédicas, y que resultan ser de interés no solo para profesionales de la salud, sino también para actores malintencionados. Por ello, garantizar la ciberseguridad de estos sistemas no es una opción, sino una imperiosa necesidad. Para enfrentar estos desafíos, el Esquema Nacional de Seguridad (ENS) en España establece una serie de medidas, protocolos y buenas prácticas destinadas a proteger la información y las infraestructuras críticas, incluyendo las sanitarias. Este artículo tiene por objetivo analizar la importancia de la ciberseguridad en el sistema sanitario español, destacando la relevancia y aplicabilidad del ENS en este contexto. Abordaremos las principales amenazas, los desafíos actuales y cómo las directrices del ENS ofrecen un marco robusto para una defensa eficaz.

PALABRAS CLAVE

Ciberseguridad, ciberseguridad en el sistema sanitario, seguridad de la información, dimensiones de la ciberseguridad, Esquema Nacional de Seguridad, ENS, ciberataques.

ABSTRACT

In the digital era, where interconnection and immediacy in information management prevail, information systems have become essential assets for various institutions, and among them, the healthcare system stands out. In Spain, this system stores an enormous amount of sensitive data, ranging from clinical records to biomedical research, which are of interest not only to health professionals, but also to malicious actors. Ensuring the cybersecurity of these systems is therefore not an option, but an absolute necessity. To face these challenges, the National Security Scheme (ENS) in Spain establishes a series of measures, protocols and good practices aimed at protecting information and critical infrastructures, including healthcare infrastructures. This article aims to analyse the importance of cybersecurity in the Spanish healthcare system, highlighting the relevance and applicability of the ENS in this context. We will address the main threats, the current challenges and how the ENS guidelines provide a robust framework for effective defence.

KEYWORDS

Cybersecurity, cybersecurity in the healthcare system, information security, cybersecurity dimensions, National Security Framework, ENS, cyberattacks

I. LOS SISTEMAS DE INFORMACIÓN Y LA CIBERSEGURIDAD

1. Los conceptos de sistemas de información y ciberseguridad

Antes de introducirnos de lleno en la materia, y con el propósito de favorecer su comprensión, conviene comenzar recordando algunos conceptos esenciales antes de sumergirnos en unos contenidos tan poliédricos como los que presenta la ciberseguridad.

Como toda aproximación científica, lo primero que hemos de hacer es definir el campo de nuestro estudio: los *sistemas de información* y su *ciberseguridad*.

Apoyándonos en la regulación vigente, podemos definir sistema de información como[1]:

> *Cualquiera de los elementos siguientes:*
>
> *1º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.*
>
> *2º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.*
>
> *3º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1º y 2º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.*

Por su parte, podemos definir ciberseguridad (o seguridad de los sistemas de información) como:

> *La capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos*[2].

Obsérvese que, de estas definiciones, podemos extraer ya algunas conclusiones:

1) El concepto sistema de información comprende cualquier elemento físico (*hardware*) o lógico (*software*) que se vea involucrado en el tratamiento de datos, cualesquiera que sean estos.

2) La ciberseguridad no persigue garantizar siempre y en cualquier situación la absoluta inmunidad de los sistemas de información concernidos frente a las amenazas -cuestión esta imposible de alcanzar, por otro lado-, sino más bien construir un modelo de seguridad sustentado en medidas de *resistencia* -aquellas que razonable y ponderadamente impiden la penetración del ataque y, en general, el progreso del ciberincidente-, y en medidas de *resiliencia* -aquellas dirigidas a recuperar la plena funcionalidad de un sistema de información, una vez concluido el ciberincidente.

2. La ciberseguridad como manifestación de la seguridad

Definidos los conceptos esenciales del trabajo, debemos proseguir analizando hasta qué punto *seguridad* y *ciberseguridad* son conceptos jurídicamente diferenciados; análisis que no resulta baladí, pues, de estar ubicados dentro de un bien jurídico protegido común, cabría deducir que podrían ser igualmente aplicables las precisiones que en torno a cualquiera de ellos pudieran realizarse.

Debemos mencionar, en primer lugar, lo señalado por la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que identifica en su artículo 10 la ciberseguridad como uno de los "*ámbitos de especial interés de la seguridad nacional... que requieren una atención específica, por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales*".

