uc3m | Universidad Carlos III de Madrid

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Coordinadora Curso: **-Profª (PhD) María Nieves de la Serna Bilbao**

Titular de Derecho Administrativo UC3M// Departamento de Derecho Público

Co-directora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

TEMA 10: CIBERSEGURIDAD Y AMENAZAS HÍBRIDAS

III. EL PANORAMA REGULATORIO BÁSICO DE LA CIBERSEGURIDAD NACIONAL.

Elaborado por Profs. Dr. Carlos Galán Pascual (PhD) y Carlos Galán Cordero
Profesores Área Derecho Administrativo// Departamento de Derecho Público
Profesores Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz
Universidad Carlos III de Madrid

SUMARIO:

III. EL PANORAMA REGULATORIO BÁSICO DE LA CIBERSEGURIDAD NACIONAL.

3.1 Las Directivas NIS y su transposición al ordenamiento jurídico nacional.

3.2 La ciberseguridad pública: el Esquema Nacional de Seguridad.

III. EL PANORAMA REGULATORIO BÁSICO DE LA CIBERSEGURIDAD NACIONAL.

Si contemplamos la ciberseguridad como el conjunto de medidas dirigidas a satisfacer las exigencias de las que hemos denominado *dimensiones de la ciberseguridad* (disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y su conformidad legal) encontramos un significativo número de regulaciones que, en mayor o menor medida, generales o sectoriales, abordan tal problemática.

3.1 Las Directivas NIS y su transposición al ordenamiento jurídico nacional.

La que ha venido siendo conocida como Directiva NIS (**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**) fue publicada en el DOUE el 19 de julio de ese mismo año, y consideraba esencial que todos los Estados miembros de la UE poseyeran unas capacidades mínimas y una estrategia que garanticen un elevado nivel de seguridad de las redes y sistemas de información en su territorio, especialmente en lo tocante a lo que la norma europea definió como *operadores de servicios esenciales* y *proveedores de servicios digitales*, lo que debía traducirse en la adopción de un conjunto de medidas de ciberseguridad exigibles a tales entidades, tendentes a mejorar el funcionamiento del mercado interior.

Los destinatarios últimos de la norma se muestran en el cuadro siguiente:

Operadores de servicios esenciales, de los sectores…[1]
Energía: electricidad, crudo y gas.
Transporte: aéreo, ferrocarril, marítimo y fluvial y carretera.
Banca.
Infraestructuras de los mercados financieros.
Sector sanitario: entornos de asistencia sanitaria (entre ellos hospitales y clínicas privadas).
Suministro y distribución de agua potable.
Infraestructura digital: IXP, Proveedores de servicios DNS y Registros de nombres de dominio de primer nivel.
Proveedores de servicios digitales
Mercados en línea.
Motores de búsqueda en línea.
Servicios de computación en la nube.

Los **criterios** para la identificación de los operadores esenciales fueron:

a) Presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales;
b) La prestación de dicho servicio depende de las redes y sistemas de información, y
c) Un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.

La Directiva NIS, en resumen:

a) Establecía la obligación para todos los Estados miembros de adoptar una **estrategia nacional de seguridad** de las redes y sistemas de información;
b) Creaba un **Grupo de Cooperación** para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;

[1] Siempre que sean: a) una entidad presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales; b) la prestación de dicho servicio depende de las redes y sistemas de información, y c) un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.

c) Creaba una red de equipos de respuesta a incidentes de seguridad informática (Red de CSIRT[2]), con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;
d) Establecía **requisitos en materia de seguridad** y **notificación** para los operadores de servicios esenciales y para los proveedores de servicios digitales;
e) Establecía obligaciones para que los Estados miembros designen **autoridades nacionales competentes**, **puntos de contacto únicos** y **CSIRT** con funciones relacionadas con la seguridad de las redes y sistemas de información.

El 8 de septiembre de 2018, el Boletín Oficial del Estado publicaba el **Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información**, cumpliendo el mandato de transposición de la Directiva NIS.

Aunque la Directiva de la que traía causa limitaba su ámbito de aplicación a los denominados "operadores de servicios esenciales" y los "proveedores de servicios digitales", la norma española aprovechó el mandato para ampliar su alcance a sectores no expresamente incluidos en la europea (sin que ello suponga una derogación encubierta o un desplazamiento normativo de la legislación española vigente). Ejemplos significativos de esta ampliación lo constituyen los **prestadores de servicios de confianza** o los **operadores de redes y servicios de comunicaciones electrónicas**, que entran a formar parte de los destinatarios de la norma, en cuanto puedan ser designados operadores críticos.

