VICEPRESIDENCIA SEGUNDA
DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

MAIN V-1 (14-6-21)

MEMORIA DEL ANÁLISIS DE IMPACTO NORMATIVO DEL PROYECTO DE REAL DECRETO POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD

RESUMEN EJECUTIVO

Ministerio/s	Ministerio de Asuntos Económicos y Transformación Digital	**Fecha**	14/6/2021
Órgano proponente	Secretaría General de Administración Digital		
Título de la norma	**PROYECTO DE REAL DECRETO POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD**		
Tipo de Memoria	Normal [X] Abreviada [ ]		
OPORTUNIDAD DE LA PROPUESTA			
Situación que se regula	Se regula el Esquema Nacional de Seguridad, actualizando el contenido del RD 3/2010, de 8 de enero, a la realidad impuesta por el marco legal, la evolución tecnológica, las nuevas ciberamenazas y sus actores, facilitando su implantación por las entidades del sector público y aquellas entidades del sector privado que colaboran con aquellas en el tratamiento de información o en la prestación de servicios públicos. Por estas razones es necesario acometer una actualización del Esquema Nacional de Seguridad que derogue el vigente Real Decreto 3/2010, de 8 de enero y que se apliquen en su tramitación las previsiones del artículo 27.1 b) de la Ley 50/1997, de 27 de noviembre, del Gobierno, pues la intensificación de las ciberamenazas y ciberincidentes que se está produciendo y la imprevisibilidad en cuanto a su número, complejidad técnica y daño potencial que pueden causar al sector público y al privado, justifican la tramitación urgente de dicho proyecto de real decreto para disponer cuanto antes del instrumento normativo adecuado para dar respuesta a estas circunstancias.		

Objetivos que se persiguen	Acomodar la respuesta de las entidades públicas a las amenazas provenientes del ciberespacio, propiciando su resiliencia ante los ataques y ciberincidentes y propiciando un tratamiento más seguro de la información pública y de los servicios públicos prestados a la ciudadanía y las empresas, determinando la política, los principios básicos, los requisitos mínimos de seguridad y medidas de protección que deberán adoptarse por parte de las entidades del Sector Público (y por aquellas entidades del sector privado que colaboran con aquellas), y atendiendo al nuevo marco legal impuesto por las normativas europeas y nacionales en materia de seguridad de la información, al tiempo que se introduce la capacidad de personalizar los requisitos del ENS a cada colectivo considerado, reduciendo vulnerabilidades y promoviendo la defensa activa.
Principales alternativas consideradas	Inicialmente se valoró la posibilidad de modificar el Real Decreto 3/2010, de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Sin embargo, el Real Decreto 3/2010 ha quedado significativamente obsoleto con el tiempo como para abordar una nueva modificación, se por ello se ha considerado más oportuno tramitar un real decreto de nueva planta, al amparo de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y de acuerdo con la nueva regulación existente en materia de protección de datos, protección de las redes y los sistemas de información, la Estrategia Nacional de Ciberseguridad de 2019, las infraestructuras disponibles y los actuales estándares tecnológicos de seguridad y auditoría.
CONTENIDO Y ANÁLISIS JURÍDICO	
Tipo de norma	Real Decreto.
Estructura de la Norma	El real decreto consta de 41 artículos distribuidos en nueve capítulos, cuatro disposiciones adicionales, una disposición transitoria, una disposición derogatoria, tres disposiciones finales y cuatro anexos. El Anexo I regula las categorías de seguridad de los sistemas de información detallando la secuencia de actuaciones para determinar la categoría de seguridad de un sistema; el Anexo II detalla las diferentes medidas de seguridad; el Anexo III trata la Auditoría de la seguridad y, por último, el Anexo IV incluye el glosario de términos y definiciones.

Informes recabados	
Informes pendientes	- Informe de los diferentes ministerios, de acuerdo con lo previsto en el artículo 26.5 de la Ley 50/1997, de 27 de noviembre. - Consulta a las CCAA y a la FEMP a través de la Comisión Sectorial de Administración Electrónica - Informe de la Agencia Española de Protección de Datos - Informe de la Secretaría General de Coordinación Territorial del Ministerio de Política Territorial y Función Pública evacuado para de dar cumplimiento al trámite previsto en el artículo 26.5 LG - Informe de la Secretaría General Técnica del Ministerio de Política Territorial y Función Pública, conforme a lo previsto en el artículo 26.5 de la Ley 50/1997, del Gobierno. - Informe de la Oficina de Coordinación y Calidad Normativa del Ministerio de la Presidencia y para las Administraciones Territoriales de conformidad con lo dispuesto en el artículo 26.9 de la Ley 50/1997. - Informe de la Secretaría General Técnica del Ministerio de Asuntos Económicos y Transformación Digital, conforme a lo previsto en el artículo 26.5 de la Ley 50/1997, del Gobierno. - Dictamen del Consejo de Estado, en aplicación del artículo 22.3 de la Ley Orgánica 3/1980, de 22 de abril, del Consejo de Estado.
Consulta pública previa	No se realiza, de acuerdo con lo previsto en el artículo 27.1 y 27.2.b) Ley 50/1997, de 27 de noviembre, del Gobierno, al tramitarse el proyecto normativo con carácter urgente en virtud del punto segundo del Acuerdo de Consejo de Ministros de 25 de mayo de 2021 sobre actuaciones urgentes en materia de ciberseguridad, que ordena la actualización del Esquema Nacional de Seguridad mediante la tramitación y aprobación urgente de un real decreto que sustituya al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, como medida urgente de refuerzo del marco normativo.
Audiencia pública	Trámite de información pública, previsto en el artículo 133.2 de la Ley 39/2015, de 1 de octubre, así como en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

ANALISIS DE IMPACTOS		
ADECUACIÓN AL ORDEN DE COMPETENCIAS	Este real decreto se dicta al amparo de lo dispuesto en ejercicio de las competencias previstas en los artículos 149.1.18ª, 149.1.21ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las Administraciones públicas, sobre las telecomunicaciones y sobre la seguridad pública, respectivamente.	
IMPACTO ECONÓMICO Y PRESUPUESTARIO	**Efectos sobre la economía en general.**	La norma tendrá efectos positivos de forma indirecta en la economía como consecuencia de la mejora en la seguridad de la información y la reducción del impacto de los incidentes de ciberseguridad, así como debido al fomento de la utilización de los medios electrónicos para la realización de trámites y procedimientos. Además de ello, el marco dibujado por el nuevo ENS contribuirá a incrementar el desarrollo tecnológico nacional y el despliegue de soluciones y servicios prestados por el tejido industrial español. Las medidas tendrán un efecto positivo sobre la productividad. El incremento y racionalización de medidas de seguridad de los datos e información que circulan por las diferentes infraestructuras y que son empleadas en la prestación de los servicios por parte de las empresas del Sector Privado, así como por las propias Administraciones Públicas y demás entidades del Sector Público, junto con la mayor eficacia en la gestión de los riesgos de incidentes de seguridad de la información, reducirá el impacto perjudicial de estos incidentes en los servicios, redundando en una mayor productividad en su prestación y garantizará, además, el derecho de los ciudadanos y empresas a preservar sus datos y operar con una mayor confianza en el mercado y hacia el Sector Público.

