INFORME SOBRE LA PROPUESTA DE PROYECTO DE REAL DECRETO POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD

Expediente nº: IPN/CNMC/018/21

PLENO

Presidenta
Dª. Cani Fernández Vicién

Vicepresidente
D. Ángel Torres Torres

Consejeros
Dª. María Ortiz Aguilar
D. Mariano Bacigalupo Saggese
Dª. María Pilar Canedo Arrillaga
D. Bernardo Lorenzo Almendros
D. Xavier Ormaetxea Garai
Dª. Pilar Sánchez Núñez
D. Carlos Aguilar Paredes
D. Josep Maria Salas Prat

Secretario del Consejo
D. Joaquim Hortalà i Vallvé

En Madrid, a 22 de julio de 2021

Vista la solicitud de informe de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital sobre la propuesta de Proyecto de Real Decreto (PRD) por el que se regula el Esquema Nacional de Seguridad, que tuvo entrada en la Comisión Nacional de los Mercados y la Competencia (CNMC) el 15 de junio de 2021, en ejercicio de las competencias que le atribuye el artículo 5.2 de la Ley 3/2013, de 4 de junio, de creación de la CNMC, el Pleno acuerda emitir el presente informe.

1. ANTECEDENTES

El Esquema Nacional de Seguridad (en adelante ENS), regulado por el Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y está

constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

El artículo 42 del Real Decreto 3/2020, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica establece el principio de actualización permanente del Esquema 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"*. 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.

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 tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información.

El preámbulo del PRD indica la necesidad de actualizar el ENS atendiendo a tres grandes cuestiones:

En primer lugar, se persigue alinear el ENS con el marco normativo y el contexto estratégico existente para facilitar la seguridad en la Administración Digital. Se trata de reflejar con claridad el ámbito de aplicación del ENS en beneficio de la ciberseguridad y de los derechos de los ciudadanos, actualizar referencias al marco legal actualizado y revisar la formulación de ciertas cuestiones a la luz del mismo, alinearlo con el contexto establecido en la Estrategia Nacional de Ciberseguridad 2019 y mejorar diversos aspectos para simplificar, precisar o armonizar, eliminar aspectos excesivos, o añadir aquellos que se identifican como necesarios.

En segundo lugar, se persigue introducir la capacidad de ajustar los requisitos del ENS para adaptarse a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y servicios, que aconseja la inclusión en el ENS del concepto de "perfil de cumplimiento específico" que, aprobado por el Centro Criptológico Nacional (CCN), permitan alcanzar una adaptación al ENS más eficaz y eficiente,

racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

En tercer lugar, se persigue actualizar el ENS para facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua, mediante la revisión, a la luz del estado del arte, de los principios básicos, los requisitos mínimos y las medidas de seguridad.

2. CONTENIDO DE LA PROPUESTA

El PRD consta de un preámbulo, 41 artículos estructurados 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 y las Instrucciones técnicas de seguridad y guías de seguridad.

- El **Capítulo II** regula en cada uno de sus diferentes artículos los principios básicos que deben regir el ENS: 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.

- El **Capítulo IV** trata sobre la auditoría de la seguridad detallando las características del procedimiento de auditoría, así como de los correspondientes informes.

- El **Capítulo V** versa sobre el Estado de la Seguridad de los sistemas 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 AGE.

- 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 y, por otro, lo relativo a la prestación de los servicios de respuesta a incidentes de seguridad a las entidades del Sector Público.

- En el **Capítulo VII** 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** 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 amenazas.

- Por último, el **Capítulo IX** desarrolla el procedimiento de categorización de los sistemas de información, definiendo las categorías de seguridad y las facultades al respecto.

Por su parte, las **cuatro disposiciones adicionales** regulan (i) los programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público que desarrollarán el CCN y el INAP; (ii) 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; (iii) 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 (iv) 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.

Además, 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 tercera ordena la entrada en vigor al día siguiente al de su publicación en el BOE.

Por último, 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.

