4.
Protección de datos y seguridad de la información

La ciberseguridad

Marta Cabrera de Arrate
Letrada del Parlamento de Canarias

RESUMEN: El **mundo digital** ha supuesto la transformación de la sociedad a un nivel inimaginable lo que ha repercutido directamente en el funcionamiento de las administraciones públicas que se han visto obligadas a adaptar la prestación de sus servicios de forma segura. Aquí entra en juego la **ciberseguridad** esencial para proteger datos y garantizar derechos digitales en un mundo constantemente amenazado por los ataques informáticos. Los **ciberataques r**epresentan riesgos económicos, sociales y políticos, lo que ha determinado la necesidad de crear marcos normativos como el **Esquema Nacional de Seguridad (ENS)** en España y **la Directiva NIS2** en la Unión Europea. Ambas regulaciones normativas establecen principios, medidas y obligaciones para proteger **infraestructuras críticas, datos y servicios públicos**, fomentando la confianza ciudadana y la **resiliencia** frente a amenazas digitales en un entorno cada vez más interconectado.

ABSTRACT: The **digital world** has brought about the transformation of society to an unimaginable level, which has directly impacted the functioning of public administrations, forcing them to adapt the delivery of their services in a secure manner. This is where **cybersecurity** comes into play, as it is essential to protect data and safeguard digital rights in a world constantly threatened by cyberattacks. Cyberattacks pose economic, social, and political risks, which has led to the need for regulatory frameworks such as the **National Security Framework (ENS)** in Spain and the **NIS2 Directive** in the European Union. Both regulations establish principles, measures, and obligations to **protect critical infrastructures, data, and public services**, fostering citizen trust and resilience against digital threats in an increasingly interconnected environment.

https://doi.org/10.36151/RCAP.6.10

I. LA CIBERSEGURIDAD, EL ENS, LA NIS2, Y LAS ADMINISTRACIONES PÚBLICAS

El mundo digital es una realidad presente y futura, y ha transformado completamente la forma en que la sociedad se relaciona hasta el punto de que prácticamente todas las actividades —profesionales, económicas y privadas— se desarrollan haciendo uso de las nuevas tecnologías y están estrechamente vinculadas desde el nivel social y económico al mundo virtual e internet[1].

Las administraciones públicas también han tenido que adaptar su actividad a este mundo digital debiendo de adecuar la prestación de sus servicios respondiendo a las nuevas demandas del ciudadano, un servicio público electrónico que integra las nuevas tecnologías dentro del sistema de información. En este aspecto, la administración pública y la ciberseguridad han demostrado estar entrelazadas actuando de la mano en la práctica totalidad del ejercicio de sus funciones ya que las primeras deben responder con un mínimo de seguridad en los respectivos ámbitos competenciales encomendados, la administración sirve al ciudadano y este servicio se ha de prestar con la garantía de seguridad propia. Por ello, recae sobre las administraciones públicas la función de impulsar las políticas necesarias que hagan efectiva los derechos digitales de la ciudadanía, particularmente en el uso de internet[2].

Consideramos a la ciberseguridad como un elemento estratégico dentro del mundo digital en el que vivimos lo que evidentemente implica que todas la Administraciones Públicas del estado español, de la Unión a nivel internacional e incluso global, deban de observar la rápida transformación digital que afecta a nuestra sociedad de una forma indiscutible y que debe actuar en consecuencia, tanto por los beneficios que ha demostrado instaurar en nuestra sociedad como por los incidentes que se han tenido que afrontar. La digitalización de la administración pública también ha determinado nuevos desafíos frente a las amenazas o ciberataques soportados propias del medio virtual.

En esta era digital el nacimiento de la ciberseguridad se debe claramente a las medidas de seguridad con las que se contraponen los ciberataques. Por ello, debemos de entender el término de ciberataque como atacar a un bien jurídico y sus consecuencias, para entonces comprender la necesidad de la ciberseguridad.

---

1 Ley 3/2018, de 5 de diciembre, de protección de Datos Personales y de garantía de los derechos digitales: "Internet, por otra parte, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad."

2 Ley 3/2018, de 5 de diciembre, de protección de Datos Personales y de garantía de los derechos digitales: "Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de los ciudadanos en internet promoviendo la igualdad d ellos ciudadanos y de los grupos en las que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital"

El ciberataque puede determinarse como un riesgo constatable para la sociedad de la más diversa índole, cuyo nivel de gravedad según el objeto puede alcanzar incluso la paralización completa de una actividad económica, suponer una grave crisis sanitaria o filtrar datos personales de los ciudadanos, etc. Así se pueden distinguir tres objetos de un ciberataque: económico, personal o social, y político [3]. Por esta razón, el ciberataque o ciberdelito es un elemento que genera desconfianza para los usuarios de internet de los sistemas electrónicos y digitales de los que la Administración pública dispone. El elemento crucial de protección son los datos que aportan los ciudadanos y las empresas en sus relaciones con la administración pública, datos que se filtran en las redes y que como consecuencia de un ciberataque o amenaza puede afectar al sistema de funcionamiento y prestación de servicios del sector público.

Estos ciberataques se transforman avanzando a pasos agigantados al igual que evoluciona el mundo digital.