	En relación con la competencia	☐ La norma no tiene efectos significativos sobre la competencia. ■ La norma tiene efectos positivos sobre la competencia. ☐ La norma tiene efectos negativos sobre la competencia.
	Desde el punto de vista de las cargas administrativas.	☐ Supone una reducción de cargas administrativas. Cuantificación estimada_____€ ☐ Incorpora nuevas cargas administrativas. Cuantificación estimada_____€ ■ No afecta a las cargas administrativas
	Desde el punto de vista de los presupuestos, la norma ☐ Afecta a los presupuestos de la Administración General del Estado. ☐ Afecta a los presupuestos de otras Administraciones Territoriales.	☐ Implica un gasto. El impacto en los presupuestos de las demás Administraciones Territoriales dependerá de las necesidades y decisiones que adopte cada Administración competente. ☐ Implica un ingreso. Cuantificación estimada: _____€
IMPACTO DIGITAL	Las medidas propuestas en este real decreto mejorarán la protección de la información manejada y de los servicios prestados, contribuyendo a una mayor confianza y continuidad de los servicios, particularmente en relación con el ejercicio de derechos y el cumplimiento de obligaciones, gracias a una mejor protección frente a ciberamenazas y ciberataques orientados a la información.	
IMPACTO DE GÉNERO	La norma tiene un impacto de género	Negativo ☐ Nulo ■ Positivo ☐

OTROS IMPACTOS CONSIDERADOS	• **Impacto en la seguridad pública y en la seguridad nacional**: La mejora en la seguridad sobre el acceso a medios electrónicos, así como en el aseguramiento de la integridad, la disponibilidad, la autenticidad, la confidencialidad y privacidad, la trazabilidad y conservación de los datos, ayudará a reducir los riesgos en ciberamenazas que atenten contra la seguridad pública y la seguridad nacional. • No tiene impacto de carácter social, en materia de protección a la familia, ni respecto a la infancia y la adolescencia. • Respecto al **impacto medioambiental**, no obstante, señalar que el perfeccionamiento del ENS fomenta necesaria y directamente el empleo de la tecnología y los canales electrónicos de comunicación y relación, por lo que puede tener un impacto positivo en la medida en que se reducen desplazamientos superfluos, se reduce el consumo de papel y ayuda a reducir la generación de residuos en general. • Por los mismos motivos, en materia de **igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad** el perfeccionamiento del ENS refuerza de forma indirecta la defensa de derechos individuales, como el derecho a un acceso rápido, eficaz y eficiente a los servicios web públicos a través de los medios electrónicos, derecho a disponer de unos servicios web de calidad que sean útiles y satisfagan sus necesidades, derecho a recibir una información transparente y veraz, y al mismo tiempo, derecho a preservar la privacidad de los ciudadanos y sus datos personales.
OTRAS CONSIDERACIONES	No se realizan

ÍNDICE DE LA MEMORIA

2. Principales novedades
3. Análisis jurídico.

III.- ADECUACIÓN DE LA NORMA AL ORDEN DE DISTRIBUCIÓN DE COMPETENCIAS
IV.- DESCRIPCIÓN DE LA TRAMITACIÓN

1. Descripción de los trámites realizados.
2. Trámites pendientes.

V.- ANÁLISIS DE IMPACTOS

1. Impacto económico
2. Impacto presupuestario.
3. Análisis de las cargas administrativas.
4. Impacto de los medios y servicios digitales que conlleva la norma.
5. Impacto por razón de género.
6. Impacto en la infancia y en la adolescencia.
7. Impacto en la familia.
8. Impacto por razón de materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

I.- OPORTUNIDAD DE LA PROPUESTA

1.- MOTIVACIÓN

a) Causa de la propuesta.

El artículo 42 del Real Decreto 3/2020, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en lo sucesivo, "ENS") establece el principio de actualización permanente del ENS en los siguientes términos: "*El Esquema Nacional de Seguridad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, de la evolución tecnológica y nuevos estándares internacionales sobre seguridad y auditoría en los sistemas y tecnologías de la información a medida que vayan consolidándose las infraestructuras que lo apoyan*".

Pues bien, tras la última actualización del ENS operada en el año 2015 por el Real Decreto 951/2015, de 23 de noviembre, se han sucedido múltiples hitos que requieren una revisión integral de la norma que regula el ENS:

- La experiencia obtenida de la implantación del ENS en las Administraciones Públicas desde su aprobación hace más de una década.
- La evolución y especialización de los agentes afectados directa o indirectamente por el ENS.
- La instauración de la certificación del ENS, hace cinco años, a raíz de la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprobaba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, y el

conocimiento inferido a consecuencia de las numerosas evaluaciones exhaustivas realizadas y certificaciones otorgadas.

- La redefinición de una posición institucional en el ámbito de la ciberseguridad, de acuerdo con la Estrategia Nacional de Ciberseguridad de 2019.
- El surgimiento de nuevos vectores de ataque y amenazas cada vez más complejas y sofisticadas de difícil trazabilidad.
- Las actualizaciones en el marco jurídico aplicable, con importantes novedades, trae como consecuencia la necesidad de adaptación del ENS:
  - en materia de seguridad de las redes y sistemas de información mediante el Real Decreto-ley 12/2018, de 7 de septiembre, desarrollado a su vez por el Real Decreto 43/2021, de 26 de enero, que señala que las medidas para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales tomarán como referencia las recogidas en el anexo II Real Decreto 3/2010 (Esquema Nacional de Seguridad);
  - en materia de seguridad pública (Real Decreto-ley 14/2019, de 31 de octubre);
  - en materia de protección de datos, mediante el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE – Reglamento General de Protección de Datos – y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales);
  - los postulados recogidos en el reciente 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, exigen la recepción de un actualizado marco de la ciberseguridad pública, pretensión de la que asimismo trae causa este renovado Esquema Nacional de Seguridad.
- El Plan Digitalización de las Administraciones Públicas, instrumento para la ejecución de los fondos del Componente 11 «Modernización de las Administraciones Públicas» del Plan de Recuperación, Transformación y Resiliencia, así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025, contempla la actualización del ENS entre las reformas normativas a abordar con el fin de evolucionar la política de seguridad de las Administraciones Públicas españolas (que alcanza a todas las entidades del Sector Público), tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información. Se trata de una reforma que se ve complementada por la inversión destinada a constituir el Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos que servirá de referencia para las demás Administraciones Públicas y contribuirá a mejorar en cumplimiento del ENS de las entidades en su alcance de servicio. Posteriormente esta previsión

ha sido respaldada por el Acuerdo de Consejo de Ministros de 25 de mayo de 2021 sobre medidas urgentes en materia de ciberseguridad.

b) Identificación de los colectivos afectados

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos a cuyo ámbito de aplicación se remitía el ENS fue derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Esta última norma, además, introduce la obligación para todas las personas jurídicas de relacionarse por medios electrónicos con las Administraciones Públicas.

Asimismo, la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, amplia el ámbito de aplicación – que originariamente alcanzaba solamente a las Administraciones Públicas y ciudadanos – a todo el Sector Público, en las condiciones señaladas por la norma.

Adicionalmente, la Ley Orgánica 3/2018, de 5 de diciembre, establece que el ENS deberá regular aquellas medidas a implantar en caso de tratamiento de datos personales de acuerdo con los criterios del artículo 32 del Reglamento General de Protección de Datos. Esta circunstancia afecta directamente a todas aquellas organizaciones del Sector Privado que colaboran de algún modo u otro con las Administraciones Públicas y demás entidades del Sector Público (particularmente en el ámbito de la seguridad de la información, infraestructuras electrónicas, desarrollo de aplicaciones, transformación digital y ciberseguridad).

