RECOMENDACIONES

RECOMENDACIÓN (UE) 2019/534 DE LA COMISIÓN

de 26 de marzo de 2019

Ciberseguridad de las redes 5G

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 292,

Considerando que:

(1) La Comisión ha reconocido que el despliegue de la 5.ª generación (5G) de las tecnologías de red constituye un importante elemento promotor de los futuros servicios digitales y una prioridad de la Estrategia para el Mercado Único Digital. La Comisión adoptó el Plan de Acción 5G para garantizar que la Unión disponga de la infraestructura de conectividad necesaria para su transformación digital a partir de 2020 ([1]).

(2) Las redes 5G se basarán en la actual 4.ª generación de tecnologías de red (4G), proporcionarán nuevas capacidades de servicio y se convertirán en la infraestructura central facilitadora de grandes partes de la economía de la Unión. Una vez desplegadas, las redes 5G constituirán la espina dorsal de una amplia gama de servicios esenciales para el funcionamiento del mercado interior y el mantenimiento y el ejercicio de funciones sociales y económicas vitales, como la energía, el transporte, la banca y la sanidad, así como los sistemas de control industrial. La organización de los procesos democráticos, como las elecciones, también se basará cada vez más en las infraestructuras digitales y las redes 5G.

(3) La dependencia de muchos servicios esenciales de las redes 5G provocaría que las consecuencias de las perturbaciones sistémicas y generalizadas fueran especialmente graves. En consecuencia, garantizar la ciberseguridad de las redes 5G es una cuestión de importancia estratégica para la Unión, en un momento en que los ciberataques van en aumento y son más sofisticados que nunca.

(4) La naturaleza interconectada y transnacional de las infraestructuras que sustentan el ecosistema digital y la dimensión transfronteriza de las amenazas significan que cualquier vulnerabilidad o incidente de ciberseguridad importante de las redes 5G que ocurra en un Estado miembro afectaría a la Unión en su conjunto. Esta es la razón por la que deben adoptarse medidas para mantener un elevado nivel común de ciberseguridad de las redes 5G.

(5) La necesidad de actuar a nivel de la Unión ha sido confirmada por los Estados miembros. En sus conclusiones de 21 de marzo de 2019, el Consejo Europeo solicita una recomendación de la Comisión sobre un enfoque concertado de la seguridad de las redes 5G ([2]).

(6) Garantizar la soberanía europea debe ser un objetivo fundamental, respetando plenamente los valores europeos de apertura y tolerancia ([3]). La inversión extranjera en sectores estratégicos, la adquisición de activos, tecnologías e infraestructuras críticos en la Unión y el suministro de equipos críticos también pueden plantear riesgos para la seguridad de la Unión.

(7) La ciberseguridad de las redes 5G es fundamental para garantizar la autonomía estratégica de la Unión, tal como se reconoce en la Comunicación Conjunta «UE-China-Una perspectiva estratégica» ([4]).

(8) La Resolución del Parlamento Europeo sobre las amenazas a la seguridad relacionadas con la creciente presencia tecnológica de China en la Unión también pide a la Comisión y a los Estados miembros que tomen medidas a escala de la Unión ([5]).

(9) La presente Recomendación aborda los riesgos de ciberseguridad de las redes 5G y establece orientaciones sobre las medidas adecuadas de análisis y gestión de riesgos a nivel nacional, el desarrollo de una evaluación coordinada de los riesgos a escala europea y el establecimiento de un proceso para crear un conjunto común de medidas apropiadas de gestión de riesgos.

(10) Existe un sólido marco legislativo de la Unión para proteger las redes de comunicaciones electrónicas.

([1]) COM(2016) 588 final.
([2]) Conclusiones del Consejo Europeo de 21 y 22 de marzo de 2019.
([3]) Estado de la Unión 2018-La hora de la soberanía europea, 12 de septiembre de 2018.
([4]) JOIN (2019) 5 final.
([5]) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0112+0+DOC+XML+V0//ES.

