E.M. nº 62 Mayo-Agosto 2019

AVANCES Y RETOS DE LA AGENCIA EUROPEA PARA LA CIBERSEGURIDAD. EL NUEVO MARCO DE LA CERTIFICACIÓN

Imma Garrós Font
Doctora en Derecho

RESUMEN

El objetivo del presente estudio consiste en ofrecer un análisis jurídico-administrativo de las principales novedades del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 ("Reglamento sobre la Ciberseguridad"). Concretamente, se examina la evolución normativa de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y su actual configuración jurídica, centrándose particularmente en su dimensión funcional. Finalmente, se aborda el estudio del nuevo marco europeo de certificación de la ciberseguridad desde la perspectiva de los principales requisitos que exige la norma para organizar la certificación de ciberseguridad en la Unión.

1. CONSIDERACIONES PRELIMINARES

El pasado 7 de junio, se publicó en el Diario Oficial de la Unión Europea el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 ("Reglamento sobre la Ciberseguridad")[1].

Conscientes de la amplia y compleja regulación de la norma europea resulta necesario invocar, con carácter previo y a los efectos de determinar su ámbito objetivo de aplicación, la previsión que contiene el artículo 1 de este texto reglamentario y que justifica la necesidad de la regulación normativa con vistas a garantizar el correcto funcionamiento del mercado interior, aspirando al mismo tiempo a alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión. Según el mencionado artículo, el Reglamento establece los objetivos, tareas y aspectos organizativos relativos a ENISA y un marco[2] para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión.

Partiendo de estas consideraciones, el presente Reglamento se entenderá sin perjuicio de las competencias de los Estados miembros en materia de actividades relacionadas con la seguridad pública, la defensa, la seguridad nacional y las actividades del Estado en ámbitos del Derecho penal.

[1] Diario Oficial de la Unión Europea nº L 151/15, de 7 de junio de 2019.

[2] Este marco se aplicará sin perjuicio de las disposiciones específicas contenidas en otros actos jurídicos de la Unión relativas a la certificación de carácter voluntario u obligatorio.

Por último, conviene destacar que el Reglamento entró en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea, es decir el pasado 27 de junio, salvo los artículos 58, 60, 61, 63, 64 y 65, que se aplicarán a partir del 28 de junio de 2021.

2. LA AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA)

2.1. Antecedentes normativos

Sobre la evolución normativa de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) es preciso resaltar algunos extremos.

En primer lugar, la seguridad en las redes de comunicación y los sistemas de información se ha convertido en uno de los temas de mayor preocupación por parte de la ciudadanía, las organizaciones y empresas hasta los poderes públicos.

En segundo lugar, las tecnologías de la información y la comunicación (TIC) garantizan el funcionamiento de nuestras economías y se han convertido en un motor decisivo de crecimiento económico, especialmente en sectores clave como la salud, la energía, las finanzas y el transporte y, en particular, respaldan el funcionamiento del mercado interior.

Con el fin de garantizar a los usuarios el mayor grado de seguridad frente a los riesgos en materia de ciberseguridad y ciberamenazas a las redes y los sistemas de información, las redes de telecomunicaciones y los productos, los servicios y dispositivos digitales utilizados, la Unión Europea (UE) se ha dotado de una agencia europea encargada de la seguridad de las redes y de la información (ENISA), que tiene como función principal el asesoramiento y coordinación de las medidas adoptadas por la Comisión y los países de la Unión para dar seguridad a sus redes y sistemas de información.

Analizaremos sucintamente los antecedentes normativos de la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

2.1.1. El Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información

Con carácter previo hemos de señalar que el Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información[3] se aprobó como el objetivo principal reforzar la capacidad de la Comunidad y de los Estados miembros en materia de seguridad de las redes y de la información y, en consecuencia, la de la comunidad empresarial para prevenir, tratar y dar respuesta a los problemas de seguridad de las redes y de la información.

Hay que añadir, que la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) fue diseñada con el fin de prestar asistencia y asesoramiento a la Comisión y a los Estados miembros sobre cuestiones relacionadas con la seguridad de las redes y de la información que entren dentro de sus competencias, de acuerdo con lo establecido en el presente Reglamento; así como facilitar y fomentar la cooperación entre los agentes de los sectores público y privado y así, alcanzar un nivel de seguridad suficientemente elevado en los países de la Unión.