Lo anterior, unido al carácter heterogéneo de todas y cada una de las Administraciones Públicas y entidades afectadas, trae consigo la necesidad de identificar específicamente los actores involucrados directa o indirectamente en el proceso de elaboración de la norma y que se ven afectados por ella:

- De acuerdo con el apartado 2 del artículo 156 de la Ley 40/2015, de 1 de octubre, el ámbito de aplicación es el previsto en el artículo 2 de la misma.
- En aplicación de lo dispuesto en el artículo 27.2 del proyecto, los requisitos establecidos en el mismo se aplicarán a los sistemas de información que permitan los tratamientos de datos personales en el ámbito subjetivo y con el alcance al que se refieren el artículo 77.1 y la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre.
- Resultará de aplicación 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 a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

Además, será de aplicación a los sistemas que manejan o tratan información clasificada, sin perjuicio de que pudiera resultar necesario complementar las medidas señaladas en el presente real decreto con otras específicas para tales sistemas, derivadas de los compromisos internacionales contraídos por España o su pertenencia a organismos o foros internacionales en la materia.

c) Interés público afectado

Desde la aparición del Esquema Nacional de Seguridad en 2010, la realidad nos muestra un escenario de incremento de los ciberataques, en número, frecuencia, sofisticación y severidad del impacto, con agentes y actores de la amenaza que han ampliado sus capacidades técnicas y su operativa; y que, aprovechando la dependencia de las tecnologías de la información y las comunicaciones de nuestra sociedad y la interconexión de los sistemas, vienen afectando, incesantemente, a un número cada vez mayor de entidades públicas y privadas, a sus cadenas de suministro, a los ciudadanos y, por ende, a la ciberseguridad nacional, comprometiendo el normal desenvolvimiento social y económico de nuestra sociedad y el ejercicio de los derechos y libertades de los ciudadanos.

El proyecto sirve al interés de adecuar el ENS al contexto legal y tecnológico actual en aras de proteger los servicios prestados a la ciudadanía, junto a la información que éstos manejan, que adquieren en su conjunto, en calidad de servicios públicos, la condición de materia de seguridad nacional. Por consiguiente, el interés público afectado se circunscribe, de forma más general y abstracta, en la seguridad nacional y, de forma más concreta, en el derecho de la ciudadanía y demás colectivos involucrados a preservar la seguridad de sus datos e información, a la vez que asegurar la disponibilidad de los servicios públicos que les son ofrecidos.

d) *Necesidad de aprobación*

El progreso de la transformación digital de nuestra sociedad nos expone de forma cada vez más intensa a la materialización de ciberamenazas, a los ciberincidentes, que constituyen hoy en día una de las amenazas más significativas para el normal desenvolvimiento de las sociedades, instituciones, empresas y ciudadanía.

España afronta un escenario en el que los ciberataques son crecientes y se intensifican en frecuencia, sofisticación, alcance, número de entidades afectadas y severidad del impacto. Estos ciberataques amenazan a entidades del sector público, así como del sector privado, y a la ciudadanía en definitiva, comprometiendo la seguridad, la protección de los datos, así como el ejercicio de derechos y libertades, a la vez que nuestro progreso social y económico.

Ante esta evidencia, la Estrategia Nacional de Ciberseguridad, publicada en 2019, consignó entre sus objetivos la seguridad y resiliencia de las redes y sistemas de información y comunicaciones del Sector Público a lograr a través de medidas tales como la plena implantación del Esquema Nacional de Seguridad y la implantación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos.

No obstante, la creciente presión de ciberataques sobre entidades del Sector Público, así como sobre entidades del Sector Privado en calidad de proveedores o suministradores tecnológicos del Sector Público, aconseja reforzar la capacidad de ciberresiliencia y fortalecer la ciberseguridad entre otras medidas a través de robustecer el marco normativo.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y su modificación parcial en 2015, se aprobaron en contexto normativo, social y tecnológico que ha sufrido una

evolución radical desde entonces. Por ello es imprescindible contar con una norma reglamentaria que sustituya a la vigente para dar respuesta al nuevo escenario de ciberseguridad, en el que se han intensificado de forma creciente las ciberamenazas y los ciberincidentes. A la vez, en el contexto de transformación digital en que estamos inmersos, han avanzado las tecnologías de aplicación, ha evolucionado el marco regulador del procedimiento administrativo y del régimen jurídico del sector público, seguridad de las redes y sistemas de información y protección de datos; se ha actualizado el marco estratégico de ciberseguridad y se ha extendido su implantación a la vez que se dispone de una mayor experiencia acumulada sobre su aplicación, de un mejor conocimiento de su situación, así como de un cuerpo de guías de aplicación y de servicios de apoyo.

Todo ello, con el objetivo de que, desde ya, puedan aplicar las medidas de seguridad necesarias y garantizar una correcta seguridad en los datos manejados y los servicios prestados. La generación de sinergias entre los diferentes actores resulta fundamental y, para ello, es preciso que, más pronto que tarde, todos ellos interioricen los principios básicos, requisitos mínimos y medidas de protección regulados por el ENS. La calidad y eficiencia de los resultados dependerá, en gran medida, de que la aprobación de la revisión integral del ENS se efectúe, precisamente, en este momento.

Por estas razones es necesario acometer una actualización del Esquema Nacional de Seguridad que derogue el vigente Real Decreto 3/2010, de 8 de enero y que se apliquen en su tramitación las previsiones del artículo 27.1 b) de la Ley 50/1997, de 27 de noviembre, del Gobierno, pues la intensificación de las ciberamenazas y ciberincidentes que se está produciendo y la imprevisibilidad en cuanto a su número, complejidad técnica y daño potencial que pueden causar al sector público y al privado, justifican la tramitación urgente de dicho proyecto de real decreto para disponer cuanto antes del instrumento normativo adecuado para dar respuesta a estas circunstancias.

2.- OBJETIVOS

La nueva norma busca regular el ENS y establecer los principios básicos y requisitos mínimos necesarios para la protección de la información tratada y servicios prestados por los colectivos involucrados, de acuerdo con el marco jurídico, tecnológico, estratégico y de ciberamenazas actuales, adaptándose a las tendencias en ciberseguridad y desarrollando mecanismos de respuesta y medidas de seguridad óptimas para ello. Adicionalmente, se persigue implementar un ENS de forma más eficiente y eficaz personalizando sus requisitos a las características propias que muestran cada uno de los colectivos involucrados.

Por ello, el proyecto persigue esencialmente:

1º. Alinear el ENS con el nuevo marco normativo de referencia para facilitar la seguridad en la Administración Digital

2º. Introducir la capacidad de ajustar los requisitos del ENS a necesidades específicas, a determinados colectivos de entidades, o a determinados ámbitos

tecnológicos, dando respuesta a las nuevas demandas provenientes de unas organizaciones más maduras y unos ciudadanos más exigentes con sus derechos, para una aplicación más eficaz y eficiente del ENS, sin menoscabo de la protección perseguida y exigible

3º. Actualizar los principios básicos, los requisitos mínimos y las medidas de seguridad para facilitar la respuesta a las nuevas tendencias y necesidades de ciberseguridad, de modo que siga garantizando la protección de los sistemas de información en las entidades de su ámbito de aplicación, reduciendo vulnerabilidades y promoviendo la vigilancia continua.

3.- ADECUACIÓN A LOS PRINCIPIOS DE BUENA REGULACIÓN.

De acuerdo con lo previsto en el artículo 2, apartado 1, párrafo 2º del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria de Análisis de Impacto Normativo, procede analizar la adecuación del real decreto a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre.

El proyecto de Real Decreto es conforme con lo dispuesto en el artículo 129 apartado 1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas con relación a los principios de buena regulación.

Responde a los principios de necesidad y eficacia, en tanto que se dicta en cumplimiento de la propia normativa que regula el ENS hasta la fecha, así como en clara sintonía con las Directivas y Reglamentos europeos en materia de seguridad de la información y protección de datos fundamentalmente, que exigen una progresiva adecuación y desarrollo del ENS conforme a la realidad jurídica, tecnológica y estratégica de cada momento.

También se satisface el principio de proporcionalidad, al no existir otras medidas menos gravosas para los colectivos involucrados destinados a cumplir las obligaciones en materia de seguridad de la información, así como de implementación de las correspondientes medidas de seguridad preventivas y combativas de posibles amenazas de la seguridad de la información.