(11) El marco de la Unión en el ámbito de las comunicaciones electrónicas ([6]) promueve la competencia, el mercado interior y los intereses de los usuarios finales, y con el Código Europeo de las Comunicaciones Electrónicas ([7]) persigue un objetivo de conectividad adicional, articulado en forma de resultados: acceso y uso generalizado de la conectividad fija y móvil de muy alta capacidad por todos los ciudadanos y empresas de la Unión, salvaguardando al mismo tiempo los intereses de los ciudadanos. La Directiva 2002/21/CE exige a los Estados miembros que garanticen el mantenimiento de la integridad y la seguridad de las redes públicas de comunicaciones, con la obligación de garantizar que las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público adopten medidas técnicas y organizativas para gestionar adecuadamente los riesgos existentes para la seguridad de las redes y los servicios. También establece que las autoridades reguladoras nacionales competentes tengan competencias, incluida la facultad de emitir instrucciones vinculantes, para garantizar el cumplimiento de dichas obligaciones.

(12) Además, la Directiva 2002/20/CE del Parlamento Europeo y del Consejo ([8]) permite a los Estados miembros añadir a la autorización general condiciones relativas a la seguridad de las redes públicas contra el acceso no autorizado, con el fin de proteger la confidencialidad de las comunicaciones de conformidad con la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([9]).

(13) Para apoyar el cumplimiento de estas obligaciones, la Unión ha instituido varios organismos de cooperación. La Agencia de Seguridad de las Redes y de la Información (ENISA), la Comisión, los Estados miembros y los entes reguladores nacionales han elaborado directrices técnicas para los entes reguladores nacionales sobre la notificación de incidentes, las medidas de seguridad y las amenazas y los recursos ([10]). El Grupo de cooperación establecido por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([11]) («Grupo de cooperación») reúne a las autoridades competentes para apoyar y facilitar la cooperación, en particular proporcionando orientaciones estratégicas para las actividades de la red de equipos de respuesta a incidentes de seguridad informática, que facilita la cooperación operativa a nivel técnico.

(14) El futuro marco europeo de certificación de la ciberseguridad ([12]) debe proporcionar un instrumento de apoyo esencial para promover unos niveles de seguridad coherentes. Debe permitir el desarrollo de unos sistemas de certificación de la ciberseguridad que respondan a las necesidades de los usuarios de equipos y programas informáticos 5G. Dada la importancia crítica de estas infraestructuras, el desarrollo de sistemas europeos de certificación de la ciberseguridad pertinentes de los productos, servicios o procesos de las tecnologías de la información y las comunicaciones utilizados en las redes 5G debe constituir una prioridad inmediata. Los Estados miembros y los agentes del mercado deben participar activamente en el desarrollo de dichos sistemas de certificación, incluido el apoyo a la definición de perfiles de protección específicos de las redes 5G.

(15) En ausencia de una legislación armonizada de la Unión, los Estados miembros podrán especificar, mediante reglamentos técnicos nacionales adoptados de conformidad con el Derecho de la Unión, la obligatoriedad de un sistema europeo de certificación de la ciberseguridad. Los Estados miembros también recurren a los sistemas europeos de certificación de la ciberseguridad en el contexto de la contratación pública y la Directiva 2014/24/UE del Parlamento Europeo y del Consejo ([13]) y podrían apoyar el desarrollo de mecanismos de asistencia, como un centro de asistencia, para la adquisición de soluciones de ciberseguridad por los compradores públicos.

(16) Un elevado nivel de protección de los datos y de la privacidad es un elemento importante para garantizar la seguridad de las redes 5G. Se han definido también normas a nivel de la Unión que garantizan la seguridad del tratamiento de los datos personales, incluidas las comunicaciones electrónicas. El Reglamento general de protección de datos ([14]) establece la obligación de tratar los datos personales de manera que se garantice su seguridad, en particular impidiendo el acceso o el uso no autorizado de datos personales y del equipo utilizado para su tratamiento. La Directiva sobre la privacidad y las comunicaciones electrónicas establece normas

([6]) Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco) (DO L 108 de 24.4.2002, p. 33), y Directivas específicas.