Toda esta evolución tecnológica ha requerido que nuestras administraciones públicas estén en una constante actualización y desarrollo normativo, avanzando de forma sinérgica con los procesos transformadores que experimenta la sociedad, estableciendo medidas que permitan garantizar el funcionamiento de los servicios públicos, es la ciberseguridad la que en su respectivo ámbito de aplicación blinda de seguridad a nivel nacional a cada uno de los Estados miembros respectivamente, la ciberseguridad cumple con su fin cual es proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales, ciberataques que ocasionan graves lesiones a los derechos de la sociedad, y con ello preservar los derechos del ciudadano garantizando la funcionalidad de los servicios y recursos, públicos, esenciales [4]. Pues bien hasta la fecha este dato se puede fácilmente constatar en los numerosos textos normativos tanto nacionales aprobados hasta la fecha como a nivel comunitario que se han tenido que transponer al nuestro derecho español, entre los que podemos destacar el ya derogado Real decreto 3/2010, de 9 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica; la Ley 36/2015, de 28 de septiembre, de Seguridad nacional; el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad nacional 2017; el Real decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 (ENS, en adelante); la Direc-

---

3 Miró Llinares, distingue tres categorías (I)"cibercriminalidad económica", que incluye todas aquellas conductas en las que el autor ataca bienes patrimoniales de los que pretende apropiarse, como las ciberestafas; (II) "cibercriminalidad personal o social" que tiene por objeto la persona y las relaciones personales, como el ciberbullying, y (III) "cibercriminalidad política" que incluye todos los ciberdelitos que tienen como objeto los Estados u organizaciones políticas que persiguen su desestabilización, como es el ciberterrorismo.

4 Ley Orgánica 3/2018, de 5 de diciembre, de protección de Datos Personales y de garantía de los derechos digitales: "En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía".

tiva (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 (NIS2 en adelante), por la que se modifican el Reglamento (UE) n.º 910/2014; o la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

II. EL ESQUEMA NACIONAL DE SEGURIDAD (ENS) Y LA DIRECTIVA 2022/2555 (NIS2)

A continuación, desarrollaremos el impacto que ha supuesto en nuestro Estado español, en especial en nuestras administraciones públicas la aplicación en un primer momento del ENS y, a continuación, la trasposición de la Directiva conocida como la NIS2 a nuestro ordenamiento jurídico; participando ambas normas en el desarrollo y aplicación de las medidas de seguridad a nivel nacional, y en especial como consecuencia de la trasposición de la normativa comunitaria a nuestro derecho nacional. A estos efectos podemos confirmar que el derecho a la seguridad digital se contempla como: «Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos" [5].

III. LA CIBERSEGURIDAD COMO CONSECUENCIA DEL ESQUEMA NACIONAL DE SEGURIDAD (ENS).

1. Teniendo pues por sentado lo anterior, en lo que respecta a la totalidad del sector público en el ejercicio de las funciones que tiene encomendadas deberán actuar salvaguardando la confidencialidad de las personas físicas y jurídicas y con ello cualquier dato identificativo como titulares del derecho que son, en garantía del principio legítimo cumpliendo con la normativa que protege al ciudadano. De acuerdo con los párrafos anteriores con el fin de acercarnos a las demandas sociales el legislador debe actualizar constantemente nuestros textos normativos, razón por la que entra en vigor el reciente Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, (ENS, en adelante), que tiene como principal objetivo que mediante el mismo se cumplan los principios básicos y requisitos mínimos necesarios que blinden de protección adecuada toda la información que se tramite por las entidades públicas en sus sistemas electrónicos y de información en atención a los servicios prestados por estas. Con estos principios y requisitos se pretende asegurar los siguientes parámetros: el acceso, la confidencialidad, la integridad, la trazabilidad, la au-

[5] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y de Garantía de los Derechos Digitales, en su artículo 82 reconoce el derecho a la seguridad digital.

tenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos gestionados por todo el sector público y por el sector privado vinculados o dependientes de la administración pública, esto es, cuando presten servicios o provean soluciones a las entidades del sector público para el ejercicio por éstas de sus competencias y potestades normativas[6].

Los organismos públicos en el ejercicio de sus competencias disponen diariamente de las tecnologías de la información y de las comunicaciones (TIC, en adelante), considerándose como aquel *conjunto de recursos, herramientas y sistemas que permiten la gestión, procesamiento, almacenamiento y transmisión de datos, voz, texto, video e imágenes para facilitar la interacción y el acceso a la información. Incluyen desde hardware y software hasta internet, redes y medios de comunicación como la radio, la televisión y los teléfonos*, por lo que al hacer uso de los sistemas de información se debe actuar garantizando la seguridad de los usuarios y, concretamente, en lo que respecta a la salvaguarda y confidencialidad de los datos personales que se trate mediante la normativa que resulte de aplicación como la directiva de protección de datos básica y su Ley de trasposición (Directiva 95/46/CE, reglamento General de Protección de Datos; Ley Orgánica 7/2021, de 26 de mayo, de protección de datos digitales, entre otras, o la propia actuación de la Agencia Española de Protección de Datos). En el mismo sentido, se deberá observar los principios básicos que el ENS establece, pues para que las administraciones públicas puedan alcanzar sus objetivos todos los elementos de seguridad y recursos en ella implicados deberán ser atendidos con carácter prioritario dentro del sistema de información que actúa de forma garantista contribuyendo a que una organización pueda alcanzar sus objetivos de una forma óptima. En consecuencia, tanto el principio de seguridad entendido dentro de un proceso integral de intercambio de comunicación e información entre las entidades públicas y privadas, como el resto de los principios básicos actuaran reduciendo los posibles riesgos y amenazas cibernéticas, o anulando los efectos adversos a los que la administración puede y debe enfrentarse cuando se vea afectada por la complejidad y sofisticación de los cada vez más frecuentes ciberataques.