Asimismo, la Ley 8/2011, de 28 abril, de medidas para la Protección de las Infraestructuras Críticas -a las que define como aquellas infraestructuras estratégicas "*cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales*", dictada al amparo

1 Según aparece en el Anexo IV-Glosario del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)

2 Idem. Definición asimismo coincidente con la recogida en el artículo 3 b) del Real Decreto-ley 12/2018, dictado al amparo de las competencias exclusivas del Estado en materia de telecomunicaciones y régimen general de comunicaciones (art. 149.1.21 CE) y seguridad pública (art. 149.1.29 CE), que define la *seguridad de las redes y sistemas de información* del mismo modo.

de la competencia atribuida al Estado en virtud del artículo 149.1.29 de la Constitución Española (CE), hace referencia a la ciberseguridad. El artículo 2 de esta Ley define las infraestructuras estratégicas como "*las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales*", entendiendo que tales servicios son los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las Administraciones públicas.

Además, el mantenimiento de la ciberseguridad es una de las funciones propias del Centro Nacional de Inteligencia (CNI), según establece el artículo 4 b) de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

Finalmente, debemos mencionar el 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 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Esta norma tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales y establecer un sistema de notificación de incidentes, además de un marco institucional para su aplicación y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario. Como es sabido, este Real Decreto-ley se aplica a los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, así como a los servicios de la sociedad de la información en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Sobre estas cuestiones ha venido a pronunciarse el Tribunal Constitucional en su sentencia 142/2018, de 20 de diciembre de 2018, en relación con el recurso de inconstitucionalidad 5284-2017 interpuesto por el Presidente del Gobierno respecto de la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña, sobre las competencias en materia de telecomunicaciones, defensa y seguridad pública[3].

3 BOE, núm 22, viernes 25 de enero de 2019.

De la citada sentencia y de la normativa que invoca, a modo de resumen, extraemos las consecuencias más significativas:

- 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. A partir de su conceptuación como conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan, fácilmente se infiere que, en tanto que dedicada a la seguridad de las tecnologías de la información, presenta un componente tuitivo que se proyecta específicamente sobre el concreto ámbito de la protección de las redes y sistemas de información que utilizan los ciudadanos, empresas y administraciones públicas, (FJ 1).

- La ciberseguridad se incluye en materias de competencia estatal en cuanto, al referirse a las necesarias acciones de prevención, detección y respuesta frente a las ciberamenazas, afecta a cuestiones relacionadas con la seguridad pública y la defensa, las infraestructuras, redes y sistemas y el régimen general de telecomunicaciones, (FJ 1)[4].

Todas estas cuestiones han encontrado definitiva consolidación en el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, en el que la ciberseguridad pública se configura como parte integrante de la Seguridad Nacional, al encuadrar el ciberespacio dentro de los objetos materiales de la seguridad exigible a los espacios comunes globales e integrando el modelo de gobernanza de la ciberseguridad en el marco del Sistema de Seguridad Nacional.

3. Las dimensiones de la ciberseguridad

Como hemos señalado en otros trabajos[5], la ciberseguridad es un concepto poliédrico que puede estudiarse desde diferentes puntos de vista, atendiendo precisamente a las garantías exigibles a la información tratada o los servicios que deben ser preservados.

4 Efectivamente, la citada sentencia TC 142/2018, señala que "*la seguridad pública es, en principio, competencia exclusiva del Estado ex artículo 149.1.29 CE, precepto constitucional que pone de manifiesto que ya en él se establecen salvedades («sin perjuicio de») que, en cierto sentido, vienen a modular la exclusividad de la competencia estatal, proclamada en el párrafo inicial del artículo 149 CE*", añadiendo que "*la competencia exclusiva del Estado en materia de seguridad pública no admite más excepción que la que derive de la creación de las policías autónomas*" (STC 104/1989, de 8 de junio, FJ 3).

5 Galán Pascual, Carlos Manuel. *El Derecho a la Ciberseguridad*, en *Sociedad Digital y Derecho*. Varios autores. BOE, 2018.

El Esquema Nacional de Seguridad (ENS), siguiendo la metodología MAGERIT de análisis y gestión de riesgos[6]- establece cinco dimensiones de seguridad: *Confidencialidad*, *Integridad*, *Autenticidad*, *Trazabilidad* y *Disponibilidad*, a las que nosotros hemos añadido una más, de carácter genérico: *Conformidad Legal.*

El cuadro siguiente muestra las definiciones de estas dimensiones, así como su aplicabilidad a la información tratada o los servicios prestados por los sistemas de información de que se trate.