([7]) Directiva 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (DO L 321 de 17.12.2018, p. 36).

([8]) Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización) (DO L 108 de 24.4.2002, p. 21).

([9]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) 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 (DO L 194 de 19.7.2016, p. 1).

([12]) Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.o 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación [COM(2017) 477 final-2017/0225 (COD)].

([13]) Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

([14]) 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) (DO L 119 de 4.5.2016, p. 1).

específicas para la protección de la confidencialidad de las comunicaciones y de los equipos terminales de los usuarios finales. También impone a los proveedores de servicios la obligación de adoptar las medidas técnicas y organizativas adecuadas para garantizar la seguridad de sus servicios.

(17) La Unión también ha adoptado un instrumento que protegerá las infraestructuras y tecnologías críticas, como las utilizadas en las comunicaciones, merced a la autorización otorgada a los Estados miembros para controlar las inversiones extranjeras directas por motivos de seguridad o de orden público, y mediante la creación de un mecanismo de cooperación en el que los Estados miembros y la Comisión puedan intercambiar información y expresar sus inquietudes sobre inversiones específicas ([15]).

(18) Los Estados miembros y los operadores están tomando actualmente importantes medidas preparatorias que posibiliten el despliegue a gran escala de las redes 5G. Varios Estados miembros han expresado su preocupación por los posibles riesgos de seguridad relacionados con las redes 5G en el contexto de la aplicación de procedimientos para la concesión de derechos de uso de bandas de espectro radioeléctrico asignadas para las redes 5G ([16]) y han explorado medidas para hacer frente a estos riesgos.

(19) Al abordar los riesgos de ciberseguridad en las redes 5G, deben tenerse en cuenta tanto los factores técnicos como de otro tipo. Los factores técnicos pueden incluir las vulnerabilidades de ciberseguridad que puedan explotarse para acceder sin autorización a la información (ciberespionaje, por motivos económicos o políticos) o para otros fines dolosos (ciberataques destinados a perturbar o destruir sistemas y datos). Entre los aspectos relevantes que deben considerarse figuran la necesidad de proteger las redes a lo largo de todo su ciclo de vida y la necesidad de abarcar todos los equipos pertinentes, en particular en las fases de diseño, desarrollo, licitación, despliegue, explotación y mantenimiento de las redes 5G.

(20) Otros factores pueden ser los requisitos reglamentarios o de otro tipo impuestos a los proveedores de equipos de tecnologías de la información y las comunicaciones. Una evaluación de la importancia de tales factores debería tener en cuenta, entre otras cosas, el riesgo global de influencia de terceros países, especialmente en relación con su modelo de gobernanza; la ausencia de acuerdos de cooperación en materia de seguridad o de acuerdos similares, como las decisiones de adecuación, en materia de protección de datos entre la Unión y el tercer país de que se trate, o si este país es parte en acuerdos multilaterales, internacionales o bilaterales en materia de ciberseguridad, lucha contra la ciberdelincuencia o protección de datos.

(21) Un elemento importante para el desarrollo de un enfoque de la Unión sobre la ciberseguridad de las redes 5G es la realización de una evaluación de riesgos a nivel nacional. Ayudaría a los Estados miembros a adaptar las medidas nacionales sobre los requisitos de seguridad y gestión de riesgos a la luz de sus resultados.

(22) Debe desarrollarse la coordinación para garantizar la eficacia de las medidas destinadas a hacer frente a estas amenazas a la ciberseguridad, medidas que son esenciales para el buen funcionamiento del mercado interior y para la protección de los datos personales y la privacidad.

(23) Las evaluaciones nacionales de riesgos deben constituir la base de una evaluación coordinada de riesgos de la Unión, compuesta por un mapa de amenazas y una revisión conjunta de los Estados miembros, con el apoyo de la Comisión y en colaboración con la Agencia Europea de Ciberseguridad (ENISA).