2. Para garantizar la seguridad de la información que el sector público maneja se tendrá que actuar conforme a los principios básicos [7] que la norma establece para prevenir y detectar las amenazas e incidentes que se puedan produ-

---

6 Ley 40/2015, de 2 de octubre, del Régimen Jurídico del Sector público, artículo 2 relativo al ámbito subjetivo de aplicación.

7 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, los principios básicos vienen regulados en el artículo 5, y son: a) Seguridad como proceso integral; b) Gestión de la seguridad basada en los riesgos; c) Prevención, detección, respuesta y conservación; d) Existencia de líneas de defensa; e) Vigilancia continua; f) Reevaluación periódica; y g) Diferenciación de responsabilidades.

cir o llegar a manifestar, en cuyo caso se dará oportuna respuesta mediante la restauración de la información y servicios que pudieran resultar afectados. Las medidas de seguridad atenderán a diferentes niveles de protección de los datos e información según la relevancia o importancia de la información en juego y los efectos negativos que un ciberataque o ciberamenaza pudiera suponer para el conjunto de la sociedad. Por las razones expuestas es por lo que también integran los principios básicos la vigilancia continua para actuar ante una posible amenaza y, en caso de producirse, reaccionar conforme a una línea de defensa preestablecida estratégicamente que minimice los resultados que comprometan el sistema de información del que la administración pública sea responsable.

Los principios básicos advertidos serán gestionados por las personas responsables del servicio, de la seguridad y del sistema que hubieren sido designados al efecto para el tratamiento de la información y prestación de los servicios [8], y que deberán actuar atendiendo a las políticas de seguridad aprobada en cada administración pública. Las personas responsables del sistema de información desempeñan una laboriosa e importante función dentro del ENS, pues ostentan la facultad de valorar la información que ha de estar cubierta por la seguridad correspondiente en atención a su importancia, para la posterior categorización de la información por el responsable de la seguridad, es decir, una vez valorada la información por el responsable de la información o servicio pasaría a integrarse en la categoría de seguridad determinada por el responsable de la seguridad.

3. Los Anexos I y II del Real Decreto 2011/2022, de 3 de mayo por el que se regula el ENS, respectivamente determinan las categorías de seguridad de los sistemas de información y las distintas medidas de seguridad que serían aplicables a cada una de las categorías. Es el responsable de la información o del servicio quien valorará el impacto que tendría sobre la sociedad un incidente que afectase a la seguridad de la información, valoración que atenderá las cinco dimensiones de seguridad establecidas que son: la confidencialidad, la integridad, la trazabilidad, la autenticidad y la disponibilidad. Para seguidamente el responsable de la seguridad determine el nivel de seguridad correspondiente con la dimensión según el grado en el que pudiera verse afectado por el incidente cibernético, así, si la dimensión de seguridad no se viera afectada evidentemente no se adscribirá a ningún nivel, si el perjuicio que pudiere causar la organización fuere limitado se adscribiría al nivel bajo, si fuere grave perjuicio entonces pasaría a nivel medio, y si fuere muy grave se adscribiría al nivel alto [9].

En cuanto a las medidas de seguridad que el ENS desarrolla e implementa se distinguen las medidas de seguridad físicas (protección de las instalaciones, control de accesos, vigilancia, entre otros); técnicas (implementación de siste-

---

[8] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el artículo 7 dedica la regulación a la organización e implantación del proceso de seguridad.

[9] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, ANEXO I.2 y 3 determinan las dimensiones y el nivel de seguridad que corresponda.

mas de seguridad, software de seguridad, antivirus, firewalls, etc); y organizativas (gestión de personal, formación, políticas de seguridad, planes de contingencia, etc), que tienen en común garantizar el cumplimiento y efectividad de los principios básicos y requisitos mínimos advertidos por el ENS, son medidas de seguridad diversas que se seleccionan y se aplican según la dimensión, el nivel y la categoría de seguridad de que se trate.

Además, cabría advertir que el citado ENS se aplicará de forma complementaria con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD, en adelante), normativa con la que comparte ámbito material. Así, la disposición adicional primera de la LOPDP, observa las medidas de seguridad en el ámbito del sector público mencionando las obligaciones que el ENS debe implantar en el 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*, y matiza que, en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad deberán corresponderse con las de la Administración pública de origen y, en todo caso, observando lo que indique al respecto el ENS en su Real Decreto.