DIMENSIÓN DE LA CIBER-SEGURIDAD	DEFINICIÓN	APLICA-BILIDAD
Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.	Información
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.	Información
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.	Información y Servicios
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.	Información y Servicios
Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.	Información y Servicios
Conformidad legal	Propiedad o característica de las tecnologías, productos, soluciones o servicios que sustentan las operaciones, para mantenerse permanentemente alineados con lo dispuesto en la legislación nacional, europea o internacional que resulte de aplicación.	Sistemas de Información, en su conjunto.

Naturalmente, dependiendo de la aplicación o del servicio concreto de que se trate, ciertas dimensiones de seguridad cobrarán más importancia que las restantes. En el caso de las telecomunicaciones, todas ellas, en mayor o menor medida, constituyen los elementos esenciales de la ciberseguridad en el ámbito de los servicios de telecomunicaciones, como se verá a lo largo de este capítulo.

II. EL ESQUEMA NACIONAL DE SEGURIDAD

Tratándose de sistemas de información destinados a prestar servicios públicos, prescindiendo por tanto en este momento del análisis de otras regulaciones, centraremos nuestra reflexión en el examen del Esquema Nacional de Seguridad, operado por Real decreto 311/2022, de 3 de mayo, que, entre otros ámbitos de aplicación que también comentaremos, regula la (ciber)seguridad de los sistemas de información públicos.

La Constitución española de 1978, en su artículo 103.1, proclama: "*La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Ley y al Derecho*."

6 MAGERIT versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Así pues, y amparado genéricamente en el principio irrenunciable de la eficacia, el despliegue de los servicios que el Sector Público (Administraciones Públicas y Sector Público Institucional) debe prestar a los ciudadanos, especialmente cuando se usan las Tecnologías de la Información y la Comunicación (TIC), exige contar –para dar cumplida respuesta a aquella exigencia constitucional- con los procedimientos administrativos, métodos y herramientas más adecuados que vengan a garantizar a todos sus destinatarios: ciudadanos y empresas, pero también el resto del Sector Público, la seguridad y confiabilidad de sus actos.

Efectivamente, de poco serviría poseer unas magníficas tecnologías que posibilitaran el tratamiento y la comunicación de millones de datos si los actores implicados en la vida de los procedimientos administrativos no percibieran los sistemas de información en los que se sustenta su relación como infraestructuras seguras y tan confiables como la misma esencia que sus actividades requiere.

No cabe duda –como así se ha afirmado-, que el mejor servicio al ciudadano constituye la razón de las reformas que, tras la aprobación de la Constitución, se han ido acometiendo en España para configurar una Administración moderna que haga de los principios de eficacia y eficiencia su razón última, y siempre con la mirada puesta en los ciudadanos y en los intereses generales.

Tal interés constituyó la principal razón de ser de la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP, en adelante), eje vertebrador originario de la que se ha dado en llamar *Administración electrónica*, persiguiendo estar a la altura de nuestra época y del adecuado posicionamiento de nuestras Administraciones Públicas en el marco europeo e internacional. La publicación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP, en adelante) y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP, en adelante), que derogan la anterior, consolidan la primacía del uso de los medios electrónicos en el desenvolvimiento de las entidades públicas.

El reconocimiento general de la relación electrónica en y con el Sector Público plantea varias cuestiones que es necesario contemplar:

- La progresiva utilización de medios electrónicos suscita la cuestión de la privacidad de los datos que se facilitan electrónicamente en relación con un expediente.

- Los legitimados tienen derecho de acceso al estado de tramitación del procedimiento administrativo, así como examinar los documentos de los que se compone. Lo mismo debe suceder, como mínimo, en un expediente iniciado electrónicamente o tramitado de esta forma. Dicho expediente debe permitir el acceso en línea a los interesados para verificar su situación, sin mengua de las garantías de privacidad.

- En todo caso, la progresiva utilización de comunicaciones electrónicas, derivada del reconocimiento del derecho a comunicarse electrónicamente con la Administración, suscita la cuestión no ya de la adaptación de ésta -recursos humanos y materiales a una nueva forma de relacionarse con los ciudadanos-, sino también la cuestión de la manera de adaptar sus formas de actuación y tramitación de los expedientes y, en general, racionalizar, simplificar y adaptar los procedimientos, aprovechando la nueva realidad que imponen las TIC.