En materia de transparencia, reside sobre las funciones de la Agencia el deber de velar por que el público y las partes interesadas reciban información objetiva, fiable y de fácil acceso, especialmente en lo que respecta a los resultados de su trabajo, si procede. Asimismo, deberá hacer públicas las

[3] Diario Oficial de la Unión Europea nº L 77/1, de 13 de marzo de 2004. Texto normativo derogado

declaraciones de intereses presentadas por el Director Ejecutivo y por los funcionarios enviados en comisión de servicios por los Estados miembros con carácter temporal, así como las declaraciones de intereses presentadas por expertos en relación con asuntos incluidos en los órdenes del día de las reuniones de los grupos de trabajo ad hoc.

El acceso a los documentos de ENISA se realiza con arreglo a lo indicado en el Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

2.1.2. El Reglamento (UE) nº 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo, de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) nº 460/2004

Posteriormente, se publicó el Reglamento (UE) nº 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo, de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) nº 460/2004. Mediante este texto reglamentario fue establecida la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA)[4] con la finalidad de contribuir al desarrollo del sector de la ciberseguridad en la Unión, en particular en lo que respecta a las pymes y las empresas emergentes.

2.1.3. La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

Como consecuencia de esta regulación normativa se aprobó la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[5], más conocida como Directiva NIS "*Network and Information Systems*", con el fin de garantizar un marco normativo respetuoso con la confianza y la seguridad en la utilización de las tecnologías de la información y la comunicación (TIC), el pleno desarrollo de la actividad económica y empresarial, así como la preservación y protección efectiva de los derechos fundamentales.

Esta Directiva constituye el elemento esencial de la estrategia de la Unión Europea en materia de ciberseguridad, estableciendo la figura del operador de servicios esenciales (art. 4.4) y se define como "*aquella entidad pública o privada de uno de los tipos que figuran en el anexo II, que reúna los criterios establecidos en el artículo 5, apartado 2*" (art. 5.2).

En concreto, la Directiva:

a) Establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;

b) Crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;

c) Crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, "red de CSIRT", por sus siglas en inglés de "computer security incident response teams") con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;

[4] Diario Oficial de la Unión Europea nº L 165/41, de 18 de junio de 2013. Texto normativo derogado.
[5] Diario Oficial de la Unión Europea nº L 194/1, de 19 de julio de 2016.

d) Establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;

e) Establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información.

Sea como fuere, uno de los fundamentos sobre los cuales descansa la norma comunitaria reside en establecer unos requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación, así como unos requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.

La coordinación de las legislaciones nacionales debe garantizar un elevado grado de integración jurídica comunitaria y un alto nivel de protección de los intereses generales, de desarrollo económico, de bienestar social y, especialmente, de protección de los consumidores; indispensables para establecer una confianza entre los Estados miembros. Todo ello, a través del fomento de políticas públicas y estrategias comprometidas en el ámbito de la ciberseguridad, orientadas a garantizar un entorno normativo eficiente y un contexto económico dinámico y competitivo de progreso económico y social para el funcionamiento del mercado interior[6].

La Directiva NIS sostiene la necesidad de que todos los Estados miembros posean unas capacidades mínimas y una estrategia que garanticen un elevado nivel de seguridad de las redes y sistemas de información en su territorio.

Hay que precisar que la Directiva establece un régimen jurídico novedoso especialmente para los operadores de servicios esenciales y los proveedores de servicios digitales en materia de seguridad de las redes y sistemas de información.

Desde esa perspectiva, podemos afirmar sin reserva que resulta necesario que todos ellos deban estar sujetos a requisitos en materia de seguridad y notificación de incidentes, con el fin de fomentar una cultura de gestión de riesgos y garantizar que se informe de los incidentes más graves[7].

2.2. Funciones

ENISA desempeñará sus funciones con el objetivo de contribuir a un nivel elevado de ciberseguridad común en toda la Unión y, especialmente, asesorar y sensibilizar en cuestiones relacionadas con la ciberseguridad a las instituciones, órganos y organismos de la Unión, así como otras partes interesadas pertinentes a ésta. Todo ello, desarrollando y promoviendo una cultura de la seguridad de las redes y de la información en beneficio de los ciudadanos, los consumidores, las