(24) Teniendo en cuenta las evaluaciones de riesgo nacionales y de la Unión, el Grupo de cooperación debe establecer un conjunto de herramientas que identifique los tipos de riesgos de ciberseguridad y las posibles medidas para mitigarlos en ámbitos como la certificación, las pruebas y los controles de acceso. También debe identificar posibles medidas específicas adecuadas para hacer frente a los riesgos detectados por uno o varios Estados miembros. El Grupo de cooperación debe contar con el apoyo de la Agencia Europea de Ciberseguridad (ENISA), Europol, el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) y el Centro de Inteligencia y Situación de la UE. Este conjunto de herramientas debe servir para asesorar a la Comisión en el desarrollo de requisitos mínimos comunes para seguir garantizando un elevado nivel de ciberseguridad de las redes 5G en toda la Unión.

(25) Cuando se adopten medidas para hacer frente a los riesgos de ciberseguridad, deberá tenerse en cuenta la promoción de la ciberseguridad a través de la diversidad de proveedores al construir las redes respectivas.

([15]) Reglamento (UE) 2019/452 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019, para el control de las inversiones extranjeras directas en la Unión, DO L 79 I de 21.3.2019, p. 1-14..

([16]) El procedimiento de subasta en al menos una banda del espectro está previsto para 2019 en 11 Estados miembros: Austria, Bélgica, República Checa, Francia, Alemania, Grecia, Hungría, Irlanda, Países Bajos, Lituania y Portugal. Para 2020 están previstas seis subastas más: España, Malta, Lituania (distintas frecuencias), Eslovaquia, Polonia y Reino Unido. *Fuente:* http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) La presente Recomendación debe entenderse sin perjuicio de las competencias de los Estados miembros en relación con las actividades relativas a la seguridad pública, la defensa, la seguridad nacional y las actividades del Estado en ámbitos del Derecho penal, incluido el derecho de los Estados miembros a excluir proveedores o suministradores de sus mercados por motivos de seguridad nacional.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

I. **OBJETIVOS**

(1) Con el fin de apoyar el desarrollo de un enfoque de la Unión para garantizar la ciberseguridad de las redes 5G, la presente Recomendación determina las medidas que deben adoptarse para permitir que:

a) los Estados miembros evalúen los riesgos de ciberseguridad que afectan a las redes 5G a nivel nacional y adopten las medidas de seguridad necesarias;

b) los Estados miembros y las instituciones, agencias y otros organismos pertinentes de la Unión desarrollen conjuntamente una evaluación coordinada de riesgos de la Unión, basada en las evaluaciones nacionales de riesgos;

c) el Grupo de cooperación instituido en virtud de la Directiva (UE) 2016/1148 (Grupo de cooperación) establezca un posible conjunto común de medidas para su adopción a fin de mitigar los riesgos de ciberseguridad relacionados con las infraestructuras que sustentan el ecosistema digital, en particular las redes 5G.

II. **DEFINICIONES**

(2) A efectos de la presente Recomendación, se entiende por:

a) «redes 5G»: el conjunto de todos los elementos de la infraestructura de red pertinentes para las tecnologías de las comunicaciones móviles e inalámbricas utilizados en los servicios de conectividad y de valor añadido con características de alto rendimiento, tales como capacidades y velocidades de datos muy elevadas, comunicaciones de baja latencia, fiabilidad ultraelevada o soporte de un elevado número de dispositivos conectados. Pueden incluir elementos de la red preexistentes basados en generaciones anteriores de tecnologías de las comunicaciones móviles e inalámbricas, como 4G o 3G. Se entiende que las redes 5G incluyen todas las partes pertinentes de la red;

b) «infraestructuras que sustentan el ecosistema digital»: las infraestructuras utilizadas para permitir la digitalización a través de una amplia gama de aplicaciones críticas en la economía y la sociedad.

III. **ACCIÓN A NIVEL NACIONAL**

(3) A más tardar el 30 de junio de 2019, los Estados miembros deben llevar a cabo una evaluación de riesgos de la infraestructura de red 5G, incluida la detección de los elementos más sensibles cuyos fallos de seguridad tendrían un impacto negativo importante. Para esa misma fecha, los Estados miembros también deben revisar los requisitos de seguridad y los métodos de gestión de riesgos aplicables a nivel nacional, teniendo en cuenta las amenazas de ciberseguridad que puedan derivarse de i) factores técnicos, como las características técnicas específicas de las redes 5G, y ii) otros factores, como el marco jurídico y político al que pueden estar sujetos los proveedores de equipos de tecnologías de la información y las comunicaciones en terceros países.