De la misma manera, se cumple con el principio de seguridad jurídica, resultando el proyecto conforme a la Ley 40/2015, de 1 de octubre, donde se establece el ENS. Por otro lado, la propuesta normativa es respetuosa con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y su normativa de desarrollo, así como con la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, así como la normativa comunitaria y nacional en materia de protección de datos.

Se ha cumplido igualmente con el principio de transparencia, al someterse al trámite de audiencia un texto que define claramente los objetivos de la iniciativa normativa y su justificación.

Por último, resulta conforme con el principio de eficiencia, dado que no se establecen cargas adicionales a las contempladas en el anterior Real Decreto 3/2010, de 8 de enero y que el presente proyecto viene a derogar.

4.- ALTERNATIVAS

Se ha considerado la posibilidad de articular un texto que simplemente modifique el Real Decreto 3/2010, de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, tal y como se hizo por medio del Real Decreto 951/2015, de 23 de octubre.

Sin embargo, como se ha explicado, el Real Decreto 3/2010 ha quedado demasiado obsoleto como para abordar una nueva modificación, siendo necesaria una nueva regulación integral, al amparo de la Ley 40/2015, de 1 de octubre, en sintonía con la nueva regulación europea y nacional, así como con los actuales estándares tecnológicos de seguridad y auditoría, la Estrategia Nacional de Ciberseguridad de 2019 y las nuevas amenazas en el plano cibernético.

5.- INCLUSIÓN EN EL PLAN ANUAL NORMATIVO Y EVALUACIÓN EX POST

Este proyecto se ha propuesto para su inclusión en el Plan Anual Normativo correspondiente a 2021 que deberá ser aprobado por el Consejo de Ministros, de acuerdo con lo previsto en el artículo 25 de la Ley 50/1997 del Gobierno.

No está incluida entre las normas del Plan que serán objeto de una evaluación ex post.

II.- CONTENIDO Y ANÁLISIS JURÍDICO

1.- CONTENIDO

El real decreto consta de 41 artículos distribuidos en nueve capítulos, cuatro disposiciones adicionales, una disposición transitoria, una disposición derogatoria, tres disposiciones finales y cuatro anexos.

El Capítulo I comprende las disposiciones generales que regulan el objeto, ámbito de aplicación, las definiciones y estándares aplicables para las que se remite al anexo IV y las Instrucciones técnicas de seguridad y guías de seguridad. El ámbito de aplicación se remite al ámbito del artículo 2 de la Ley 40/2015, de 1 de octubre y, se añade que también será de aplicación a los sistemas que manejan o tratan información clasificada, sin perjuicio de que pudiera resultar necesario complementar las medidas de seguridad previstas en el presente real decreto con otras específicas para tales sistemas, derivadas de los compromisos internacionales contraídos por España o su pertenencia a organismos o foros internacionales en la materia. Por su parte, en el artículo 4 se prevé que en desarrollo de lo dispuesto en el real decreto, el Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del CCN, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de la Secretaría de Estado Digitalización e Inteligencia Artificial. Asimismo, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (Guías CCN-STIC).

El Capítulo II regula en cada uno de sus diferentes artículos los principios básicos que deben regir el ENS, enumerados en su artículo 5, a saber: seguridad integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua y reevaluación periódica; y diferenciación de responsabilidades.

El Capítulo III se refiere a la Política de Seguridad y los requisitos mínimos para permitir una protección adecuada de la información y los servicios. En los artículos 13 a 27 se definen tales requisitos: organización e implantación del proceso de seguridad; gestión de riesgos, consistente en un proceso de identificación, análisis, evaluación y tratamiento de los mismos; 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; y mejora continua del proceso de seguridad. Seguidamente, en su artículo 28, se indica que para dar cumplimiento a tales requisitos mínimos se deberán adoptar las medidas referidas en el Anexo II apreciando una serie de consideraciones al efecto. No obstante, tales medidas de seguridad podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que son igual o más eficaces y satisfacen los principios básicos y requisitos mínimos indicados previamente. En el artículo 29 se hace un llamamiento a la utilización de infraestructuras y servicios comunes de las Administraciones Públicas en aras de lograr una mayor eficiencia y retroalimentarse de las sinergias de cada colectivo. Por último, el artículo 30 establece la posibilidad de implementar perfiles de cumplimiento específicos, así como esquemas de acreditación de entidades de implementación de configuraciones seguras.

El Capítulo IV versa sobre la auditoría de la seguridad, que se desarrolla íntegramente en el artículo 31, detallando las características del procedimiento de auditoría, así como de los correspondientes informes.

El Capítulo V relativo al Estado de la Seguridad de los sistemas, se desarrolla íntegramente en el artículo 32, destacando el papel de la Comisión Sectorial de Administración Electrónica en este ámbito, así como del CCN y los órganos colegiados competentes en el ámbito de la Administración Digital en la Administración General del Estado.

El Capítulo VI regula la prevención, detección y respuesta a incidentes de seguridad, separando por un lado los aspectos relativos a la capacidad de respuesta (artículo 33) y, por otro, lo relativo a la prestación de los servicios de respuesta a incidentes de seguridad a las entidades del Sector Público (artículo 34).

En el Capítulo VII, que ocupa los artículos 35 a 38, se definen las normas de conformidad. Dichas normas se concretan en cuatro: Administración Digital, ciclo de vida de servicios y sistemas, mecanismos de control y procedimientos de determinación de la conformidad con el ENS.

El Capítulo VIII compuesto por su único artículo 39, establece la obligación de

actualización permanente, de acuerdo con el marco jurídico vigente en cada momento, la evolución de la tecnología y los estándares en materia de seguridad y sistemas, así como de los nuevos vectores de ataque y amenazadas.

Por último, el Capítulo IX desarrolla el procedimiento de categorización de los sistemas de información, definiendo en el artículo 40 las categorías de seguridad y en el artículo 41 las facultades al respecto.

Por su parte, las cuatro disposiciones adicionales regulan, respectivamente, los programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público que desarrollarán el CCN y el Instituto Nacional de Administración Pública; la habilitación a la Comisión Sectorial de Administración Electrónica para proponer el desarrollo de las instrucciones técnicas de seguridad para lograr la mejor implantación del ENS; la tercera prevé la aplicación 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 a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas y, la cuarta, la aplicación de los requisitos del ENS a los sistemas de información que permitan los tratamientos de datos personales de acuerdo con la Ley Orgánica 3/2018, de 5 de diciembre.

La Disposición transitoria única fija un plazo de veinticuatro meses para que los sistemas de información del ámbito de aplicación del presente real decreto, preexistentes a su entrada en vigor alcancen su plena adecuación al ENS.

Por último, el real decreto cuenta con tres disposiciones finales. La primera enumera los títulos competenciales; la segunda habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado y la disposición final tercera ordena la entrada en vigor al día siguiente al de su publicación en el Boletín Oficial del Estado.

El real decreto se complementa con cuatro anexos. El Anexo I regula las categorías de seguridad de los sistemas de información detallando la secuencia de actuaciones para determinar la categoría de seguridad de un sistema. El Anexo II detalla las diferentes medidas de seguridad estructuradas en tres grupos: marco organizativo, constituido por el conjunto de medidas relacionadas con la organización global de la seguridad; marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin; y medidas de protección que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas; el Anexo III trata la Auditoría de la seguridad y el Anexo IV incluye el glosario de términos y definiciones.

2.-PRINCIPALES NOVEDADES

- Se ha revisado y actualizado la redacción del ámbito de aplicación (art 2 y DA 3ª) con una doble finalidad:

1º. En primer lugar, para clarificarlo y que ambos sectores, público y privado (proveedores o suministradores tecnológicos de las entidades del sector público), sean conscientes de lo que les es exigible, en beneficio último de la ciberseguridad pública y de los derechos de los ciudadanos.