[6] Al hilo de lo expuesto es de resaltar el Considerando núm. 36 de la Directiva, según el cual ENISA debe prestar asistencia a los Estados miembros y a la Comisión ofreciéndoles su experiencia, conocimientos y asesoramiento y facilitando el intercambio de buenas prácticas. En concreto, a la hora de aplicar la mencionada Directiva, la Comisión debe consultar a la ENISA, y los Estados miembros deben poder hacerlo. Para desarrollar las capacidades y los conocimientos en los Estados miembros, el Grupo de cooperación debe servir también de instrumento para intercambiar información sobre buenas prácticas, discutir sobre las capacidades y el grado de preparación de los Estados miembros y, a título voluntario, prestar ayuda a los miembros del grupo para evaluar las estrategias nacionales en materia de seguridad de las redes y sistemas de información, la creación de capacidades y los ejercicios de evaluación relativos a la seguridad de las redes y sistemas de información.

[7] A este respecto expresa ALEJANDRO SÁNCHEZ que "*la Directiva NIS conlleva nuevas exigencias en el ámbito de la seguridad cibernética y requiere de una mayor colaboración público-privada"*. Véase el artículo "Implicaciones legales de la Directiva NIS en el ámbito de la seguridad cibernética". *Actualidad Jurídica Aranzadi* núm. 923 (2016). Parte Comentario. Editorial Aranzadi, S.A.U., Cizur Menor. 2016.

empresas y las organizaciones del sector público de la Unión, contribuyendo así a la realización y al correcto funcionamiento del mercado interior.

El artículo 4 del Reglamento preceptúa de una forma exhaustiva los objetivos de ENISA:

1. Será un centro de conocimientos técnicos sobre ciberseguridad en virtud de su independencia, la calidad científica y técnica del asesoramiento y la asistencia prestada y la información ofrecida, la transparencia de sus procedimientos operativos y métodos de funcionamiento y su diligencia en el desempeño de sus funciones.

2. Asistirá a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros, en la elaboración y aplicación de políticas de la Unión relativas a la ciberseguridad, en particular políticas sectoriales sobre ciberseguridad.

3. Prestará su apoyo a la creación de capacidades y a la preparación en toda la Unión, asistiendo a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros y las partes interesadas públicas y privadas a fin de incrementar la protección de sus redes y sistemas de información, desarrollar y mejorar la ciberresiliencia y la capacidad de respuesta y desarrollar las capacidades y competencias en el ámbito de la ciberseguridad.

4. Fomentará la cooperación, en particular el intercambio de información y la coordinación a nivel de la Unión entre los Estados miembros, las instituciones, órganos y organismos de la Unión y las partes interesadas pertinentes, públicas y privadas, sobre las cuestiones relacionadas con la ciberseguridad.

5. Contribuirá a incrementar las capacidades de ciberseguridad a nivel de la Unión para apoyar las acciones de los Estados miembros en la prevención y respuesta a las ciberamenazas, especialmente en caso de incidentes transfronterizos.

6. Promoverá el uso de la certificación europea de ciberseguridad, con vistas a evitar la fragmentación del mercado interior. ENISA contribuirá a la creación y al mantenimiento de un marco de certificación europea de la ciberseguridad de conformidad con el título III del presente Reglamento, con el fin de aumentar la transparencia de la garantía de ciberseguridad de los productos, servicios y procesos de TIC y reforzar así la confianza en el mercado interior digital y su competitividad.

7. Promoverá un alto nivel de sensibilización sobre ciberseguridad, en particular ciberhigiene y ciberalfabetización de los ciudadanos, organizaciones y empresas.

Sobre estas bases, ENISA contribuirá a la elaboración y ejecución de la política y del Derecho de la Unión (art. 5 Reglamento) mediante las siguientes tareas:

1. Prestando asistencia y asesoramiento, en la elaboración y la revisión de la política y del Derecho de la Unión en el ámbito de la ciberseguridad, así como las iniciativas políticas y legislativas sectoriales cuando estén presentes cuestiones relacionadas con la ciberseguridad en particular emitiendo su dictamen y sus análisis independientes y aportando trabajos preparatorios.

2. Asistiendo a los Estados miembros para que apliquen de manera coherente la política y el Derecho de la Unión en materia de ciberseguridad, especialmente en relación con la Directiva (UE) 2016/1148, en particular a través de dictámenes, directrices, recomendaciones y mejores prácticas sobre temas como la gestión de riesgos, la notificación

de incidentes y el compartir información, así como facilitando el intercambio de mejores prácticas entre las autoridades competentes a este respecto.