- El hecho de reconocer el derecho (obligación, en algunos casos) de los ciudadanos a comunicarse electrónicamente con la Administración, plantea, en primer lugar, la necesidad de definir claramente la sede administrativa electrónica con la que se establecen las relaciones, promoviendo un régimen de identificación, autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad.

Son muchos los preceptos contenidos en nuestras leyes administrativas de referencia (Ley 39/2015 y Ley 40/2015, ambas de 1 de octubre) que insisten en la necesidad de que el desenvolvimiento de las entidades del Sector Público, tanto si obedece al desarrollo del procedimiento como si responde al ejercicio general de sus competencias, debe tener lugar en el marco de un entorno que contemple todas las medidas de seguridad que sean precisas para garantizar a los administrados y a las propias entidades públicas, la integridad, confidencialidad, autenticidad y trazabilidad de la información tratada y la disponibilidad de los servicios prestados, en el marco del respeto a la legislación vigente.

La Ley 39/2015, de 1 de octubre, recoge, 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 al cumplimiento de las garantías y medidas de seguridad, cuando se refiere a los registros, archivo de documentos y copias.

Por su parte, la Ley 40/2015, de 1 de octubre, que recoge en su artículo 156 el Esquema Nacional de Seguridad, así mismo menciona la seguridad al referirse a las relaciones de las administraciones por medios electrónicos, la sede electrónica, el archivo electrónico de documentos, los intercambios electrónicos en entornos cerrados de comunicaciones y las transmisiones de datos entre Administraciones Públicas.

El Esquema Nacional de Seguridad (ENS), operado en la actualidad por Real Decreto 311/2022, de 3 de mayo, constituye uno de los mejores ejemplos europeos de tratamiento de la ciberseguridad.

El vigente ENS, actualizado y heredero del originariamente regulado en el Real Decreto 3/2010, de 8 de enero, ha tenido los siguientes objetivos:

- Alinear el ENS al marco normativo y al contexto estratégico existente para garantizar la seguridad en la administración digital, tratando de reflejar con claridad su ámbito de aplicación en beneficio de la ciberseguridad y de los derechos de los ciudadanos, así como actualizar las referencias al marco legal vigente y revisar la formulación de ciertas cuestiones a la luz de éste, conforme a la Estrategia Nacional de Ciberseguridad 2019, de forma que se logre simplificar, precisar o armonizar los mandatos del ENS, eliminar aspectos que hayan podido considerarse excesivos, o añadir aquellos otros que se identifican como necesarios.

- Introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de "Perfil de Cumplimiento Específico" que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

- Facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, los requisitos mínimos y las medidas de seguridad.

Como señala el Centro Criptológico Nacional en su documentación de referencia, el ENS ha sufrido un proceso permanente de evolución desde su publicación inicial en 2010, con actualizaciones en 2015 y en 2022.

La experiencia acumulada a lo largo de estos años en la implantación del ENS, la evolución y especialización de los agentes afectados directa o indirectamente, la implantación de la certificación de la conformidad con el ENS en 2016 (lo que ha venido proporcionando un amplio conocimiento de centenares de sistemas de información a partir de las evaluaciones y certificaciones), junto con la constitución del Consejo de Certificación del ENS (CoCENS, en 2018) han sentado las bases para que el Esquema Nacional de Seguridad sea una realidad plenamente adaptada a las necesidades actuales y a la regulación europea y nacional de aplicación, como es el caso de la normativa de transposición de la Directiva NIS o la vigente legislación nacional sobre protección de datos, que viene a desarrollar y complementar al RGPD.

De hecho, la actualización del ENS publicada en 2022 ha perseguido en primer lugar, alinear el instrumento con el marco normativo de referencia, nacional y europeo, para facilitar la seguridad en la administración digital. En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS a necesidades específicas de determinados colectivos de entidades, o de determinados ámbitos tecnológicos, dando respuesta a las nuevas demandas. Y, en tercer lugar, actualizar los principios básicos, los requisitos mínimos y las medidas de seguridad para facilitar la respuesta a las nuevas tendencias y necesidades de ciberseguridad.