Conviene señalar, llegado este punto, el esfuerzo desarrollado por el grupo de trabajo de redacción del RD-ley para cohonestar en aquel momento las tres normas estatales de especial significación en materia de (ciber)seguridad: el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS)[3], la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas y la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional[4].

---

[2] *Computer Security Incident Response Team*
[3] Recientemente derogado por Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
[4] Recordamos que los sectores estratégicos definidos en la Ley 8/2011, de 28 de abril, son: Administración; Espacio; Industria Nuclear; Industria Química; Instalaciones de Investigación; Agua; Energía; Salud; TIC; Transporte; Alimentación y Sistema Financiero y Tributario.

El modelo de gobernanza recogido en este RD-ley se sustenta en el esquema de competencias que las vigentes Estrategias de Seguridad y Ciberseguridad nacionales han dibujado: el Consejo de Seguridad Nacional, el Consejo Nacional de Ciberseguridad, las Autoridades Competentes y los CSIRT de referencia, confiriendo a las así denominadas Autoridades Competentes las funciones de supervisión, vigilancia y sancionadora, reservando para los CSIRT de referencia las funciones más operativas, tales como el análisis de riesgos y la conducción operativa nacional de la respuesta a incidentes, actuación nacional amparada en lo dispuesto en el art. 1491.29ª de nuestra Constitución, que confiere al Estado las competencias exclusivas en materia de seguridad nacional, siendo la ciberseguridad una de sus manifestaciones, como hemos señalado antes.

Estos CSIRT de referencia constituyen, a nuestro entender, la piedra angular sobre la que descansa el tratamiento de la ciberseguridad, pues, más allá de las funciones otorgadas legalmente a las Autoridades Competentes, materializan los mecanismos de prevención, detección y respuesta a los incidentes, funciones que, a partir de la entrada en vigor de este nuevo RD-ley, vienen exigiendo de todos ellos la máxima coordinación, como asimismo prevé la norma, que confiere al CCN-CERT (del Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia) la función de coordinador nacional en los supuestos de especial gravedad.

Pese a tratarse de una norma en vigor y, por tanto, ejecutiva, el Real Decreto-ley pospuso a su desarrollo reglamentario determinadas cuestiones que veremos más adelante.

En la actualidad, son numerosas las regulaciones de sustrato tecnológico que prescriben la notificación de incidentes al organismo competente de que se trate en cada caso. Esta diversidad, de la que en muchas ocasiones es sujeto obligado la misma entidad, alienta y justifica la existencia de una Plataforma Común para la notificación de incidentes, capaz de dar respuesta, a través de un solo proceso (contemplando la notificación inicial, las intermedias y la final) dirigido automáticamente a cada autoridad competente por razón de la legislación afectada, lo que puede constituir, a nuestro juicio, una de las medidas más innovadoras de este Real Decreto-ley en materia de ciberseguridad, a imagen de lo que ha venido desarrollando en CCN-CERT en el Sector Público con la plataforma LUCIA.

El RD-ley exhibe un régimen de infracciones especialmente riguroso. Un solo ejemplo: en determinadas circunstancias, tipifica como muy grave la falta de adopción de las medidas para subsanar las deficiencias detectadas o el incumplimiento reiterado de la obligación de notificar los incidentes.

El desarrollo reglamentario al que antes nos hemos referido tuvo lugar por **Real Decreto 43/2021, de 26 de enero**, que vino a regular los siguientes aspectos:

- La identificación de los factores específicos en los sectores de los operadores de servicios esenciales para determinar si un incidente podría tener efectos perturbadores significativos.
- En la determinación de las Autoridades Competentes, la autoridad sectorial correspondiente por razón de la materia, cuando no se trate de operadores críticos.
- Dentro de las funciones de las Autoridades Competentes, el establecimiento de canales de comunicación con los operadores de servicios esenciales y los proveedores de servicios digitales, y los protocolos de actuación para la coordinación con los CSIRT de referencia.
- La identificación de los operadores de servicios esenciales con incidencia en la Defensa Nacional.
- La determinación de los supuestos de especial gravedad que requieran de la coordinación nacional del CCN-CERT.
- La determinación de los mecanismos de coordinación de los CSIRT de referencia con la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras y Ciberseguridad del Ministerio del Interior, cuando las actividades de respuesta puedan afectar a un operador crítico.
- La determinación de las medidas técnicas y de organización que deberán adoptar los operadores de servicios esenciales y los proveedores de servicios digitales.
- La fijación de los plazos para la designación y comunicación a la Autoridad Competente por parte de los operadores de servicios esenciales, de la persona, unidad u órgano colegiado responsable de la seguridad de la información y la identificación de sus funciones.
- La determinación, a efectos de notificación, de los sucesos o incidencias que podrían afectar a las redes y sistemas de información, aun cuando todavía no lo hayan hecho.
- La determinación de las medidas necesarias relativas a la notificación de incidentes por parte de los operadores de servicios esenciales.
- El órgano de la autoridad competente para la imposición de sanciones en el caso de infracciones graves o leves.