3. Asistiendo a los Estados miembros y a las instituciones, órganos y organismos de la Unión para que elaboren y promuevan políticas de ciberseguridad que apoyen la disponibilidad general y la integridad del núcleo público de la internet abierta.

4. Contribuyendo a los trabajos del Grupo de cooperación con arreglo al artículo 11 de la Directiva (UE) 2016/1148, ofreciendo su asesoramiento y asistencia.

5. Respaldando:

   a) la elaboración y la ejecución de la política de la Unión en el ámbito de la identidad electrónica y los servicios de confianza, en particular ofreciendo asesoramiento y directrices técnicas, y facilitando el intercambio de mejores prácticas entre las autoridades competentes;

   b) la promoción de una mejora del nivel de seguridad de las comunicaciones electrónicas, en particular ofreciendo asistencia y asesoramiento, y facilitando el intercambio de mejores prácticas entre las autoridades competentes;

   c) la asistencia a los Estados miembros en la ejecución de aspectos específicos de ciberseguridad de la política y el Derecho de la Unión en materia de protección de los datos y la privacidad, así como la emisión, previa solicitud, de un dictamen para el Comité Europeo de Protección de Datos.

6. Respaldando la revisión periódica de las actividades políticas de la Unión mediante la preparación de un informe anual sobre el estado de la aplicación del marco jurídico respectivo en relación con:

   a) Las informaciones sobre las notificaciones de incidentes de los Estados miembros transmitidas por el punto de contacto único al Grupo de cooperación de conformidad con el artículo 10, apartado 3, de la Directiva (UE) 2016/1148;

   b) El resumen de las notificaciones de violación de la seguridad y pérdida de la integridad respecto de los proveedores de servicios de confianza, transmitidas por los organismos de supervisión a ENISA, de conformidad con el artículo 19, apartado 3, del Reglamento (UE) n. o 910/2014 del Parlamento Europeo y del Consejo (23);

   c) Las notificaciones de incidentes relacionados con la seguridad transmitidas por los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público, transmitidas por las autoridades competentes a ENISA, de conformidad con el artículo 40 de la Directiva (UE) 2018/1972.

2.3. Transparencia

Sin duda, una de las garantías que ofrece el Reglamento europeo y que presenta mayor peso es la relativa a la transparencia. El artículo 26 de la regulación normativa reconoce y garantiza la transparencia[8], disponiendo que ENISA llevará a cabo sus actividades con un alto grado de

[8] La concepción del principio de transparencia queda plasmada en el Considerando 20 del Reglamento, según el cual ENISA debe actuar como punto de referencia que genere confianza en el mercado único en virtud de su independencia, la calidad del asesoramiento prestado y la información difundida, la transparencia de sus

transparencia[9] y de conformidad con el artículo 28. Recordemos que la mencionada previsión normativa regula el acceso a los documentos.

Desde esta perspectiva, ENISA velará por que el público y las partes interesadas reciban información adecuada, objetiva, fiable y de fácil acceso, especialmente en lo que respecta a los resultados de su trabajo.

Asimismo, deberá hacer públicas las declaraciones de intereses realizadas según lo previsto en el artículo 25. Este precepto regula la declaración de intereses que, con carácter preceptivo, deberán de efectuar con carácter temporal los miembros del Consejo de Administración, el director ejecutivo y los funcionarios enviados en comisión de servicios por los Estados miembros. En concreto, deberán efectuar cada uno de ellos una declaración de compromisos y una declaración en la que indiquen si tienen o no intereses directos o indirectos que pudieran considerarse perjudiciales para su independencia. Las declaraciones serán exactas y completas, se presentarán anualmente por escrito y se actualizarán siempre que sea necesario.

Por otra parte, la nueva regulación exige a los miembros del Consejo de Administración, el director ejecutivo y los expertos externos que participen en los grupos de trabajo *ad hoc* que declaren cada uno de ellos de forma exacta y completa, a más tardar al comienzo de cada reunión, cualquier interés que pudiera considerarse perjudicial para su independencia en relación con los puntos del orden del día y deberán abstenerse de participar en los debates y en la votación sobre esos puntos.

En todo caso, ENISA establecerá en su reglamento operativo interno las medidas prácticas correspondientes a las normas sobre declaraciones de intereses a que se refieren los apartados 1 y 2.