Como resultado de este esfuerzo, el nuevo Esquema Nacional de Seguridad publicado en 2022 constituye la plataforma más significativa para afrontar, a través de un nuevo marco regulatorio firme y consolidado, la ciberseguridad indisoluble de la transformación digital del sector público y sus proveedores del sector privado, mediante un Framework de Seguridad que contempla todos los elementos necesarios: medidas de gobernanza, organizativas, operativas y tecnológicas, esquemas

de certificación de la conformidad, mecanismos de adaptación al medio o modelos de monitorización y vigilancia continua, todo ello, como decimos, incardinado en nuestro ordenamiento jurídico.

Conviene recordar que el ámbito subjetivo de aplicación de esta norma es la totalidad de las entidades comprendidas en el denominado Sector Público, en los términos en que se define en el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma, siendo también exigible a los sistemas de información de las entidades del sector privado, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas, lo que alcanza también, aunque de una forma instrumental, a los operadores de telecomunicaciones, extendiéndose también a la cadena de suministro de los antedichos contratistas o proveedores, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

En resumen, el ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

PRINCIPIOS BÁSICOS	REQUISITOS MÍNIMOS
• Seguridad como proceso integral. • Gestión de la seguridad basada en los riesgos. • Prevención, detección, respuesta y conservación. • Existencia de líneas de defensa. • Vigilancia continua. • Reevaluación periódica. • Diferenciación de responsabilidades.	• Organización e implantación del proceso de seguridad. • Análisis y gestión de los riesgos. • Gestión de personal. • Profesionalidad. • Autorización y control de los accesos. • Protección de las instalaciones. • Adquisición de productos de seguridad y contratación de servicios de seguridad. • Mínimo privilegio. • Integridad y actualización del sistema. • Protección de la información almacenada y en tránsito. • Prevención ante otros sistemas de información interconectados. • Registro de la actividad y detección de código dañino. • Incidentes de seguridad. • Continuidad de la actividad. • Mejora continua del proceso de seguridad.

El ENS contempla la adopción por parte de las entidades de su ámbito de aplicación de medidas de seguridad concretas, de naturaleza organizativa y técnica, según la siguiente distribución:

• Marco organizativo: medidas relacionadas con la organización global de la seguridad.

• Marco operacional: medidas para proteger la operación del sistema como conjunto integral de componentes para un fin.

- Medidas de protección: para proteger activos concretos, según su naturaleza, con el nivel requerido, en cada dimensión de seguridad.

Como señala el propio Real Decreto, lo dispuesto en él, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

El ámbito de aplicación del ENS es amplio y lógico, y se extiende a los sistemas de información:

- De las entidades de todo el sector público, según se encuentra definido este término en el artículo 2 de la Ley 40/2015.

- Que tratan información clasificada.

- De las entidades del sector privado cuando, presten servicios o provean soluciones a los anteriores, incluyendo los elementos de la cadena de suministro hasta donde un análisis de riesgo así lo determine.

Para garantizar tal cumplimiento, los pliegos de prescripciones de los concursos públicos contemplarán los requisitos de conformidad con el ENS.

Constituyendo las telecomunicaciones un riesgo significativo adicional para garantizar la conformidad de las dimensiones de seguridad antes citadas, especialmente las de última generación, no podía quedar al margen de este nuevo ENS la referencia a la instalación, despliegue, explotación de redes 5G o prestación de servicios 5G por entidades del sector público.

Finalmente, la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, confiere al ENS la inclusión de las medidas que deban implantarse en caso de tratamiento de datos personales 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, obligando a los responsables enumerados en el artículo 77.1 de esta ley orgánica la aplicación a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado, obligación que se extiende a los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Un aspecto interesante de este nuevo ENS son los llamados Perfiles de Cumplimiento Específicos, y que comprenden aquel conjunto de medidas de seguridad que resultando del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad; haciendo posible la capacidad de ajustar los requisitos del ENS a necesidades específicas de determinados colectivos tales como Entidades Locales, Universidades, Organismos Pagadores, etc., u ámbitos tecnológicos concretos, tales como los servicios en la nube, por ejemplo.

Nada obsta para que, llegado el caso y planteada la necesidad, pudiera desarrollarse un Perfil de Cumplimiento específico para los sistemas de información que presten servicios públicos sanitarios.