4. En resumen, el ENS constituye una herramienta de seguridad clave para el sistema de información que actúa en garantía de la información y datos que las administraciones públicas manejan, estableciendo los criterios y estándares necesarios de seguridad para proteger particularmente la información sensible a la que tiene acceso la administración pública y que utiliza para el cumplimiento de sus fines, tanto datos personales como aquella otra información relevante para la sociedad que un ciberataque o amenaza cibernética pudiera producir efectos tan negativos como llegar a estar dentro del nivel alto, por ejemplo, la anulación de la capacidad de la organización en el ejercicio de sus funciones, que puede causar un daño incluso irreparable en los activos de la organización o daño grave a las personas de imposible o difícil reparación. A estos efectos podríamos citar el reciente caso del ciberataque producido al servidor del SEPE sin que hubiera entrado en vigor el ENS en aquel momento, pues *el pasado 9 de marzo de 2021, el Servicio Público de Empleo Estatal (SEPE) sufrió un ciberataque que dejó inoperativo su sistema informático durante más de dos semanas. Aunque, la actividad habitual no se recobra completamente hasta cerca de un mes después de que tuviese lugar el suceso. Se relata a través de los medios de comunicación que los trabajadores del SEPE se encontraron esa mañana el sistema operativo bloqueado, el cual ni permitía el acceso al control de asistencia de los trabajadores, ni tampoco a la gestión de los servicios electrónicos. Ante esta situación, se toma la decisión de apagar los ordenadores para estudiar de dónde provenía el error del sistema.*[10]

---

[10] Juan FERRI, "Los retrasos por el ciberataque en el SEPE afectarán a 90.000 personas", Europress, 8 de abril de 2021.

Se desprende fácilmente de todo este engranaje que mediante el ENS se interesa fomentar la confianza de los ciudadanos en su relación con la Administración pública electrónica que en el ejercicio de sus funciones pretende blindar de seguridad los sistemas y datos que actual y particularmente el servicio público ofrece a través TIC. Para ello, el ENS no debe ignorar la rapidez con la que avanza el mundo digital razón por la que debe actualizar su normativa de forma sinérgica para enfrentar la amenazas a la par que se actualice la ciberseguridad, lo que va a permitir que las organizaciones públicas estén preparadas ante los desafíos emergentes que se puedan producir incluso a nivel mundial.

En definitiva, consideramos al ENS como un marco legal y técnico que ayuda a las organizaciones a implementar medidas de seguridad efectivas para proteger la información y los sistemas, garantizando la confianza del ciudadano en el actuar de la administración electrónica. Así mismo, persigue fomentar la seguridad en el sector público, para lo que promueve la cultura de la seguridad, pues si bien es cierto que un correcto funcionamiento del ENS fomenta la creación de una cultura de seguridad en las organizaciones, donde la seguridad de la información es considerada como un aspecto fundamental y prioritario; también es cierto que los ciberataques se producen constantemente en el mundo digital que avanza a su vez a gran velocidad esquivando las medidas de seguridad que frente estos adoptan las administraciones públicas, siendo muy complicado que las medidas de seguridad se articulen estratégicamente con carácter previsor reaccionando a los incidentes o hackeos que se puedan producir normalmente con técnicas más avanzadas.

IV. LA CIBERSEGURIDAD COMO CONSECUENCIA DE LA NIS2

1. La transformación del mundo digital en el que nos desenvolvemos requieren una actualización constante del ordenamiento jurídico vigente, en el que la ciberseguridad y la privacidad de datos no pasan desapercibidas, sino muy al contrario podemos referirnos a ella sin lugar a dudas como un pilar fundamental en el funcionamiento y estrategias que las instituciones europeas, entidades tanto públicas como privadas, deben observar y mediante su óptima utilización se pretende garantizar el correcto funcionamiento de los estados miembros de la Unión, que tienen el deber de responder ante las constantes amenazas y resultados consecuencia de los ciberataques sufridos por las entidades de la Unión, siendo el sector público una de las instituciones más afectadas debido a los intereses en juego, esto es, en relación con la información y datos que manejan.

La introducción de las nuevas normativas debe garantizar un equilibrio entre la protección de los derechos de las personas y la capacidad de las empresas para implementar estrategias que aseguren su viabilidad operativa en un entorno di-

gital cada vez más desafiante[11]. En este ámbito, la ciberseguridad desempeña un papel esencial en el continuo funcionamiento de todas las instituciones, entidades públicas y privadas, dentro de un contexto social digitalizado mediante el que prestan los servicios que llevan implícito garantizar la integridad de la información protegiendo de este modo la soberanía nacional, las infraestructuras críticas y los derechos de los ciudadanos. Razones por las que las instituciones afectadas deben adaptarse al entorno digital, y, en consecuencia, hacer frente a la avalancha de ciberataques que se producen a diario.

En este contexto normativo entra en vigor la Directiva 2022/2555, (NIS2, en adelante) "*Network and Information Security 2*", que actualiza la anterior Directiva 2016/1148, sobre la seguridad de las redes y los sistemas de información en la Unión Europea (NIS). El objetivo principal de la NIS2 es alcanzar el fortalecimiento y armonización normativa aplicable a todos los Estados miembros en materia de ciberseguridad con el fin de proteger la infraestructura digital implantada en los sistemas de información. Así, en los últimos tiempos se ha constatado que los ciberataques sufridos han ido *in crescendo* pudiéndose demostrar una interrelación y dependencia de la sociedad con la actividad digital, en consecuencia, resultando afectado la economía mundial.

La NIS2, nace para alcanzar un nivel de ciberseguridad común en toda la Unión mediante la implantación de medidas que determinan una mejora en el funcionamiento del mercado interior fortaleciendo la ciberseguridad particularmente en las infraestructuras críticas esenciales para el funcionamiento de la sociedad y la economía, como la energía, el transporte, la salud, el agua y las telecomunicaciones, entre otras. La aplicación de la NIS2 por los estados miembros de la Unión persigue el cumplimiento de un marco común que gestione los riesgos que aparezcan, las notificaciones de incidentes y la cooperación entre los diferentes sectores implicados, y así mejorar el funcionamiento del mercado interior mediante, en definitiva, un nivel común de ciberseguridad.