En este orden de consideraciones debe añadirse, como novedad, que ENISA establecerá en sus normas internas de funcionamiento, las medidas prácticas de aplicación de las normas de transparencia a que se refieren los apartados 1 y 2.

2.4. Acceso a los documentos

Con arreglo a lo previsto en el artículo 28.1 de la norma objeto de análisis, el Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión, se aplicará a los documentos en poder de ENISA. La mencionada norma establece los principios generales y los límites de acceso con la finalidad que los ciudadanos puedan ejercer su derecho de acceso de la manera más

procedimientos, la transparencia de sus métodos de funcionamiento y su diligencia en el desempeño de sus tareas.

[9] ENISA será un centro de conocimientos técnicos sobre ciberseguridad en virtud de su independencia, la calidad científica y técnica del asesoramiento y la asistencia prestados y la información ofrecida, la transparencia de sus procedimientos operativos y métodos de funcionamiento y su diligencia en el desempeño de sus funciones (art. 4.1 Reglamento).

fácil posible[10]. Se puede solicitar acceso a todos los documentos que haya elaborado o recibido una institución, en todos los ámbitos de actividad de la Unión Europea[11].

Hay que notar que el artículo 15, apartado 3, del Tratado de Funcionamiento de la Unión Europea (TFUE) otorga a todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, el derecho a acceder a los documentos de las instituciones, órganos y organismos de la Unión, cualquiera que sea su soporte, con arreglo a los principios y las condiciones que se establecerán de conformidad con el mencionado apartado.

---

[10] Debe precisarse que el propio Considerando 1 del Reglamento (CE) nº 1049/2001, de 30 de mayo, justifica acertadamente la introducción por parte del Tratado de la Unión Europea del concepto de "apertura" en el párrafo segundo de su artículo 1, en virtud del cual el citado Tratado constituye una nueva etapa en el proceso creador de una unión cada vez más estrecha entre los pueblos de Europa, en la cual las decisiones serán tomadas de la forma más abierta y próxima a los ciudadanos que sea posible. La apertura permite garantizar una mayor participación de los ciudadanos en el proceso de toma de decisiones, así como una mayor legitimidad, eficacia y responsabilidad de la administración para con los ciudadanos en un sistema democrático. La apertura contribuye a reforzar los principios de democracia y respeto de los derechos fundamentales contemplados en el artículo 6 del Tratado UE y en la Carta de los Derechos Fundamentales de la Unión Europea.

[11] De acuerdo con lo establecido en el artículo 4 del Reglamento (CE) nº 1049/2001, de 30 de mayo que regula las excepciones:

1. Las instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para la protección de:
   a) el interés público, por lo que respecta a:
      - la seguridad pública,
      - la defensa y los asuntos militares,
      - las relaciones internacionales,
      - la política financiera, monetaria o económica de la Comunidad o de un Estado miembro;
   b) la intimidad y la integridad de la persona, en particular de conformidad con la legislación comunitaria sobre protección de los datos personales.
2. Las instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para la protección de:
   - los intereses comerciales de una persona física o jurídica, incluida la propiedad intelectual,
   - los procedimientos judiciales y el asesoramiento jurídico,
   - el objetivo de las actividades de inspección, investigación y auditoría, salvo que su divulgación revista un interés público superior.
3. Se denegará el acceso a un documento elaborado por una institución para su uso interno o recibido por ella, relacionado con un asunto sobre el que la institución no haya tomado todavía una decisión, si su divulgación perjudicara gravemente el proceso de toma de decisiones de la institución, salvo que dicha divulgación revista un interés público superior. Se denegará el acceso a un documento que contenga opiniones para uso interno, en el marco de deliberaciones o consultas previas en el seno de la institución, incluso después de adoptada la decisión, si la divulgación del documento perjudicará gravemente el proceso de toma de decisiones de la institución, salvo que dicha divulgación revista un interés público superior.
4. En el caso de documentos de terceros, la institución consultará a los terceros con el fin de verificar si son aplicables las excepciones previstas en los apartados 1 o 2, salvo que se deduzca con claridad que se ha de permitir o denegar la divulgación de los mismos.
5. Un Estado miembro podrá solicitar a una institución que no divulgue sin su consentimiento previo un documento originario de dicho Estado.
6. En el caso de que las excepciones previstas se apliquen únicamente a determinadas partes del documento solicitado, las demás partes se divulgarán.
7. Las excepciones, tal y como se hayan establecido en los apartados 1, 2 y 3 sólo se aplicarán durante el período en que esté justificada la protección en función del contenido del documento. Podrán aplicarse las excepciones durante un período máximo de 30 años. En el caso de los documentos cubiertos por las excepciones relativas a la intimidad o a los intereses comerciales, así como en el caso de los documentos sensibles, las excepciones podrán seguir aplicándose después de dicho período, si fuere necesario.