3. CONSIDERACIONES

Se valora positivamente el objetivo del PRD de 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. Asimismo, se determinan los principios y requisitos mínimos de seguridad que deberán adoptarse por parte de las entidades del Sector Público (y por aquellas entidades del sector privado que colaboran con aquellas) atendiendo al nuevo marco legal impuesto por las normativas europeas y nacionales en materia de seguridad de la información.

En la actualidad, tanto para las Administraciones Públicas como para las entidades privadas (en su doble vertiente de operadores independientes o de contratistas de la propia Administración) la información es un activo esencial que debe ser preservado para evitar todo tipo de abusos y/o ataques. En este sentido, se resalta la importancia de la seguridad como razón imperiosa de interés general que, dentro del respeto a los principios de buena regulación[1], podría legitimar la adopción de medidas regulatorias de esta naturaleza.

En líneas generales, el texto normativo analizado no presenta restricciones a la competencia reseñables por su potencial falta de justificación desde la óptica de tales principios. En cualquier caso, se realizan dos comentarios respecto a la cualificación del personal para prestar ciertos servicios y a la adquisición de productos y servicios de seguridad, a modo de recordatorio de las posiciones de esta Comisión al respecto de futuros desarrollos regulatorios o decisorios sobre los mismos.

Por una parte, en relación con la profesionalidad estipulada en el artículo 16. El apartado primero de este artículo establece que la *"seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida"*. Asimismo, su apartado segundo indica que las entidades exigirán, *"de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados"*. Finalmente, el apartado tercero señala que

[1] El art. 129 de la Ley 39/2015 recoge los principios de necesidad y proporcionalidad, entre otros, en el ejercicio de la iniciativa normativa. Así mismo, el art. 5 de la LGUM, exige la motivación desde la óptica de los principios de necesidad, proporcionalidad y mínima distorsión de la competencia..

las organizaciones *"determinarán el diseño curricular y experiencia necesaria del personal para el desarrollo de su puesto trabajo".*

En relación con ello, se recuerda que la CNMC ha recomendado en repetidas ocasiones no circunscribir el ejercicio de actividades a disponer de una titulación específica, siempre que sea posible. La aptitud para desarrollar las funciones requeridas podría demostrarse a través de la acreditación de competencias específicas relativas, en su caso, a diferentes titulaciones o de la experiencia determinada en el ejercicio de unas funciones concretas. En definitiva, cuando se defina el personal que se considera cualificado, resulta preferible el criterio de la capacitación técnica de los profesionales frente al de una concreta titulación.

Por otra, en lo referente a la adquisición de productos de seguridad y contratación de servicios de seguridad. El apartado primero del artículo 19 señala que "*en la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación del presente real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición."* Además, se indica que *"Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16"*.

Por otro lado, el artículo 30.2 señala que: "Análogamente, para posibilitar la adecuada implantación y configuración de soluciones o plataformas suministradas por terceros, que vayan a ser usadas por las entidades del ámbito de aplicación del presente real decreto, se podrán implementar esquemas de acreditación de entidades y validación de personas, que garanticen la seguridad de dichas soluciones o plataformas y la conformidad con lo dispuesto en el presente real decreto".

En este sentido, se recuerda que, siempre que las funcionalidades de seguridad de los productos y servicios queden garantizadas, se recomienda que para la adquisición y contratación de estos productos y servicios se utilicen procedimientos de contratación favorecedores de la concurrencia de operadores, maximizando así la eficiencia en la gestión de los fondos públicos invertidos. De igual forma, se recuerda que los esquemas de acreditación de entidades o personas deberán basarse en criterios objetivos, transparentes y no discriminatorios, promoviendo la competencia en la provisión de estos servicios.Igualmente, dado el ámbito técnico del ENS, cabe realizar especial hincapié en la observancia del principio de neutralidad tecnológica, con la interpretación que la jurisprudencia[2] ha realizado del mismo en este tipo de

[2] Para la interpretación del concepto de neutralidad tecnología cabe indicar la Sentencia del Tribunal Supremo de noviembre de 2009 (recurso contencioso administrativo núm. 54/2006) en la que expresamente se indica lo siguiente: '*La flexibilidad con la que se recoge este principio*

procedimientos, y en línea con lo recogido en el artículo 126.6 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (LCSP)[3].