La NIS2 es una Directiva novedosa en tanto que entró en vigor el 16 de enero de 2023, cuya trasposición al ordenamiento jurídico de los estados miembros de los que España forma parte se ordena para la fecha 17 de octubre de 2024. En este sentido la NIS2 obliga a los Estados miembros a que adopten estrategias nacionales de ciberseguridad y designen autoridades competentes para gestionar la ciberseguridad, puntos de contacto únicos y equipos de respuesta a los incidentes de seguridad informática (CSIRT, en adelante).

2. En cuanto al ámbito de aplicación, particularmente, la NIS2 afecta a la mayoría de las entidades que están bajo el obligado cumplimiento del ENS, el cual ha ido incorporando progresivamente las nuevas exigencias establecidas en la NIS2 que trataremos seguidamente en este artículo.

---

[11] Prieto Pérez, Tamara. Revista Crítica de Relaciones de Trabajo. Laborum n.º 12 (3.º Trimestre 2024).

Por una parte, se dirige a las entidades identificadas en los Anexos I y II de la NIS2 y las de carácter crítico que deberán de aplicar las medidas de gestión de riesgos de ciberseguridad, así como los procedimientos de notificación establecidos. De esta forma vamos a observar cómo comienzan a actuar interconectados en este ámbito material concreto los estados miembros para poder hacer frente de una forma efectiva a los ciberataques, entre otras, mediante las notificaciones sobre las estrategias nacionales de ciberseguridad adoptadas, los planes nacionales de respuesta frente a los incidente y crisis de ciberseguridad afrontados, normas y obligaciones que se imponen a los estados miembros de la Unión para hacer efectivo el intercambio de información sobre la ciberseguridad que se deba de aplicar.

Concretamente, la directiva obliga a las empresas, entidades públicas y privadas, dentro del ámbito de aplicación de la NIS2 a que estén identificadas en los términos establecidos y teniendo como fecha límite para ello el 17 de abril de 2025 [12], pues solo así se daría cumplimiento al objetivo que persigue la NIS2. Principalmente, afecta a las entidades públicas o privadas que cumplan con los tipos previstos en el anexo I y II de la citada Directiva, y que se consideran como medianas empresas o que presten sus servicios o realicen sus actividades dentro de la Unión, pero también aquellas otras superen el límite de mediana empresa y cumplan con las particularidades previstas en la Directiva que se analiza.

La explicación de que las entidades a los que va dirigida la NIS2 deban estar identificadas correctamente antes del 17 de abril de 2025, se encuentra en hacer efectivo el principio de coordinación entre las entidades afectadas pues de esta forma las entidades concernidas podrán actuar coordinadamente ante un ciberataque ya que una vez identificadas entra en juego el sistema de notificaciones predispuesto para este fin. Así como la obligación que recae sobre los Estados miembros consistente en designar a las autoridades competentes al efecto, los puntos de contacto únicos y los CSIRT, conformándose un equipo de actuación frente a los ciberataques y amenazas, y las crisis que puedan producirse, poniendo de manifiesto entonces el nivel de efectividad de la ciberseguridad aplicada.

Por tanto, queda claro que la Directiva que nos concierne, en su artículo 2 impone obligaciones a las medianas y grandes empresas que presten sus servicios o realicen sus actividades dentro de la Unión, y en todo caso a las entidades mencionadas en el Anexo I "sectores de alta criticidad" y II "otros sectores críticos" de la presente Directiva (entidades esenciales); y que las entidades que se encuentran dentro de los sectores de alta criticidad son las referidas al sector

---

[12] 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, establece en su artículo 3 el deber que tienen los Estados miembros de elaborar una lista de las entidades esenciales e importantes así como de las entidades que prestan servicios de registro de nombres de dominio, supervisando que dichas entidades estén identificadas y registradas oportunamente.

de la energía (electricidad, red de transporte, mercado eléctrico…); el crudo, el gas, hidrógeno; sector del transporte; sector de la banca; sector de las infraestructuras de los mercados financieros; sector sanitario (farmacéuticos, laboratorios…); sector del agua; sector de la infraestructura digital; sector de la gestión de servicios de las TIC.

Por otra parte, en lo que respecta a la aplicación de la NIS2 por las administraciones públicas, se exige que estas cumplan con el carácter de esencial, destacando que en todo caso es de obligado cumplimiento la aplicación de la NIS2 por las administraciones públicas centrales y regionales reconocidas por nuestro derecho nacional, cuya explicación está en que su funcionamiento y actividad tiene un impacto significativo en las actividades sociales y económicas críticas. En tanto que la administración pública a nivel local y los centros de enseñanza cuando practiquen estas últimas actividades críticas de investigación, podrán aplicar la NIS2, desprendiéndose por tanto el carácter potestativo para la aplicación de la NIS2 por estas entidades. No obstante, estarían excluidas del ámbito de aplicación de la NIS2 las administraciones públicas que desempeñen actividades de seguridad nacional, seguridad pública, y defensa en los términos indicados, así mismo están expresamente excluidos de su ámbito de aplicación el poder judicial, los parlamentos y los bancos centrales, como se indica en diversos artículos de la Directiva y en la definición que esta describe de "entidad de la Administración pública".[13]