Conviene recordar, a este respecto, que el Consejo de Administración adoptará las disposiciones para la aplicación del Reglamento (CE) nº 1049/2001, a más tardar el 28 de diciembre de 2019.

Establecidas las anteriores precisiones, resta añadir que las decisiones tomadas por ENISA en virtud del artículo 8 del Reglamento (CE) nº 1049/2001 podrán ser objeto de una reclamación ante el Defensor del Pueblo Europeo en virtud del artículo 228 del TFUE o de un recurso ante el Tribunal de Justicia de la Unión Europea en virtud del artículo 263 del TFUE.

3. EL MARCO EUROPEO DE CERTIFICACIÓN DE LA CIBERSEGURIDAD

3.1. Consideraciones preliminares

Con carácter previo conviene precisar que el marco europeo de certificación de la ciberseguridad queda regulado en los artículos 46 a 65 del Reglamento.

En la actualidad, la certificación de la ciberseguridad desempeña un papel importante en aras a aumentar la confianza y la seguridad en los productos, servicios y procesos de TIC. Por consiguiente, es necesario establecer un marco europeo de certificación de la ciberseguridad que establezca los principales requisitos horizontales para desarrollar esquemas europeos de certificación de la ciberseguridad y permita que los certificados de ciberseguridad europeos y las declaraciones de conformidad de la UE de productos, servicios o procesos de TIC sean reconocidos y usados en todos los Estados miembros[12].

A estos efectos, el Reglamento regula la creación del marco europeo de certificación de la ciberseguridad**,** con el fin de mejorar las condiciones de funcionamiento del mercado interior incrementando el nivel de ciberseguridad dentro de la Unión y haciendo posible un planteamiento armonizado a nivel de la Unión de esquemas europeos de certificación de la ciberseguridad, con el objetivo de crear un mercado único digital para los productos, servicios y procesos de TIC.

El marco europeo de certificación de la ciberseguridad define un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas cumplen los requisitos de seguridad especificados con el objetivo de proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, dichos productos, servicios y procesos durante todo su ciclo de vida.

Sobre esta base resulta fácil concluir que el marco europeo de certificación de la ciberseguridad debe implantarse de forma uniforme en todos los Estados miembros

La Comisión publicará un programa de trabajo evolutivo para los esquemas europeos de certificación de la ciberseguridad (en lo sucesivo, «programa de trabajo evolutivo de la Unión») que definirá las prioridades estratégicas para los futuros esquemas europeos de certificación de la ciberseguridad (art. 47.1 Reglamento). Este programa de trabajo incluirá en particular una lista de

[12] Como se afirma en el Considerando nº 69 del Reglamento, el marco europeo de certificación de la ciberseguridad debe tener un doble objetivo. En primer lugar, aumentar la confianza en los productos, servicios y procesos de TIC que hayan sido certificados con arreglo a los esquemas europeos de certificación de la ciberseguridad. En segundo lugar, proporcionar un marco para la creación de esquemas europeos de certificación de la ciberseguridad, al objeto de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la UE, así como de evitar la fragmentación del mercado interior en el terreno de los esquemas de certificación de la ciberseguridad. En definitiva, se persigue un planteamiento armonizado de esquemas europeos de certificación de la ciberseguridad en la Unión Europea.

productos, servicios y procesos de TIC, o de categorías de los mismos, que pudieran beneficiarse de la inclusión en el ámbito de aplicación de un esquema europeo de certificación de la ciberseguridad.

El Reglamento establece las condiciones para la solicitud, preparación, adopción y revisión de esquemas europeos de certificación de la ciberseguridad; así como sobre sus elementos, niveles de garantía, difusión. También establece previsiones sobre la certificación de la ciberseguridad; los Esquemas y certificados nacionales de certificación de la ciberseguridad; las autoridades nacionales de certificación de la ciberseguridad; los organismos de evaluación de la conformidad; y sobre un Grupo Europeo de Certificación de la Ciberseguridad de nueva creación.