2º. En segundo lugar, para extender su aplicación a los sistemas que manejan o tratan información clasificada, sin perjuicio de que pudiera resultar necesario complementar las medidas de seguridad previstas en el ENS con otras específicas para tales sistemas.

- Se ha realizado la clarificación, precisión, homogeneización, simplificación, o actualización de distintos aspectos del texto, así como la eliminación de aspectos no necesarios o excesivos (un capítulo de 'Comunicaciones electrónicas', con tres artículos, ya superado por las leyes 39/2015 y 40/2015 y sus desarrollo reglamentario).

- A través del nuevo artículo 30 se han incorporado los perfiles de cumplimiento específicos que introducen la capacidad de ajustar los requisitos del ENS a necesidades específicas, mediante la definición de un conjunto de medidas de seguridad que resulten de aplicación a una entidad o sector de actividad concreta, y para una determinada categoría de seguridad (por ej. para Entidades Locales), lo que permite alcanzar una adaptación al ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

- Se han revisado los principios básicos, los requisitos mínimos y las medidas de seguridad:

  1º. El principio antes denominado 'prevención, reacción y recuperación' pasa a denominarse 'prevención, detección y respuesta'.

  2º. Se introduce el principio 'vigilancia continua' para permitir la detección de actividades o comportamientos anómalos y su oportuna respuesta e impulsar la evaluación permanente del estado de la seguridad de los activos, para detectar vulnerabilidades e identificar deficiencia de configuración.

  3º. Se clarifica la redacción del principio 'responsabilidades diferenciadas' para precisar los aspectos relativos al responsable de la seguridad y al responsable del sistema.

- En el capítulo de los requisitos mínimos de seguridad se refuerzan la importancia de la política de seguridad y el requisito mínimo 'seguridad por defecto' que pasa a denominarse 'mínimo privilegio', con diversas mejoras en otros requisitos mínimos.

- Se ha perfeccionado el capítulo de 'Prevención, detección y respuesta a incidentes de seguridad' en el que se detallan de forma más pormenorizada:

  1º. Las condiciones relativas a la notificación de incidentes de seguridad por parte de las entidades del sector público al CCN-CERT y a las correspondientes actuaciones respuesta por parte de la Secretaría General de

Administración Digital y del CCN-CERT.

2º. Las condiciones de la notificación de incidentes de seguridad al INCIBE-CERT por parte de las entidades del sector privado que preste servicios a las entidades públicas; todo ello en el marco de lo previsto en el Real Decreto 43/2021, de 26 de enero.

- En el anexo II de **medidas de seguridad**, se han actualizado las medidas de seguridad en el marco operacional y en las medidas de protección. Como resultado de estas modificaciones de detalle, algunas medidas han ampliado considerablemente su nivel de exigencia para determinadas categorías, y otras lo han aumentado levemente. Por el contrario, otras medidas han simplificado su nivel de exigencia, y algunas medidas han sido eliminadas y/o englobadas dentro de otras. Por último, se han creado nuevas medidas que no existían. El resto, sólo han sufrido cambios de redacción, o se han concretado.

- Entre las nuevas medidas, se han incluido las relativas a servicios en la nube, interconexión de sistemas, protección de la cadena de suministro (alude a los proveedores o suministradores tecnológicos de las entidades del sector público), medios alternativos, vigilancia y otros dispositivos conectados a la red.

- Se han reforzado medidas relativas a la identificación, la configuración de seguridad, la gestión de la configuración de seguridad, la protección frente al código dañino, el registro de actividad, la gestión de capacidad, la detección de intrusión, el sistema de métricas y la aceptación y puesta en servicio.

- Otras medidas con un refuerzo más ligero incluyen los requisitos de acceso, la gestión de cambios, la gestión de incidentes, mantenimiento y actualizaciones de seguridad, protección de la confidencialidad y copias de seguridad.

- Se han simplificado algunas medidas como segregación de tareas, sellos de tiempo, calificación de la información, protección de dispositivos portátiles, protección frente a denegación de servicio o perímetro seguro.

- Se han eliminado medidas tales como las relativas a personal alternativo, medios alternativos, protección de los registros de actividad por estar cubiertas por otras medidas.

- Finalmente, como ayuda a su implantación y revisión, por una parte, se han codificado los requisitos de las medidas de protección; y, por otra parte, para indicar una mayor exigencia se emplean los refuerzos de seguridad, también codificados, que se suman a los requisitos base de la medida, pero que no siempre son incrementales entre sí; de forma que, en ciertos casos, se puede elegir entre aplicar un refuerzo u otro.

3. ANÁLISIS JURÍDICO

2.1 Derogación normativa

Mediante este proyecto de real decreto se derogan:

1º. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

2º. Las disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto.

2.2 Engarce con el derecho nacional

Al amparo de lo establecido en el artículo 149.1.18 de la Constitución, que atribuye al Estado la competencia para regular el procedimiento administrativo común y el régimen jurídico del sector público y en el artículo 97 de la Constitución que atribuye al Gobierno el ejercicio de la potestad reglamentaria, se trata de un proyecto de real decreto que viene a desarrollar la Ley 40/2015, de 1 de octubre (en ejercicio de la habilitación normativa contenida en su disposición final decimoquinta) en lo referido a lo previsto en su artículo 156.2 que señala que "*El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".*

El proyecto de real decreto se relaciona asimismo con el Reglamento general de protección de datos (Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE) y con las siguientes normas nacionales con rango de ley y de real decreto expuestas en orden cronológico:

a) Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
b) Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
c) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Púbicas.
d) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que responde al mandato de transposición de 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 en las redes y sistemas de información en la Unión.
e) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
f) 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.
g) 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.

El proyecto, por tanto, respeta la normativa comunitaria, los límites constitucionales y legales de la potestad reglamentaria y es coherente con el resto del ordenamiento jurídico.

2.3 Contribución del proyecto al engarce con iniciativas internacionales y a reforzar la posición de España en el ámbito de la administración digital a través del robustecimiento del Esquema Nacional de Seguridad.

Fortalecer la ciberseguridad demanda robustecer el marco normativo, a lo que responde la finalidad de este proyecto de real decreto, y disponer de recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al esfuerzo de defensa requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa.

Este conjunto de acciones tomadas en abstracto son indicadores del compromiso de los estados con la ciberseguridad, materia que a nivel global y en términos comparativos se analiza a través del **Índice de Ciberseguridad Global (Global Cibersecurity Index - GCI)** una iniciativa de la Unión Internacional de Telecomunicaciones (UIT).

El CGI es un índice compuesto para medir el compromiso de los 194 Estados Miembros de la UIT con la ciberseguridad. Según la edición de 2018 del GCI, publicada en abril de 2019, España figura **en séptimo lugar** en la lista de los diez países que muestran un mayor grado de compromiso con la ciberseguridad. En el análisis por áreas geográficas, España figura en quinto lugar en el ámbito europeo, tras Reino Unido, Francia, Lituania y Estonia. Según la perspectiva que pone en relación el índice de desarrollo TIC, conocido como IDI, y el GCI, España también muestra un buen posicionamiento.

Además de este índice específico, que muestra la destacada posición relativa de nuestro país respecto de la ciberseguridad, hay que tener en cuenta también que toda la política de seguridad desarrollada hasta la fecha es uno de los elementos clave que ha permitido y garantizado el importante grado de avance de España en cuanto a la evolución digital, el uso de los servicios públicos digitales y el desarrollo, en conjunto, de la administración electrónica, de ahí la importancia de robustecer nuestro ENS para que siga ejerciendo ese efecto positivo.

Tal como se ha señalado anteriormente, el Plan Digitalización de las Administraciones Públicas, instrumento para la ejecución de los fondos del Componente 11 «Modernización de las Administraciones Públicas» del Plan de Recuperación, Transformación y Resiliencia, así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025, contempla la actualización del ENS entre las reformas normativas a abordar con el fin de evolucionar la política de seguridad de las Administraciones Públicas españolas (que alcanza a todas las entidades del Sector Público), tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información.