3. En cuanto a las medidas de ciberseguridad que deben aplicar las entidades competentes van a variar según la esencialidad o la importancia de la actividad que se pretenda proteger con la NIS2. Así, entendemos por actividades críticas a las que se refiere la directiva NIS2 aquellas que ocupan su funcionamiento en los sectores esenciales para la sociedad y la economía, y que podemos desglosar en entidades "esenciales" e "importantes" según su nivel de criticidad. Concretamente, los sectores esenciales incluyen energía, transporte, banca, sanidad y administración pública; mientras que los sectores importantes abarcan la fabricación química, producción de alimentos, gestión de residuos y servicios postales. En consecuencia, cada estado miembro cuyas entidades cumplan con estas características de criticidad en la prestación de sus servicios o realización de sus actividades se verá obligado a adoptar una estrategia nacional de ciberseguridad mediante la implementación de unas medidas de seguridad robustas con planes de respuesta a incidentes que garanticen la resiliencia de sus sistemas frente a la avalancha de ciberataques que enfrentan, para lo que harán uso de los recursos necesarios medidas políticas y normativas adecuadas que alcancen un elevado nivel de ciberseguridad, como pueden ser la promoción y desarrollo de la edu-

[13] 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, artículos 2, 6 y Anexo I (apartado 10).

cación en materia de ciberseguridad o la investigación para el desarrollo de la ley y mejora de las herramientas de ciberseguridad precisas o la promoción de la ciberprotección activa.

4. Debemos tener presente que un incidente a los efectos de la aplicación normativa de la NIS2 será aquel que pueda causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada, o que el incidente pueda repercutir perjudicialmente a las personas tanto físicas como jurídicas. Por tanto, los Estados miembros, además de supervisar el que las entidades hayan cumplido, como ya hemos advertido, con estar debidamente identificadas en el sistema, deberán designar a las autoridades competentes encargadas de la ciberseguridad en el respectivo Estado miembro así como nombrar a los puntos de contacto único —correspondiendo uno por cada estado miembro— que ejercerán funciones de enlace para hacer efectiva la cooperación transfronteriza entre los estados miembros y, en su caso, con la Comisión y la ENISA.

En consecuencia, la Directiva NIS2 impone diversas obligaciones funcionales a los Estados miembros entre las que nos encontramos además de las ya mencionadas elaborar estrategias nacionales de ciberseguridad, estrategias que se harán efectivas a través de las autoridades competentes encargadas de la ciberseguridad y las autoridades de gestión de crisis de ciberseguridad, ambas autoridades deberán ser designadas por el estado miembro respectivo. Además, los "puntos de contacto únicos" designados por cada Estado miembro ejercerán una función de enlace para garantizar la cooperación transfronteriza entre los Estados miembros, la Comisión y la ENISA, y, a la que ahora unimos, la cooperación intersectorial con las autoridades competentes designadas al efecto.

En el mismo sentido, los Estados miembros deberán designar uno o varios equipos de respuesta a incidentes de seguridad informática (CSIRT, en adelante (*Computer Security Incident Response Team*)) [14]. En cada caso las entidades afectadas deberán notificar al CSIRT una alerta para atender de manera temprana el incidente que se describa detalladamente lo que incluye la gravedad del impacto, el tipo de amenaza, las medidas aplicadas y las posibles repercusiones transfronterizas. Los CSIRT en el marco de la autoridad competente cubriendo a las entidades esenciales o críticas, según el caso, a efectos de responsabilizarse procedimentalmente de la gestión de los incidentes que deban ser afrontados por estos haciendo uso de los recursos necesarios para tal fin. Así mismo, la identidad de los CSIRT también deberá constar en el sistema y notificarse a la Comisión. De esta forma se pretende dar efectividad a la cooperación entre las

[14] Equipo de Respuesta ante Emergencias Informáticas (Computer emergency response team: Un Equipo de Respuesta ante Emergencias Informáticas es un centro de respuesta para incidentes de seguridad en tecnologías de la información. Está formado por un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información (Fuente Wikipedia).

múltiples entidades tanto a escala nacional como internacional y a nivel de la Unión entre los Estados miembros.

En lo que se refiere los CSIRT, en resumen, las autoridades competentes practicarán las notificaciones precisas para combatir los incidentes cibernéticos y las ciberamenazas, e informarán al respecto al punto de contacto único nacional afectado o sin son varias naciones afectadas a nivel transfronterizo se notificará a sus respectivos puntos de contacto respectivos. Observando, en consecuencia, que las actuaciones acometidas por estas entidades realizadas de manera efectiva conformarían un engranaje de cooperación e intercambio de información sobre los incidentes y ciberamenazas que con los oportunos contraataques se garantizaría unos resultados competentes que anulen, reduzcan o eviten los posibles daños generados en el bien protegido.

En estas operaciones cibernéticas mediante las redes de cooperación internacional se actúa garantizando el principio confidencialidad en el plan nacional de ciberseguridad que se apruebe.

Así mismo, se designará un Grupo de Cooperación que estará integrado por representantes de los Estados miembros, de la Comisión y de la ENISA. En el ejercicio de sus funciones podrán invitar a participar al Parlamento Europeo, presentar informes a la Comisión, al Parlamento Europeo y al Consejo sobre las experiencias adquiridas a nivel estratégico en materia de ciberseguridad para la mejora de esta. En lo que respecta a la cooperación internacional y a nivel de la Unión, cabría matizar que el Grupo de Cooperación designado para el apoyo y cooperación estratégica, entre otras, intercambiará información entre los Estados miembros de acuerdo con los principios de confianza y colaboración, participando en este proceso informativo tanto el Parlamento Europeo, el Consejo, y las CSIRT a las que ya hemos hecho referencia.