Asimismo, ENISA mantendrá un sitio web asignado al propósito de ofrecer información sobre los esquemas europeos de certificación de la ciberseguridad, los certificados europeos de la ciberseguridad y las declaraciones UE de conformidad y darles publicidad, también en lo que se refiere a los esquemas europeos de certificación de la ciberseguridad que ya no son válidos y certificados europeos de la ciberseguridad y las declaraciones UE de conformidad retirados o caducados y al repositorio de hiperenlaces de información sobre ciberseguridad facilitado de conformidad con el artículo 55. Respecto de esta regulación, conviene destacar que el sitio web al que se refiere el apartado 1 indicará asimismo aquellos esquemas nacionales de certificación de la ciberseguridad que hayan sido sustituidos por un esquema europeo de certificación de la ciberseguridad.

3.2. Certificación de la ciberseguridad

De acuerdo con la previsión normativa que contiene el artículo 56 del Reglamento, los productos, servicios y procesos de TIC que hayan sido certificados según un esquema europeo de certificación de la ciberseguridad[13] adoptado al amparo del artículo 49 se presumirán conformes con los requisitos de dicho esquema. Recordemos que el mencionado artículo 49 del Reglamento regula la preparación, adopción y revisión de esquemas europeos de certificación de la ciberseguridad.

La certificación de la ciberseguridad será voluntaria, salvo que se disponga otra cosa en el Derecho de la Unión o de los Estados miembros.

Los Estados miembros se abstendrán de introducir nuevos esquemas nacionales de certificación de la ciberseguridad para productos, servicios y procesos de TIC cubiertos por un esquema europeo de certificación de la ciberseguridad en vigor.

Le corresponderá a la Comisión la función de evaluar de forma periódica la eficacia y la utilización de los esquemas europeos de certificación de la ciberseguridad adoptados, así como si un esquema europeo de certificación de la ciberseguridad específico debe convertirse en obligatorio mediante el Derecho de la Unión aplicable para garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión y mejorar el funcionamiento del mercado interior.

[13] Según el Considerando 75 del Reglamento, los esquemas europeos de certificación de la ciberseguridad deben de garantizar que los productos, servicios y procesos de TIC certificados con arreglo a un esquema cumplan los requisitos especificados con objeto de proteger la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados, transmitidos o procesados o las funciones conexas de estos productos, servicios y procesos a lo largo de su ciclo de vida, o los servicios ofrecidos por ellos o accesibles a través de ellos. A estos efectos, los productos, servicios y procesos de TIC y las necesidades de ciberseguridad relativas a dichos productos, servicios y procesos son tan dispares que es muy difícil elaborar unos requisitos de ciberseguridad generales que sean válidos en todas las circunstancias. Por lo tanto, es necesario adoptar un concepto amplio y general de la ciberseguridad a efectos de la certificación, que debe ser complementado por una serie de objetivos específicos de ciberseguridad que deben tenerse en cuenta a la hora de diseñar los esquemas europeos de certificación de ciberseguridad.

La primera de tales evaluaciones debe efectuarse a más tardar el 31 de diciembre de 2023, y las evaluaciones posteriores como mínimo cada dos años. La Comisión deberá, con base en los resultados de la evaluación, determinar los productos, servicios y procesos de TIC cubiertos por un esquema de certificación existente que deben estar cubiertos por un esquema de certificación obligatorio.

Los certificados europeos de ciberseguridad se expedirán por el período previsto en el esquema europeo de certificación de la ciberseguridad y podrán renovarse siempre y cuando sigan cumpliéndose los requisitos correspondientes.

3.3. Derecho a presentar una reclamación

Partiendo de este contexto, el artículo 63 del Reglamento reconoce el derecho a que las personas físicas o jurídicas puedan presentar una reclamación ante el responsable de expedir un certificado europeo de ciberseguridad o, cuando la reclamación esté relacionada con un certificado europeo de ciberseguridad expedido por un organismo de evaluación de la conformidad que actúe con arreglo al artículo 56, apartado 6, ante la autoridad nacional de certificación de la ciberseguridad pertinente.

Llegados a este punto cabe traer a colación que la propia autoridad u organismo ante el que se haya presentado la reclamación informará al reclamante sobre el curso del procedimiento y la decisión tomada, e informará al reclamante sobre el derecho de recurso a la tutela judicial efectiva a que se refiere el artículo 64.