Posteriormente, se publicó una nueva Directiva, denominada coloquialmente NIS2.0, que deroga la anterior, la **Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas**

destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148.

Efectivamente, durante la segunda mitad de 2020, la Comisión Europea llevó a cabo una evaluación de los resultados alcanzados con la Directiva NIS, incluyendo una consulta pública que concluyó, desde diversos ámbitos, la necesidad de mejorar la transposición de la norma, su alcance y su definición.

Como consecuencia de ello, la Comisión presentó una propuesta de revisión[5] que trataba de mejorar algunos problemas que la primera Directiva NIS no había resuelto y que, como se ha dicho[6], aparecían en la antedicha evaluación, tales como la reducida ciberresiliencia empresarial, la diferente implementación según los países, el bajo conocimiento situacional y la carencia de respuestas comunes.

En su exposición de motivos, la Comisión reconoce que:

- El ámbito de aplicación de la Directiva NIS se ha quedado pequeño debido al avance de la digitalización y la conectividad en los últimos años y no incluye a servicios digitales relevantes.
- Tampoco incluye a todos los actores relevantes porque los criterios de la Directiva y de las transposiciones nacionales para identificar los proveedores de servicios digitales no han sido claros.
- Por las mismas razones, el procedimiento para la notificación de incidentes por los proveedores de servicios esenciales no es el mismo y las sanciones y exigencia de obligaciones varía en cada Estado miembro.
- El intercambio de información entre actores públicos y privados sigue siendo muy bajo y poco sistematizado.
- La disparidad de los recursos presupuestarios y humanos disponibles por los Estados miembros condiciona su nivel de madurez y su capacidad de ciberresiliencia.

La nueva Directiva refleja así el deseo de la Comisión de extender el ámbito de aplicación de la norma europea a otros actores, tales como los suministradores

[5] Propuesta de Directiva COM (2020) 823 (final) de la Comisión de 16 de diciembre sobre medidas para un alto nivel común de Ciberseguridad en la UE y Anexos sobre entidades esenciales e importantes.
[6] Arteaga. F. “La evaluación y la revisión de la Directiva NIS: la directiva NIS2.0”. R. I. Elcano (Feb., 2021)

de servicios o redes públicas de comunicación, los de contenidos o datos, los de plataformas de redes sociales y los dedicados a fomentar la confianza en los anteriores o a las Administraciones Públicas, los servicios postales, la gestión de aguas, el espacio, la alimentación, entre otros, eliminando la clasificación actual de operadores de servicios esenciales y proveedores de servicios digitales, sustituyéndolos por **entidades esenciales** y **entidades importantes.**

La adscripción por sectores de las entidades contempladas en la nueva Directiva NIS2.0 es la siguiente:

Entidades Esenciales	Entidades Importantes
- Energía (Electricidad, Calefacción y refrigeración urbana, Crudo, Gas, Hidrógeno) - Transporte (Aire, Ferrocarril, Agua, Carretera). - Banca. - Infraestructuras de los mercados financieros. - Salud. - Agua potable. - Aguas residuales. - Infraestructura Digital[7]. - Administraciones públicas. - Espacio.	- Servicios postales y de mensajería. - Gestión de residuos. - Fabricación, producción y distribución de productos químicos. - Producción, transformación y distribución de alimentos. - Fabricación[8]. - Proveedores digitales (Mercados en línea, Motores de búsqueda en línea, Plataformas de servicios de redes sociales.) - Investigación.

[7] Entre ellas: - Proveedores de Puntos de Intercambio de Internet - Proveedores de servicios de DNS, excluidos los operadores de servidores de nombres raíz - Registros de nombres de TLD - Proveedores de servicios de computación en la nube - Proveedores de servicios de centros de datos - Proveedores de redes de entrega de contenidos - Proveedores de servicios de confianza a los que se refiere el punto (19) del artículo 3 del Reglamento (UE) n.º 910/2014(1) - Proveedores de redes públicas de comunicaciones electrónicas a los que se refiere el punto (8) del artículo 2 de la Directiva (UE) 2018/1972(2) o proveedores de servicios de comunicaciones electrónicas a los que se refiere el punto (4) del artículo 2 de la Directiva (UE) 2018/1972 cuando sus servicios estén disponibles al público. Gestión de servicios de TIC (B2B); Gestión de servicios de TIC (B2B); Proveedores de servicios gestionados (MSP) - Proveedores de servicios de seguridad gestionados (MSSP).