Es importante reiterar que los Estados miembros a través de sus autoridades competentes, puntos de conexión únicos, y las CSIRT, brindarán el apoyo necesario para abordar los incidentes y ciber amenazas transfronterizas que ocurran en el Estado miembro afectado, y reducir o evitar la posible repercusión que estos incidentes pudieran ocasionar en otros Estados miembros cuando pasaran la frontera y que cuando se manifieste una crisis de ciberseguridad actúan el EU-CyCLONe[15], que está integrada por representantes de las autoridades de gestión de ciberseguridad de los Estado miembros, haciendo efectivo el intercambio de información cooperación, evaluación de las repercusiones como consecuencia de los incidentes y crisis relacionados a gran escala. En estas opera-

[15] Es la Red europea de organizaciones de enlace para las crisis de ciberseguridad, un organismo que apoya la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala en la UE, asegurando el intercambio de información relevante entre los Estados miembros y las instituciones de la UE. Establecida por la Directiva NIS2, esta red facilita la concienciación situacional compartida, la evaluación del impacto y la coordinación de la respuesta a incidentes, con el apoyo de la ENISA como secretaría.

ciones de ciberseguridad también participa a nivel de la Unión la Red Europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe). La cooperación internacional entre el Grupo de cooperación, la red de CSIRT y EU-CyCLONe, se encargará de adoptar acuerdos internacionales que cumplan con el derecho de la unión en materia de protección de datos. Por tanto, cuando las crisis cibernéticas, incidentes o ciberamenazas se detecten a nivel de la Unión entrarán en juego para su combate el Grupo de Cooperación, la red de CSIRT y EU-CyCLONe.

5. En relación con la gestión de riesgos serán las propias entidades esenciales e importantes las que adopten las medidas necesarias que gestiones los riesgos en atención a la seguridad de los sistema de redes y de información utilizados por estas para la realización de sus operaciones y prestación de servicios, medidas que podrán consistir en la adopción de políticas de seguridad de los sistemas de información, gestión de incidentes, formación en ciberseguridad, controles de acceso o procedimientos relativos a la criptografía, entre otras.

6. De conformidad con los marcos legislativos e institucionales nacionales aplicados por cada Estado miembro se respetan las normas sobre responsabilidad aplicables a sus instituciones públicas, funcionarios y cargos electos. Así mismo, los Estados miembros en la aplicación efectiva de la NIS2 podrán determinar la imposición de medidas de supervisión y ejecución adecuadas, proporcionadas y eficaces en relación con las entidades de la Administración pública, que podrán consistir en la práctica de inspecciones *in situ* de las entidades, realizar auditorías precisas de seguridad, solicitar el acceso a los datos, documentos e información necesaria para la efectiva supervisión, pudiendo llegar incluso a solicitar la imposición de multas o suspensión administrativas por el deficiente funcionamiento en atención a la gravedad del incumplimiento o la disposición en su caso infringida[16].

Los Estados miembros deben establecer mecanismos para supervisar el cumplimiento de la directiva para lo que tienen que contar con autoridades competentes encargadas de supervisar a las entidades esenciales e importantes, realizar inspecciones, proporcionar asistencia y recopilar información sobre incidentes cibernéticos para mejorar la ciberseguridad en la UE[17].

---

16 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. Capítulo VII. Supervisión y ejecución.

17 Debe prestarse la debida atención a la naturaleza, gravedad y duración de la infracción de la presente Directiva, los perjuicios materiales o inmateriales originados, la intencionalidad o negligencia en la infracción, las medidas adoptadas para prevenir o paliar los perjuicios materiales o inmateriales, el grado de responsabilidad o cualquier infracción anterior pertinente, el grado de cooperación con la autoridad competente y cualquier otra circunstancia agravante o atenuante. Las medidas de ejecución, incluidas las multas administrativas, deben ser proporcionadas y su imposición debe estar sujeta a las garantías procesales adecuadas conforme a

En relación con lo anterior, los incumplimientos relativos a la violación de seguridad de datos personales la NIS2 también busca armonizar los regímenes sancionadores entre los Estados miembros, por lo que cuando las autoridades competentes tengan constancia en el transcurso de ejercicio de sus funciones de supervisión o ejecución de que el incumplimiento de las obligaciones puede conllevar una violación de la seguridad de los datos personales deberá notificarse e informar sin demora a las autoridades de control determinadas.

Con la finalidad de garantizar el cumplimiento efectivo de las obligaciones contempladas en la NIS2, las autoridades de control designadas al efecto están facultadas para imponer multas administrativas, solicitar su imposición o imponer medidas de ejecución, según el caso concreto.

V. CONCLUSIÓN

En este contexto, la NIS2 se presenta en el mundo digital como una herramienta decisiva en el ecosistema digital más seguro y resiliente en la Unión Europea, robusteciendo y potenciando las capacidades de respuesta ante los incidentes cibernéticos emergentes, contemplando un conjunto de medidas que buscan garantizar un nivel común de ciberseguridad en los sectores críticos y esenciales, propios de una sociedad virtualmente interconectada.