3.4. Derecho a la tutela judicial efectiva

Según lo expuesto en el artículo 64 del Reglamento, sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva en lo que respecta a:

a) las decisiones de la autoridad u organismo mencionado en el artículo 63, apartado 1, en particular y cuando corresponda en lo que respecta a la expedición, la no expedición o el reconocimiento de un certificado europeo de ciberseguridad del que sea titular dicha persona física o jurídica;

b) la inacción con respecto a una reclamación presentada ante la autoridad u organismo mencionado en el artículo 63, apartado 1.

Conforme a lo expuesto, los recursos presentados en aplicación del presente artículo se dirimirán en los tribunales del Estado miembro donde se encuentre la autoridad u organismo ante el cual se plantea el procedimiento judicial.

4. CONCLUSIONES

A modo de conclusión, debemos destacar que el auge de la tecnología digital en prácticamente todos los ámbitos de la vida ha llevado a las instituciones comunitarias a diseñar un marco normativo novedoso, centrado en la exigencia de capacidades técnicas y de organización adecuadas por parte de los Estados miembros para poder adoptar medidas de prevención, detección, respuesta y mitigación de los incidentes y riesgos que afecten a las redes y sistemas de información.

A la luz de los crecientes y modernos retos a los que debe hacer frente la Unión en materia de ciberseguridad, es necesario un conjunto completo de medidas que se apoye en actuaciones previas de la Unión y promueva objetivos que se refuercen mutuamente. La finalidad no es otra que garantizar un

elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea y también abordar una cooperación internacional en la materia.

Por ello, más que nunca, los mecanismos de coordinación y cooperación adquieren un papel especialmente relevante, dado que permitirán, a los Estados miembros de la Unión Europea, avanzar hacia una mayor integración para afrontar nuevos desafíos en la seguridad de las redes y sistemas de información.

5. BIBLIOGRAFÍA

CASTILLO JIRNÉNEZ, CINTA (2005): "Agencia Europea de Seguridad de las Redes y de la Información (ENISA)". *La protección jurídica de la intimidad*/coord. per Angeles Jareño Leal Francisco Javier Boi Reig (dir.): 463-474.

CASTILLO JIMÉNEZ, CINTA (2005): "La Agencia Europea de Seguridad de las Redes y de la Información". *Nuevas Políticas Públicas: Anuario Multidisciplinar para la modernización de las Administraciones Públicas* (Ejemplar dedica a: Los derechos fundamentales y las nuevas tecnologías), nº 1: 195-209.

DÁVILA MURO, JORGE: (2016): "La Directiva NIS y el sueño del Emperador". *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, ISSN 1136-0623, vol. 25, nº 121: 102-106.

FERNÁNDEZ BERMEJO, DANIEL (2018): "Ciberseguridad, ciberespacio y ciberdelincuencia". Cizur Menor: Aranzadi: Thomson Reuters.

GALÁN, CARLOS (2018): "La Ciberseguridad como derecho". *Estudios de derecho público en homenaje a Luciano Parejo Alfonso.* Madrid: Centro de Estudios Políticos y Constitucionales: 755-770.

GALÁN, CARLOS (2017): "Ciberseguridad pública: el marco integrador de la estrategia de ciberseguridad nacional" *Retos del Estado y la administración en el siglo XXI: Libro homenaje al profesor Tomás de la Quadra-Salcedo Fernández del Castillo*. Valencia: Tirant lo Blanch, tomo II: 2167-2195.

MACHÍN, NIEVA; GAZAPO LAPAYESE, MANUEL (2016): "La Ciberseguridad como factor crítico en la Seguridad de la Unión Europea", *Revista UNISCI/UNISCI Journal*, nº 42: 47-68.

MARTÍNEZ MARTÍNEZ, RICARD (2016): "Directiva de ciberseguridad: Un nuevo escenario jurídico y material". *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, ISSN 1136-0623, vol. 25, nº 121: 98-100.

MORET MILLÁS, VICENTE (2017): "Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español". *Documento de opinión. Instituto Español de Estudios Estratégicos*, nº 21: 1- 19.

SÁNCHEZ, ALEJANDRO (2016): "Implicaciones legales de la Directiva NIS en el ámbito de la seguridad cibernética". *Actualidad Jurídica Aranzadi* nº 923. Parte Comentario. Editorial Aranzadi, S.A.U., Cizur Menor.