Este avance queda patente en informes e indicadores como los siguientes:

A) En el ámbito de la Unión Europea:
- El Índice de Economía y Sociedad Digital (DESI), publicado el 11 de junio de 2020 por la Comisión Europea, **constata el avance de la evolución digital en España y sitúa a nuestro país por encima de la media de la Unión Europea** y muy por delante de

países de similar tamaño y complejidad administrativa, como Alemania, Francia e Italia.

- **España ocupa la posición 11** en el índice DESI. Obtiene 57.5 puntos, por encima de la media de la Unión Europea (52.6). Con respecto al año anterior, España mejora su puntuación global (53.6 puntos en 2019).

- España **mejora en la mayoría de los indicadores** en las cinco dimensiones que mide el informe: conectividad, capital humano, uso de internet, integración de la tecnología digital y servicios públicos digitales. **La única dimensión del informe donde España se sitúa por debajo de la media europea es en capital humano.**

- **España obtiene 87.3** puntos sobre 100 en el indicador de servicios públicos digitales, lo que le sitúa en **segunda posición**, por detrás de Estonia (89.3 puntos) y por delante de Dinamarca (87.1) y Finlandia (87), mejorando la cuarta posición del año anterior.

- La dimensión "Servicios Públicos Digital" se compone este año de cinco indicadores: "usuarios de administración electrónica", "formularios pre-cumplimentados", "compleción de servicios en línea", "servicios públicos digitales en empresas" y "datos abiertos". España se sitúa en todos los indicadores muy por encima de la media de la Unión Europea. La posición de España en los indicadores que componen la dimensión de servicios públicos digitales es:

  - "Usuarios de administración electrónica": 9ª posición
  - "Formularios pre-cumplimentados" 8ª posición
  - "Compleción de servicios en línea" 8ª posición
  - "Servicios públicos digitales en empresas" 9ª posición
  - "Datos abiertos": 2ª posición

- La Comisión Europea destaca la posición española en la dimensión de servicios públicos digitales y la mejora con respecto al año anterior. Además, destaca: "*Los indicadores muestran un nivel alto de interacción en línea entre las autoridades públicas, los ciudadanos y las empresas. España obtiene muy buenos resultados en el indicador de datos abiertos, y ocupa el segundo puesto con el 90 % de la puntuación máxima. El 82 % de los usuarios de internet españoles participa activamente en los servicios de administración electrónica, 6 puntos porcentuales más que el año anterior*".

- Por otra parte, según el "**eGovernment Benchmark 2018"** publicado por la Comisión Europea, España se ubica con un nivel medio-alto de penetración y digitalización, formando parte del escenario Fruitful eGov, que incluye a los mejores países de su clase por encima del promedio europeo.España figura en el grupo de países "Top-performing" en varias de las facetas analizadas.

B) En el resto del contexto Internacional

- La **Organización de las Naciones Unidas (ONU)** mide el grado de desarrollo de la Administración Electrónica de sus 193 países miembros mediante el Índice de Administración Electrónica (EGDI [eGovernment Development Index]) que es hasta la fecha el único indicador en la materia con alcance global. El objetivo del EGDI es evaluar "*la capacidad y voluntad de los países de utilizar la Administración Electrónica para un desarrollo basado en las TIC*".

  En la Encuesta de Gobierno Electrónico 2020 España figura en el grupo de países con muy alto rendimiento en el Índice de Desarrollo de la Administración Electrónica (EGDI), al obtener una puntuación en el EGDI superior a 0.75. España figura, en la lista de países con un alto rendimiento de acuerdo con el índice de desarrollo de la administración electrónica (E-Government Development Index, EGDI). Liderando este indicador se sitúan en esta edición de 2020: Dinamarca, Corea, Estonia, Finlandia y Australia. Además, España mantiene el puesto número 17 igual que en la edición de 2018.

- En el marco de la **OCDE,** en octubre de 2020 se ha publicado por primera vez, el **Índice de Gobierno Digital** que analiza la transición del gobierno electrónico al gobierno digital. Entendiendo este proceso, como el paso de la mera digitalización de procedimientos administrativos en una administración online, a unos servicios públicos completamente digitales, diseñados pensando en el usuario, más sencillos, accesibles, proactivos y que realmente satisfagan las necesidades de los ciudadanos.

  En la primera edición de este índice, con datos de 2019, España ha obtenido la **séptima posición en el ranking global**, sobresaliendo su cuarta posición en tres de las seis dimensiones analizadas: digital por diseño, Sector Público impulsado por datos y proactividad.

2.4 Vigencia de la norma y entrada en vigor

De acuerdo con lo previsto en la disposición final tercera, este real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado», lo que es coherente con el carácter urgente de la tramitación acordado por el Consejo de Ministros el pasado 25 de mayo.

La norma prevé que el ENS sea desarrollado por medio de Instrucciones técnicas de seguridad de obligado cumplimiento que se aprobarán mediante Orden Ministerial o Resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Asimismo, el artículo 39 establece la exigencia de que el ENS se encuentre permanentemente actualizado conforme a la nueva regulación, al estado de la tecnología y de las infraestructuras, así como los diferentes estándares en seguridad y tipología de amenazas. Por consiguiente, es previsible que, al igual que ocurrió con el Real Decreto 3/2010, de 8 de enero, la presente norma sea modificada en un futuro.

2.5 Rango normativo

La disposición final decimoquinta de la Ley 40/2015, de 1 de octubre, faculta al Consejo de Ministros para en el ámbito de sus competencias dictar cuentas disposiciones reglamentarias sean necesarias para el desarrollo de las previsiones de la Ley.

El artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno, prevé que las decisiones que aprueben normas reglamentarias de la competencia del Consejo de Ministros adoptarán la forma de reales decretos.

III.- ADECUACIÓN DE LA NORMA AL ORDEN DE DISTRIBUCIÓN DE COMPETENCIAS

Este real decreto se dicta al amparo de lo dispuesto en el **artículo 149.1.18.ª de la Constitución**, que atribuye al Estado la competencia exclusiva en materia de procedimiento administrativo común y para dictar las bases del régimen jurídico de las Administraciones Públicas.

Asimismo el proyecto se aprueba en virtud de la competencia exclusiva del Estado sobre las telecomunicaciones y sobre la seguridad pública de acuerdo con lo previsto en los **artículos 149.1.21ª y 149.1.29.ª de la Constitución**.

A estos efectos, el Tribunal Constitucional ha abordado el concepto de ciberseguridad en la STC 142/2018, cuyo FJ 4 señala que *"La ciberseguridad, como sinónimo de la seguridad en la red, es una actividad que se integra en la seguridad pública, así como en las telecomunicaciones".*

Por su parte, el FJ 5 añade que "*la ciberseguridad no es un concepto o materia reconducible a un único título competencial*. ***Puede, como allí se recalca, identificarse con la seguridad nacional o con la seguridad pública*** *cuando se trata de la protección ordinaria de las redes y las infraestructuras de telecomunicaciones.* ***Pero también puede proyectarse sobre otros planos, como es el caso de la administración electrónica,*** *que abarca la organización de medios y previsión de* ***medidas de protección de la administración y, por extensión, la protección de los derechos de los ciudadanos cuando se relacionan con la administración por medios electrónicos*****".**
A ello añade el FJ 6 que *"****la seguridad pública es una competencia exclusiva del Estado ex artículo 149.1.29 CE*** *y solamente se encuentra limitada por las competencias que las Comunidades Autónomas hayan asumido respecto a la creación de su propia policía (por todas, STC 148/2000, de 1 de junio, FJ 5)",* y que *"Como recuerda la STC 8/2016, de 21 de enero, FJ 3:* ***"Desde una última perspectiva, más global, se integra también en la materia de telecomunicaciones y de régimen general de comunicaciones*** *(y corresponde por tanto al Estado la competencia exclusiva conforme al* ***149.1.21 CE****) la conformación, regulación o configuración del propio sector de telecomunicaciones (comunicaciones electrónicas) atendiendo a la convergencia tecnológica (y de servicios) y al marco regulador de las comunicaciones electrónicas de la Unión Europea para asegurar una regulación homogénea en todo el territorio español. Esta homogeneidad resulta necesaria, no solo para el desarrollo e innovación del sector, sino también para la garantía de los derechos de los ciudadanos en el marco de la sociedad de*

la información (o sociedad del conocimiento), si se tiene en cuenta que el desarrollo de las comunicaciones y de las nuevas tecnologías de la información constituye un factor esencial para lograr la cohesión social, económica y territorial necesarias para evitar, o al menos disminuir, la llamada fractura digital".
A este respecto, 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), ***define la seguridad de las redes y 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".*

El proyecto es plenamente respetuoso con la doctrina del Tribunal Constitucional en la materia.