Para finalizar, la reciente entrada en vigor de la Directiva NIS2 supone que la doctrina jurisprudencial sea escasa en relación con la ciberseguridad por lo que será necesario que el ordenamiento jurídico vaya incorporando los principios y normas que abordan los conceptos digitales que abran camino y establezcan una base doctrinal que vaya adquiriendo firmeza y genere seguridad jurídica a nivel global.

El Estado tiene la responsabilidad de proteger la ciberseguridad como bien jurídico para la seguridad nacional, para lo que se ha desarrollado normas que hoy integran nuestro ordenamiento jurídico, es crucial evaluar la eficacia y eficiencia de dicho marco jurídico para proteger los derechos y libertades de los ciudadanos en el ámbito virtual. Las leyes actuales considero que no son suficientes para garantizar la ciberseguridad de los ciudadanos, debiendo de desarrollar textos normativos que aseguren tanto el funcionamiento digital del Estado como del ciudadano a nivel virtual. En definitiva, el ordenamiento jurídico debe evolucionar de manera proactiva, anticipándose a los desafíos futuros y proporcionando un marco normativo que fomente la innovación, la competitividad y la protección integral en el contexto digital.

---

los principios generales del Derecho de la Unión y de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta»), entre ellas, el derecho a la tutela judicial efectiva, a un juicio justo, la presunción de inocencia y los derechos de la defensa.

Como nos indica el Tribunal Constitucional, en su sentencia 20/2023, de 23 de marzo: <<(…) se detiene en el análisis de la STC 142/2018, que definió la ciberseguridad, como el "conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno" (FJ 4), por tanto, como una materia transversal, no reconducible a un único título, y que "afecta a cuestiones relacionadas con la seguridad pública y la defensa, las infraestructuras, redes y sistemas y el régimen general de telecomunicaciones"(…) la ciberseguridad es uno de los aspectos imprescindibles a tener en cuenta al configurar la estrategia en materia de seguridad nacional, y la Ley 8/2011, de 28 de abril, que establece medidas para la protección de las infraestructuras críticas se dicta de conformidad con el art. 149.1.29 CE; (ii) que el art. 10 de la Ley 36/2015, de 28 de septiembre, de seguridad nacional —que se dicta al amparo del art. 149.1.4 y 29 CE—, incluye la ciberseguridad en los ámbitos de especial interés para la seguridad nacional; (iii) la ciberseguridad es una de las funciones propias del Centro Nacional de Inteligencia, tal y como resulta de la letra b) del art. 4 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia; (iv) la Orden PCI/870/2018, de 3 de agosto, confirma la relación entre ciberseguridad y seguridad nacional; (v) la disposición final primera del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, afirma que dicha norma, que identifica los sectores en los que es necesario garantizar la protección de las redes y sistemas de información, y establece procedimientos para identificar los servicios esenciales ofrecidos en dichos sectores, así como los principales operadores que prestan esos servicios, se dicta al amparo de las competencias estatales del art. 149.1.21 y 29 CE.(…)>>.

En conclusión, de acuerdo con Expósito Gázquez, entendemos que el propio Tribunal Constitucional reconoce que la ciberseguridad se ha convertido en una herramienta estratégica que coadyuva a preservar la seguridad del país, como una parcela más del que debe responsabilizarse el Estado. El régimen jurídico de la ciberseguridad no puede calificarse de escueto, puesto que se han dispuesto distintas normas para intentar preservar la integridad y el normal funcionamiento de la actividad del Estado. Sin embargo, la pregunta que debemos realizarnos es si todo ese conjunto normativo es eficaz y eficiente para proteger el bien jurídico que se pretende, como es el caso de la protección de los derechos y libertades de los ciudadanos en el medio virtual[18].

[18] Expósito Gázquez, Ariana. CIBERATAQUE AL SEPE: ¿POSIBLE RESPONSABILIDAD PATRIMONIAL?, en sus conclusiones, página 25.

VI. NORMATIVA RELACIONADA

- 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 (Directiva SRI 2).
- Constitución Española
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

VII. BIBLIOGRAFÍA

PRIETO PÉREZ, Tamara. Revista Crítica de Relaciones de Trabajo. Laborum n.º 12

Estudios de Doctrina Judicial ISSN: 2792-7962 – ISSNe: 2792-7970

EXPÓSITO GÁZQUEZ, Ariana. CIBERATAQUE AL SEPE: ¿POSIBLE RESPONSABILIDAD PATRIMONIAL? Revista General de Derecho Administrativo

FERNÁNDEZ BERMEJO, D. y MARTÍNEZ ATIENZA, G.: Ciberseguridad, ciberespacio y ciberdelincuencia, Cizur Menor, Aranzadi Thomson Reuters, 2018.

Articles, Directive (EU) 2022/2555 (NIS 2 Directive): https://www.nis-2-directive.com/NIS_2_Directive_Articles.html

Best Practices for Cyber Crisis Management, Febrero 28, 2024. Enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY.

MORENO FONTARROSA, Adrián. Ciberseguridad en las Administraciones Públicas: visión práctica. Actualidad Administrativa, n.º 9, Septiembre de 2022, Editorial Wolters Kluwer

TERRÓN SANTOS, D. (Dir.) y DOMÍNGUEZ ÁLVAREZ. J.L.: Inteligencia artificial y defensa: nuevos horizontes, Navarra, Aranzadi Thomson Reuters, 2021.

Jurisprudencia

- Sentencia del Tribunal Constitucional número 20/2023, de 23 de marzo
- Sentencia del Tribunal Constitucional número 142/2018, de 20 de diciembre de 2018.