[8] Fabricación de productos sanitarios y productos sanitarios para diagnóstico in vitro; productos informáticos, electrónicos y ópticos; maquinaria y equipos n.c.o.p.; vehículos de motor, remolques y semirremolques y otro material de transporte.

En ambos grupos, el nuevo texto obliga a los estados a supervisar (mediante actuaciones *ex ante* o *ex post*, atendiendo a su adscripción) las medidas de seguridad que hayan de adoptarse por las entidades afectadas, que, en caso de incumplimiento, conllevarían importantes sanciones.

De nuevo el análisis de riesgos previo, como método para la determinación de las medidas de seguridad adecuadas, se configura como un elemento esencial, también de esta nueva norma, al igual que ya lo viene siendo, por ejemplo, en el caso español con el Esquema Nacional de Seguridad.

Por último, también al tiempo de redactar estos párrafos, y dando respuesta a los llamamientos a la acción por parte del Consejo[9] y del Parlamento[10] para revisar el actual enfoque de seguridad de las entidades críticas y garantizar una mayor armonización con la Directiva NIS, acaba de publicarse la **Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo**, cuyo objeto es mejorar la prestación en el mercado interior de servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales, aumentando la resiliencia de las entidades críticas que prestan tales servicios, haciendo frente al aumento de la interconexión entre el mundo físico y digital mediante un marco legislativo con sólidas medidas de resiliencia, tanto para los aspectos cibernéticos como físicos, tal como se establece en la Estrategia para una Unión de la Seguridad[11].

Como señala su texto introductorio, la norma refleja los enfoques nacionales que ponen el acento en las interdependencias intersectoriales y transfronterizas, en las que la protección es solo un elemento junto con la prevención y mitigación de riesgos, la continuidad de las actividades y la recuperación (resiliencia).

Así pues, esta Directiva tiene por objeto:

a) Establecer la obligación de los Estados miembros de adoptar determinadas medidas destinadas a garantizar la prestación en el

[9] Conclusiones del Consejo, de 10 de diciembre de 2019, sobre las acciones complementarias para aumentar la resiliencia y luchar contra las amenazas híbridas (doc. 14972/19).
[10] Informe sobre las conclusiones y recomendaciones de la Comisión Especial sobre Terrorismo del Parlamento Europeo (2018/2044 (INI)).
[11] COM(2020) 605.

mercado interior de servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales, en particular para identificar las entidades y entidades críticas que deberán considerarse equivalentes en determinados aspectos y para permitirles cumplir sus obligaciones;

b) Establecer obligaciones de las entidades críticas destinadas a aumentar su resiliencia y mejorar su capacidad de prestar esos servicios en el mercado interior;
c) Establecer normas sobre la supervisión y ejecución de las entidades críticas, y la supervisión específica de las entidades críticas consideradas de particular importancia europea.

Siendo su ámbito de aplicación cualquiera de las entidades (públicas o privadas) de uno de los tipos mencionados en su Anexo, y que asimismo haya sido identificada como "entidad crítica" por un Estado miembro de conformidad con el artículo 5 de la misma, los tipos de entidades relacionados con el sector **Infraestructura Digital** son los siguientes:

- Los proveedores de puntos de intercambio de Internet (de la Directiva NIS2.0).
- Los proveedores de servicios de DNS (de la Directiva NIS2.0).
- Los registros de nombres del dominio de primer nivel (de la Directiva NIS2.0).
- Los proveedores de servicios de computación en nube (de la Directiva NIS2.0).
- Los proveedores del servicio de centros de datos (de la Directiva NIS2.0).
- Los proveedores de redes de distribución de contenidos (de la Directiva NIS2.0).
- Los proveedores de servicios de confianza a que se refiere el artículo 3, punto 19), del Reglamento (UE) n.º 910/2014 (Reglamento eIDAS).
- Los proveedores de redes públicas de comunicaciones electrónicas a que se refiere artículo 2, punto 8), de la ya estudiada Directiva 2018/1972/UE (Código Europeo de Comunicaciones Electrónicas) o los proveedores de servicios de comunicaciones electrónicas en el sentido del artículo 2, punto 4), de la Directiva (UE) 2018/1972, en la medida en que sus servicios estén a disposición del público.

Entre los cuales también se encuentran los proveedores de redes públicas de comunicaciones electrónicas.

3.2 La ciberseguridad pública: el Esquema Nacional de Seguridad.

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*."

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.

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 concretas, de naturaleza organizativa y técnica, según la siguiente distribución:

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.

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 Transformación Digital y para la Función Pública 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.