IV.- DESCRIPCIÓN DE LA TRAMITACIÓN

4.1. Consideración previa.

En virtud de lo dispuesto en el párrafo segundo del apartado segundo del Acuerdo de Consejo de Ministros sobre actuaciones urgentes en materia de ciberseguridad, de 25 de mayo de 2021:

> *"Por las razones expuestas, el Gobierno* ***acuerda que se someta a su aprobación un proyecto de real decreto que derogue el vigente Real Decreto 3/2010, de 8 de enero y actualice el Esquema Nacional de Seguridad y que se apliquen en su tramitación las previsiones del artículo 27.1 b) de la Ley 50/1997, de 27 de noviembre, del Gobierno****, pues la intensificación de las ciberamenazas y ciberincidentes que se está produciendo y la imprevisibilidad en cuanto a su número, complejidad técnica y daño potencial que pueden causar al sector público y al privado,* ***justifican que se acuerde la tramitación urgente de dicho proyecto de real decreto*** *para disponer cuanto antes del instrumento normativo adecuado para dar respuesta a estas circunstancias."*

El proyecto de real decreto ha sido elaborado por un equipo interministerial (Grupo de Trabajo) formado por el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Defensa (a través del Centro Criptológico Nacional, CCN del Centro Nacional de Inteligencia, CNI).

4.2. Trámites pendientes.

- De acuerdo con lo previsto en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre y el 133.2 de la Ley 39/2015, de 1 de octubre, el Texto del proyecto y esta MAIN se someterán al trámite de audiencia e información pública en el portal de internet del Ministerio de Asuntos Económicos y Transformación Digital.

- De acuerdo con lo previsto en el artículo 26.5 de la Ley 50/1997, de 27 de noviembre, el Texto del proyecto y esta Memoria del Análisis de Impacto Normativo se remitirá a informe de los diferentes ministerios.

- De acuerdo con lo previsto en el artículo 5.3 a) del Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio, el proyecto se someterá a informe de la misma.

- De acuerdo con lo previsto en el artículo 26.5, párrafo sexto, de la Ley 50/1997, de 27 de noviembre, conforme al cual "*será necesario informe previo del Ministerio de Hacienda y Administraciones Públicas* [Ministerio de Política Territorial y Función Pública] *cuando la norma pudiera afectar a la distribución de las competencias entre el Estado y las Comunidades Autónomas*"), se someterá a informe de la Secretaría General de Coordinación Territorial del Ministerio de Política Territorial y Función Pública.

- El Texto del proyecto y esta MAIN someterán a consulta a las Comunidades Autónomas y Entidades Locales(a través de la Federación Española de Municipios y Provincias (FEMP) por medio de la Comisión Sectorial de Administración Electrónica (CSAE).

- De acuerdo con lo previsto en el artículo 26.9 de la Ley 50/1997, de 27 de noviembre**,** el proyecto se someterá a informe de la Oficina de Coordinación y Calidad Normativa del Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática.

- De acuerdo con lo previsto en el artículo 26.5 de la Ley 50/1997, de 27 de noviembre, el proyecto se someterá a informe de la Secretaría General Técnica del Ministerio de Política Territorial y Función Pública.

- De acuerdo con lo previsto en el artículo 26.5, párrafo cuarto de la Ley 50/1997, de 27 de noviembre**,** el proyecto se someterá a informe de la Secretaría General Técnica del MAETD.

- Por último, el proyecto y su MAIN en su versión definitiva una vez evacuados los trámites anteriores será sometido a Dictamen del Consejo de Estado, en aplicación del artículo 22.3 de la Ley Orgánica 3/1980, de 22 de abril, del Consejo de Estado.

V.- ANÁLISIS DE IMPACTOS

1. Impacto económico

A) Impacto económico general

1. *Efectos en los precios de los servicios.*

   Las medidas tendrán un impacto neutral en los precios de servicios.

El coste, para los colectivos obligados a cumplir y adoptar las medidas de seguridad, así como los principios básicos y requisitos mínimos establecidos por la norma, debería ser marginal en el conjunto de costes del desarrollo de su actividad, ya que las obligaciones recaen sobre agentes que, por lo general, ya se encontraban en el ámbito de aplicación del ENS con anterioridad de la presente norma, por lo que sus esfuerzos se centrarán en un ejercicio de adaptación, en ocasiones ya alcanzado. Asimismo, el esfuerzo económico dedicado a medidas de seguridad debe considerarse como una inversión, puesto que genera rendimientos positivos como resultado de la reducción de las consecuencias de los incidentes de seguridad, y genera un impacto muy positivo a nivel reputacional de cada sujeto (agente) obligado y del Sector Público en general, así como los sectores del tejido empresarial que se vean afectados por la norma.

2. *Efectos en la productividad*

   Las medidas tendrán un efecto positivo sobre la productividad.

   El incremento y racionalización de medidas de seguridad de los datos e información que circulan por las diferentes infraestructuras y que son empleadas en la prestación de los servicios por parte de las empresas del Sector Privado, así como por las propias Administraciones Públicas y demás entidades del Sector Público, junto con la mayor eficacia en la gestión de los riesgos de incidentes de seguridad de la información, reducirá el impacto perjudicial de estos incidentes en los servicios, redundando en una mayor productividad en su prestación y garantizará, además, el derecho de los ciudadanos y empresas a preservar sus datos y operar con una mayor confianza en el mercado y hacia el Sector Público.

3. *Efectos en el empleo*

   Las medidas tendrán un efecto neutral sobre el empleo.

   No obstante, se verán acentuados perfiles en el ámbito de la ciberseguridad y auditoría respecto a la seguridad de sistemas, así como en materia de protección de datos.

4. *Efectos sobre la innovación*

   Las medidas tendrán un efecto positivo sobre la innovación.

   La incorporación de las tecnologías de la información y las comunicaciones a los procesos productivos y de provisión de servicios, en un entorno de digitalización progresiva, está siendo uno de los principales mecanismos para la innovación en la totalidad de sectores de actividad económica y social. Sin embargo, las incertidumbres y amenazas ciertas que constituyen los incidentes de seguridad de la información, que afecta a la información y datos que circulan y se generan durante tales procesos, suponen un freno para la incorporación de estas tecnologías.

   Por tanto, el efecto positivo que tendrán las medidas previstas en el proyecto en la reducción del impacto de estos incidentes, estableciendo las medidas de seguridad en él reguladas, tendrá, como consecuencia indirecta, una reducción en este efecto freno y un efecto positivo en la innovación como consecuencia de la incorporación más intensiva de las tecnologías de la información, las comunicaciones y la ciberseguridad.

5. *Efectos sobre los consumidores*

   Las medidas tendrán un efecto prácticamente neutro sobre los consumidores, al menos directamente.