Respecto de la respuesta a los ciberincidentes, el ENS señala la obligatoriedad de las entidades públicas en la notificación al CCN-CERT de los incidentes de seguridad de que sean víctimas, mientras que las organizaciones del sector privado que presten servicios a las entidades públicas desarrollarán tal notificación al INCIBE-CERT quien lo pondrá inmediatamente en conocimiento del CCN-CERT.

El CCN-CERT determinará técnicamente el riesgo de reconexión de sistemas afectados, indicando procedimientos a seguir y salvaguardas a implementar y la Secretaría General de Administración Digital, de la Secretaría de Estado para la Digitalización y la Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, autorizará la reconexión a medios y servicios comunes en su ámbito de responsabilidad, si un informe de superficie de exposición del CCN-CERT determina que el riesgo es asumible.

Por último, señalar que la conformidad con el ENS (y su exhibición pública) se alcanza a través de dos caminos: una Autoevaluación, solo aplicable a sistemas de información de categoría de seguridad Básica; o una Auditoría Formal, aplicable a sistemas de información de cualquier categoría (Básica, Media o Alta), desarrollada por una Entidad de Certificación del ENS previamente acreditada por la Entidad Nacional de Acreditación (ENAC), según dispone la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información y la Resolución de 13 de octubre de 2016,

de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

En este sentido, hay que señalar que el objeto de la Auditoría de Seguridad del ENS debe determinar:

a) Que la Política de Seguridad de la Información define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.

b) Que existen procedimientos para resolución de conflictos entre dichos responsables.

c) Que se han designado personas para dichos roles a la luz del principio de "separación de funciones".

d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.

e) Que se cumplen las recomendaciones de protección sobre medidas de seguridad, en función de las condiciones de aplicación en cada caso.

f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la Dirección.

En resumen: la Auditoría de la Seguridad del ENS es un proceso sistemático, independiente y documentado, para la obtención de evidencias y su evaluación objetiva, con el fin de determinar el grado de conformidad con el ENS del sistema de información auditado, debiendo permitir a sus responsables adoptar las medidas oportunas para subsanar las deficiencias y atender a las observaciones o recomendaciones que pudiera haber identificado el Equipo Auditor y, en su caso, posibilitar la obtención de la correspondiente Certificación de Conformidad con el ENS, que se examinará en el epígrafe siguiente.

Considerando que las auditorías de seguridad del ENS tienen como destinatarios los sistemas de información de las entidades del ámbito subjetivo de aplicación del RD 311/2022, de 3 de mayo, es muy importante determinar a priori cual será el alcance de la auditoría, identificando con precisión los sistemas de información comprendidos y los servicios prestados por medio de tales sistemas. Tanto unos (los sistemas de información) como los otros (los servicios sustentados en tales sistemas) deberán aparecer explícitamente mencionados en el Certificado de Conformidad con el ENS que, en su caso, se expida, y que se ajustará a lo dispuesto en la Resolución, de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad.

Desarrollar adecuadamente las Auditorías de Seguridad del ENS exige igualmente que la entidad auditora -muy especialmente, cuando se encuentra acreditada para la expedición de Certificaciones de Conformidad con el ENS, a la que se denomina Entidad de Certificación- posea unas determinadas características y capacidades.

Al objeto de facilitar la realización de las Auditorías de Seguridad, el ENS señala que el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones, para el mejor cumplimiento de lo establecido en el ENS, las Guías CCN-STIC deben considerarse como "Buenas Prácticas" o *soft law*[7]. Por tanto, no tratándose exactamente de normas imperativas, su cumplimiento no resulta obligatorio, aunque su inobservancia, caso de producirse algún incidente que pueda poner en riesgo la seguridad de los sistemas de información concernidos, podría derivar en responsabilidad.

Suele ser frecuente expresar la conformidad con una determinada normativa o regulación usando procedimientos que señalan cuales son las exigencias para poder optar a tal reconocimiento y su ulterior exhibición pública que, como en el caso del ENS, han sido regulados formalmente. La precitada ITS de Conformidad con el ENS señala los requisitos a los que deberán sujetarse las denominadas Declaraciones y Certificaciones de Conformidad con el ENS.