Por último, el artículo 34.1 señala que: "de acuerdo con lo previsto en el artículo 33, el CCN-CERT[4] prestará los siguientes servicios: a) soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las entidades del ámbito de aplicación del presente real decreto […]. Sin cuestionar la función de coordinación que parece razonable pueda ejercer dicho organismo público en materia de seguridad, en línea con el artículo 33.1 del PRD, se plantea que esta función se realice "sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública", y por tanto que no se reserve de forma exclusiva la prestación de servicios de resolución de incidentes a dicha entidad.

4. CONCLUSIONES

Se valora positivamente el objetivo del PRD de 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

evidencia de que no se trata de un mandato inexorable, sino que el legislador, por supuesto, pero también el Gobierno, podrían adoptar medidas en las que no fuera posible mantener una absoluta neutralidad entre las distintas tecnologías que concurren en este ámbito. Ahora bien, no cabe duda de que en tal caso dicha medida tecnológicamente no neutral debe estar sólidamente justificada, sin que fuese posible adoptar otra equivalente y respetuosa con el referido principio, y ser proporcionada en relación con los objetivos perseguidos.' En definitiva, puede de nuevo concluirse que el principio de neutralidad tecnológica es parte esencial del ordenamiento regulador del sector de las comunicaciones electrónicas, sin perjuicio de que las Administraciones públicas en el marco de su actuación puedan en caso de que esté justificado de manera objetiva hacer uso de la necesaria flexibilidad que reconoce la normativa sectorial a la hora de aplicar el citado principio.' De acuerdo con la citada resolución, el principio de neutralidad tecnológica puede decaer frente a la existencia de justificaciones objetivas que aconsejen el uso de una tecnología determinada."

[3] Art. 126.6 LCSP: *"Salvo que lo justifique el objeto del contrato, las prescripciones técnicas no harán referencia a una fabricación o una procedencia determinada, o a un procedimiento concreto que caracterice a los productos o servicios ofrecidos por un empresario determinado, o a marcas, patentes o tipos, o a un origen o a una producción determinados, con la finalidad de favorecer o descartar ciertas empresas o ciertos productos. Tal referencia se autorizará, con carácter excepcional, en el caso en que no sea posible hacer una descripción lo bastante precisa e inteligible del objeto del contrato en aplicación del apartado 5, en cuyo caso irá acompañada de la mención «o equivalente". En este sentido, en el anexo IV se incluye una referencia a una marca comercial (UNIX) que, en caso de no poder ser sustituida por una referencia genérica, se recomendaría que se le acompañe de la expresión "o equivalente" reseñada.*

[4] Centro Criptológico Nacional _Computer Emergency Response Team.

seguro de la información pública y de los servicios públicos prestados a la ciudadanía y las empresas.

Sin perjuicio de la ausencia de restricciones a la competencia reseñables por injustificadas, se realizan comentarios relativos a la profesionalidad del personal, la adquisición de productos de seguridad y contratación de servicios de seguridad y la existencia de potenciales reservas de actividad del CCN-CERT en la prestación de servicios frente a incidentes de seguridad.

En relación con el primero, la CNMC recuerda la importancia, siempre que sea posible, de no circunscribir el ejercicio de actividades relacionadas con la seguridad de los sistemas de información a disponer de una titulación específica. En cuanto a la adquisición de productos de seguridad y contratación de servicios de seguridad, se recuerda la preferencia por la aplicación de aquellos procedimientos de contratación más favorecedores de la concurrencia, así como del respeto al principio de neutralidad tecnológica. Por último, que la función de coordinación del CCN-CERT no suponga una reserva exclusiva de actividad para la prestación de servicios de resolución de incidentes de seguridad.