   No obstante, los incrementos en la confianza en las infraestructuras digitales, así como de la productividad e innovación asociada en la prestación de los servicios contribuirán a dinamizar los mercados de los diferentes sectores considerados, con el consiguiente aumento de la demanda de dichos servicios por parte de los consumidores (así como de las PyMEs que, en muchos casos, tienen necesidades similares a las de los consumidores).

6. *Efectos en relación con la economía europea y otras economías*

   Las medidas tendrán un efecto positivo en relación con la economía.

   El ciberespacio no conoce de fronteras, por lo que, en la medida en que las infraestructuras y colectivos afectados por el ENS cumplan los más altos estándares de seguridad garantizando la máxima protección de la información, sus efectos se verán reflejados inmediatamente en la economía europea, pues los actores de la Unión podrán beneficiarse de las ventajas proporcionadas por un sistemas e infraestructuras sólido, asumiendo las prescripciones técnicas reguladas por el ENS y sus normas de desarrollo o colaborando los agentes públicos y privados europeos con las propias instituciones y colectivos involucrados, retroalimentado así los efectos positivos en la economía.

7. *Efectos sobre las PyMEs*

   El impacto es reducido en este sentido, pues directamente, solo aquellas PyMES que colaboren con los colectivos involucrados en el ámbito de aplicación del ENS se verán obligadas a adoptar un esfuerzo siguiendo las directrices establecidas por dicha norma. Si bien, es cierto, que al amparo del ENS o no, todas las empresas se ven afectas ineludiblemente a los procesos de transformación digital que estamos viviendo por lo que ya sea en materia de protección de datos, en tramitación digital de procedimientos, o en cualquier otro ámbito relacionado, las empresas, sea cual sea su dimensión, deberán adoptar las correspondientes medidas al efecto. En este sentido, el ENS se configura, en todo caso, como una perfecta guía a la que acogerse, lo que permitirá a las PyMES ser más competitiva en el mercado, pudiendo acceder a más infraestructuras y, por ende, a más oportunidades.

B) Efectos en la competencia y la unidad de mercado

El proyecto tiene un efecto neutral en la competencia en los diferentes mercados afectados, por lo que no cabe resaltar una especial incidencia en los mismos, y se adecúa a lo dispuesto en la Ley 20/2013, de 9 de diciembre, de Garantía de la Unidad de Mercado.

Por otra parte, las obligaciones para los colectivos afectados se definen en la norma de acuerdo con el principio de proporcionalidad, afectando por igual a todos ellos y, previendo, incluso, perfiles de cumplimientos específicos, adaptados a sus dimensiones y características.

2. Impacto presupuestario.

- Desde el punto de vista de los ingresos, las medidas adoptadas no supondrán ingresos adicionales directos para el Estado.
- Desde el punto de vista del gasto las medidas adoptadas no supondrán gastos adicionales. Si bien, las relativas a la implementación de las medidas de seguridad y demás aspectos regulados por la norma serán atendidos conforme a las debidas partidas presupuestarias al efecto.
- Por último, con relación a los gastos en medios o servicios de la Administración digital, las medidas adoptadas no supondrán gastos adicionales en las mismas.
- La aprobación del real decreto se verá complementada por la inversión destinada a constituir el Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos, que servirá de referencia para las demás Administraciones Públicas y contribuirá a mejorar en cumplimiento del ENS de las entidades en su alcance de servicio.

3. Análisis de las cargas administrativas.

El artículo 26.3.e de la Ley 50/1997, de 27 de noviembre, del Gobierno establece que en las Memoria del Análisis de Impacto Normativo se identificarán las cargas administrativas que conlleva la propuesta.

El proyecto no incrementa las cargas administrativas en la medida que los aspectos novedosos en cuanto a obligaciones específicas se refieren han sido incorporados previamente por otra normativa (seguridad de redes, protección de datos), por lo que, en principio serán las Administraciones Públicas y demás entidades del Sector Público y colectivos afectados quienes deban adecuar sus procedimientos y medidas de seguridad para proteger la información de acuerdo con el ENS.

4. Impacto de los medios y servicios digitales que conlleva la norma.

De acuerdo con lo previsto en la letra g) del apartado 1 del artículo 2 del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo, en la redacción dada por el 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, la MAIN incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención, entre otros, al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma.

En este sentido, las medidas contempladas en este real decreto responden a lo previsto en los principios generales regulados en el artículo 3 de la Ley 40/2015, según el cual las administraciones públicas se relacionarán *"…a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones…, garantizarán la protección de los datos de carácter personal,…*" y a lo previsto en la Ley 39/2015, de 1 de octubre, en cuyo artículo 13 se reconoce el derecho de las personas "*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."

Teniendo en cuenta el impulso en la adopción de procesos y medios digitales, para la tramitación electrónica completa, la relación de las administraciones entre sí por medios electrónicos y en la relación digital con la ciudadanía, las medidas propuestas en este real decreto mejorarán la protección de la información manejada y de los servicios prestados, contribuyendo a una mayor confianza y continuidad de los servicios, particularmente en relación con el ejercicio de derechos y el cumplimiento de obligaciones, gracias a una mejor protección frente a ciberamenazas y ciberataques orientados a la información, con sustracción de datos (con o sin revelación posterior), alteración (incluyendo el fraude por inserción de documentos falsos), destrucción (incluyendo el cifrado irrecuperable de datos y documentos), o quiebra de la disponibilidad que afectaría al acceso a la información; de ahí que la transformación digital haya de ir acompañada de medidas organizativas y técnicas de seguridad proporcionadas a los riesgos.

5. Impacto por razón de género.

Analizada la propuesta desde la perspectiva de género, de conformidad con lo dispuesto en los artículos 19 de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva entre mujeres y hombres, y 26.3.f) de la Ley 50/1997, de 27 de noviembre, del Gobierno, se concluye que el impacto por razón de género del proyecto de real decreto es nulo.

6. Impacto en la infancia y en la adolescencia.

De conformidad con lo dispuesto en el artículo 22 quinquies de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, en la redacción dada por la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, no se considera que el proyecto de real decreto tenga un impacto específico en la infancia y en la adolescencia.

7. Impacto en la familia.

De acuerdo con lo previsto en la disposición adicional décima de la Ley 40/2003, de 18 de noviembre, de protección a las familias numerosas, introducida por la disposición final quinta de la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, se ha concluido la inexistencia de impactos significativos en este ámbito.

8. Impacto en materia de medioambiente.

Respecto al impacto medioambiental, aunque el proyecto no tienen un efectos directo sí cabe señalar que el robustecimiento del ENS fomenta necesaria y directamente el empleo de la tecnología y los canales electrónicos de comunicación y relación, por lo que puede tener un impacto positivo en la medida en que se reducen desplazamientos superfluos, se reduce el consumo de papel y ayuda a reducir la generación de residuos en general.

9. Impacto por razón de materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

En el mismo sentido descrito para el impacto medioambiental, con relación a la igualdad de oportunidades, la no discriminación y la accesibilidad universal de las personas con discapacidad, el proyecto no tiene un impacto directo, pero en la medida en que el ENS fomenta necesaria y directamente el empleo de la tecnología y los canales electrónicos de comunicación y relación tiene un efecto positivo indirecto:

- Por cuanto los medios electrónicos proporcionan, precisamente a las personas con más limitaciones, una vía alternativa de comunicación con la Administración.

- Porque al ser un presupuesto para el incremento de los servicios públicos por medios electrónicos conlleva un refuerzo de derechos individuales, como el derecho a un acceso rápido, eficaz y eficiente a los servicios web públicos a través de los medios electrónicos, derecho a disponer de unos servicios web de calidad que sean útiles y satisfagan sus necesidades, derecho a recibir una información transparente y veraz, y al mismo tiempo, derecho a preservar la privacidad de los ciudadanos y sus datos personales.