(4) Sobre la base de estas evaluaciones y revisiones de riesgos nacionales, y teniendo en cuenta la acción coordinada en curso a nivel de la Unión, los Estados miembros deben:

a) actualizar los requisitos de seguridad y los métodos de gestión de riesgos aplicados con respecto a las redes 5G;

b) actualizar las obligaciones pertinentes impuestas a las empresas que suministren redes de comunicaciones públicas o presten servicios de comunicaciones electrónicas disponibles para el público con arreglo a los artículos 13 *bis* y 13 *ter* de la Directiva 2002/21/CE;

c) añadir a la autorización general condiciones relativas a la seguridad de las redes públicas contra el acceso no autorizado y recabar de las empresas participantes en los futuros procedimientos de concesión de derechos de uso de radiofrecuencias en las bandas de 5G el compromiso de cumplimiento de los requisitos de seguridad de las redes de conformidad con la Directiva 2002/20/CE;

d) aplicar otras medidas preventivas destinadas a mitigar los posibles riesgos de ciberseguridad.

(5) Las medidas contempladas en el punto 4 deben incluir obligaciones reforzadas para que los proveedores y operadores garanticen la seguridad de los componentes sensibles de las redes, así como la obligación, en su caso, de que proporcionen información pertinente a las autoridades nacionales competentes en relación con los cambios previstos en las redes de comunicaciones electrónicas y los requisitos de prueba previa de determinados componentes y sistemas de tecnología de la información a efectos de seguridad e integridad en los laboratorios nacionales de auditoría o certificación.

(6) Las revisiones de seguridad conjuntas deben ser realizadas por dos o más Estados miembros, utilizando y compartiendo los conocimientos técnicos y los servicios adecuados en relación con las infraestructuras que sustentan el ecosistema digital y las redes 5G, por ejemplo, cuando la misma empresa opere o construya una infraestructura de red en más de un Estado miembro o cuando existan grandes semejanzas en las configuraciones de la red. La Agencia Europea de Ciberseguridad (ENISA), Europol y el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) debe conceder prioridad a las solicitudes de ayuda de los Estados miembros en este ámbito. Los resultados de estas revisiones deben transmitirse al Grupo de cooperación y a la red de equipos de respuesta a incidentes de seguridad informática.

IV. ACCIÓN COORDINADA A NIVEL DE LA UNIÓN

(7) A fin de desarrollar un enfoque común para abordar los riesgos de ciberseguridad en relación con las redes 5G, los Estados miembros deben empezar a operar en una línea de trabajo específica en el Grupo de cooperación, a más tardar el 30 de abril de 2019. Los Estados miembros deben invitar a las autoridades pertinentes a participar, en su caso, en los trabajos del Grupo de cooperación.

Una evaluación europea coordinada de los riesgos

(8) Los Estados miembros deben intercambiar información entre sí y con los organismos pertinentes de la Unión a fin de adquirir un entendimiento común de los riesgos de ciberseguridad existentes y potenciales asociados a las redes 5G.

(9) Los Estados miembros deben transmitir sus evaluaciones de riesgos nacionales a la Comisión y a la Agencia Europea de Ciberseguridad (ENISA), a más tardar el 15 de julio de 2019.

(10) La Agencia Europea de Ciberseguridad (ENISA) debe completar un mapa específico de las amenazas a las redes 5G. El Grupo de cooperación y la red de equipos de respuesta a incidentes de seguridad informática, creados en virtud de la Directiva (UE) 2016/1148, deben apoyar este proceso.