La Declaración de Conformidad con el ENS, aplicable exclusivamente a sistemas de información de categoría BÁSICA, podrá ser expedida por la propia entidad bajo cuya responsabilidad se encuentren dichos sistemas, tras haber superado una Autoevaluación, y se exhibirá mediante un Distintivo de Declaración de Conformidad cuyo uso estará condicionado a la expedición previa de la antedicha Declaración de Conformidad.

7 Que el diccionario panhispánico del español jurídico, de la Real Academia Española, define como el conjunto de normas o reglamentaciones no vigentes que pueden ser consideradas por los operadores jurídicos en materias de carácter preferentemente dispositivo y que incluye recomendaciones, principios, etc., que podrían influir en el desarrollo legislativo, pudiendo asimismo ser utilizadas como referentes específicos en la actuación judicial o arbitral.

Para publicar la Declaración de Conformidad con el ENS bastará con la exhibición en la sede electrónica (entidades del sector público) o página web (entidades del sector privado) del Distintivo de Declaración de Conformidad, que incluirá un enlace al documento de Declaración de Conformidad correspondiente, que también permanecerá accesible a través de dicha sede electrónica o página web.

Por su parte, la Certificación de Conformidad con el ENS, aplicable a los sistemas de información de cualquier categoría, solo podrá ser expedida por una Entidad de Certificación, tras haber superado una Auditoría de Certificación, y se exhibirá mediante un Distintivo de Certificación de Conformidad cuyo uso estará condicionado a la expedición previa de la antedicha Certificación de Conformidad.

La Certificación de Conformidad con el ENS, así como su Distintivo de Conformidad se expresarán en documentos electrónicos, en formato no editable.

Especialmente importante en el caso de las Certificaciones de Conformidad con el ENS es el papel desempeñado por las denominadas Entidades de Certificación, encargadas de auditar y certificar, en su caso, los sistemas de información sujetos a evaluación.

Las Entidades de Certificación deberán estar acreditadas por la Entidad Nacional de Acreditación (ENAC) para la certificación de sistemas del ámbito de aplicación del Esquema Nacional de Seguridad, conforme a la norma UNE-EN ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios. Como es sabido, la acreditación es la herramienta establecida a escala internacional para generar confianza sobre la correcta ejecución de un determinado tipo de actividades, denominadas Actividades de Evaluación de la Conformidad, y que incluyen ensayo, calibración, inspección, certificación o verificación entre otras. En general, cualquier actividad que tenga por objeto evaluar si un producto, servicio, sistema, instalación, etc. es conforme con ciertos requisitos, puede estar sujeta a acreditación. Dichos requisitos pueden estar establecidos por ley y tener por tanto carácter reglamentario o estar recogidos en normas, especificaciones u otros documentos de carácter voluntario.

Por último, el ENS confiere a la Secretaría General de Administración Digital (de la Secretaría de Estado para la Digitalización y la Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital) y al Centro Criptológico Nacional (adscrito al Centro Nacional de Inteligencia del Ministerio de Defensa), en sus respectivas competencias, la responsabilidad de velar por la adecuada implantación, desarrollo y seguimiento del ENS en las entidades de su ámbito de aplicación.

III. CONCLUSIONES

Como hemos podido analizar en los párrafos precedentes, y atendiendo a los riesgos derivados de operar en el ciberespacio, la ciberseguridad es una condición *sine qua non* para la adecuada prestación de los servicios públicos, sin la que no pueden satisfacerse los principios de atención pública señalados en nuestras leyes administrativas, en la Estrategia Nacional de Seguridad y en la Constitución.

Por tanto, habiendo descartado de su ámbito de aplicación la actual redacción de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020 los dispositivos médicos para uso humano (regulados en el Reglamento (UE) 2017/745), el modelo de ciberseguridad que habrá de aplicarse a los sistemas de los sistemas de información (y a sus elementos constitutivos individuales) dirigidos a prestar servicios sanitarios, deberá acomodarse a lo dispuesto en el antedicho real decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, del que hemos dado cuenta en estas páginas.

Es el momento, por tanto, de generar confianza en los destinatarios últimos de los servicios sanitarios, garantizando que los sistemas de información usados por las entidades públicas en su prestación son seguros y confiables.

IV. FUENTES CONSULTADAS

- Documentos de referencia del Centro Criptológico Nacional.
- MAGERIT versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
- Ley 8/2011, de 28 abril, de medidas para la Protección de las Infraestructuras Críticas.
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.