(11) Teniendo en cuenta todos estos elementos, y a más tardar el 1 de octubre de 2019, los Estados miembros, con el apoyo de la Comisión y de la Agencia Europea de Ciberseguridad (ENISA), deben completar una revisión conjunta de la exposición de la Unión a los riesgos relacionados con las infraestructuras que sustentan el ecosistema digital, en particular las redes 5G.

(12) Esta revisión conjunta debe otorgar prioridad a un análisis de riesgos aplicable a los elementos especialmente sensibles o vulnerables que constituyen el núcleo central de las redes 5G, al centro de operaciones y de mantenimiento, así como al acceso a los elementos de la red 5G utilizados en aplicaciones industriales.

(13) En una segunda fase, esta revisión conjunta deberá ampliarse a otros elementos estratégicos de la cadena de valor digital.

Un conjunto de herramientas común de la Unión para hacer frente a los riesgos

(14) El Grupo de cooperación debe determinar las mejores prácticas aplicadas a nivel nacional del tipo previsto en el punto 4. Sobre la base de estas mejores prácticas nacionales, debe acordarse, a más tardar el 31 de diciembre de 2019, un conjunto de medidas de gestión de riesgos apropiadas, eficaces y proporcionadas para mitigar los riesgos de ciberseguridad detectados a nivel nacional y de la Unión, a fin de asesorar a la Comisión sobre el desarrollo de requisitos mínimos comunes para seguir garantizando un elevado nivel de ciberseguridad de las redes 5G en toda la Unión.

(15) Este conjunto de herramientas debe incluir:

a) un inventario de los tipos de riesgos de seguridad que pueden afectar a la ciberseguridad de las redes 5G (por ejemplo, riesgo de la cadena de suministro, riesgo de vulnerabilidad de los programas informáticos, riesgo de control de acceso y riesgos derivados del marco jurídico y político al que pueden estar sujetos los proveedores de equipos de tecnologías de la información y las comunicaciones en terceros países), y

b) un conjunto de posibles medidas mitigadoras (por ejemplo, certificación de equipos, programas o servicios informáticos por terceros; ensayos formales o controles de conformidad de equipos y programas informáticos; procesos para garantizar la existencia y realización de controles de acceso; detección de productos, servicios o proveedores potencialmente no seguros, etc.). Estas medidas deberán cubrir todos los tipos de riesgos de seguridad detectados en uno o más Estados miembros a raíz de la evaluación de riesgos.

(16) Una vez desarrollados los sistemas europeos de certificación de la ciberseguridad pertinentes para las redes 5G, los Estados miembros deberán adoptar, de conformidad con el Derecho de la Unión, reglamentos técnicos nacionales que dispongan la certificación obligatoria de los productos, servicios o sistemas de tecnologías de la información y las comunicaciones cubiertos por estos sistemas.

(17) Los Estados miembros, junto con la Comisión, deben determinar las condiciones de seguridad de las redes públicas contra el acceso no autorizado que se añadirán a la autorización general y los requisitos de seguridad de las redes a efectos de recabar compromisos de las empresas participantes en los procedimientos de concesión de derechos de uso del espectro en las bandas de 5G de conformidad con la Directiva 2002/20/CE. Estos requisitos deberán reflejarse, en la medida de lo posible, en las medidas indicadas en el punto 4, letra c).

(18) Los Estados miembros deben cooperar con la Comisión en la elaboración de requisitos de seguridad específicos que puedan aplicarse en el contexto de la contratación pública relacionada con las redes 5G. Deben incluir los requisitos obligatorios para aplicar los regímenes de certificación de la ciberseguridad en la contratación pública, en la medida en que estos sistemas todavía no sean vinculantes para todos los proveedores y operadores.

V. **REVISIÓN**

(19) Los Estados miembros deben cooperar con la Comisión en la evaluación de los efectos de la presente Recomendación a más tardar el 1 de octubre de 2020, con miras a determinar la manera adecuada de seguir avanzando. Esta evaluación deberá tener en cuenta el resultado de la evaluación coordinada de riesgos de la Unión y del conjunto de herramientas de la Unión.

Hecho en Estrasburgo, el 26 de marzo de 2019.

Por la Comisión
Julian KING
Miembro de la Comisión