RECOMENDACIONES

RECOMENDACIÓN (UE) 2019/553 DE LA COMISIÓN

de 3 de abril de 2019

sobre la ciberseguridad en el sector de la energía

[notificada con el número C(2019) 2400]

LA COMISIÓN EUROPEA,

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

Considerando lo siguiente:

(1) El sector europeo de la energía está experimentando un cambio importante hacia una economía descarbonizada, al tiempo que garantiza la seguridad del suministro y la competitividad. En el marco de esa transición energética y la consiguiente descentralización de la generación de electricidad a partir de fuentes renovables, el progreso tecnológico, el acoplamiento sectorial y la digitalización están convirtiendo la red eléctrica europea en una «red inteligente». Al mismo tiempo, esto también conlleva nuevos riesgos, ya que la digitalización expone cada vez más el sistema energético a ciberataques e incidentes que pueden poner en peligro la seguridad del suministro energético.

(2) La adopción de las ocho propuestas legislativas ([1]) del paquete «Energía limpia para todos los europeos», incluida la gobernanza de la Unión de la Energía como trampolín, permite crear un entorno favorable para la transformación digital del sector de la energía. También reconoce la importancia de la ciberseguridad en el sector de la energía. En particular, la propuesta de Reglamento relativo al mercado interior de la electricidad ([2]) prevé la adopción de normas técnicas para la electricidad, como los «Códigos de red» sobre normas sectoriales específicas para aspectos de ciberseguridad de los flujos eléctricos transfronterizos, sobre los requisitos mínimos comunes, la planificación, el seguimiento, la notificación y la gestión de crisis. La propuesta de Reglamento sobre la preparación frente a los riesgos en el sector de la electricidad ([3]) sigue, en líneas generales, el planteamiento elegido en el Reglamento sobre la seguridad del suministro de gas ([4]), y hace hincapié en la necesidad de evaluar adecuadamente todos los riesgos, también los relativos a la ciberseguridad, y de proponer y adoptar medidas para prevenir y mitigar los riesgos detectados.

(3) La Comisión, al adoptar en 2013 la Estrategia de Ciberseguridad de la Unión Europea ([5]), determinó que era prioritario reforzar la ciberresiliencia de la Unión. Uno de los pilares de dicha estrategia es la Directiva sobre ciberseguridad («Directiva SRI») ([6]), que se adoptó en julio de 2016. Como primera pieza de la legislación horizontal de la UE en materia de ciberseguridad, la Directiva SRI aumenta el nivel general de ciberseguridad en la Unión desarrollando las capacidades nacionales en la materia, incrementando la cooperación a escala de la UE e introduciendo requisitos en materia de seguridad y notificación de incidentes para las empresas denominadas «operadores de servicios esenciales». La notificación de incidentes es obligatoria en sectores clave, como el de la energía.

([1]) Directiva (UE) 2018/2001 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, relativa al fomento del uso de energía procedente de fuentes renovables (DO L 328 de 21.12.2018, p. 82); Directiva (UE) 2018/2002 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se modifica la Directiva 2012/27/UE relativa a la eficiencia energética (DO L 328 de 21.12.2018, p. 210); Reglamento (UE) 2018/1999 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, sobre la gobernanza de la Unión de la Energía y de la Acción por el Clima, y por el que se modifican los Reglamentos (CE) n.º 663/2009 y (CE) n.º 715/2009 del Parlamento Europeo y del Consejo, las Directivas 94/22/CE, 98/70/CE, 2009/31/CE, 2009/73/CE, 2010/31/UE, 2012/27/UE y 2013/30/UE del Parlamento Europeo y del Consejo y las Directivas 2009/119/CE y (UE) 2015/652 del Consejo, y se deroga el Reglamento (UE) n.º 525/2013 del Parlamento Europeo y del Consejo (DO L 328 de 21.12.2018, p. 1); Directiva (UE) 2018/844 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva 2010/31/UE relativa a la eficiencia energética de los edificios y la Directiva 2012/27/UE relativa a la eficiencia energética (DO L 156 de 19.6.2018, p. 75). El Parlamento Europeo, en la sesión plenaria de marzo de 2019, confirmó los acuerdos políticos alcanzados con el Consejo sobre las propuestas de configuración del mercado de la electricidad: Reglamento de preparación frente a los riesgos, Reglamento relativo a la Agencia de Cooperación de los Reguladores de la Energía (ACER), Directiva sobre la electricidad y Reglamento sobre la electricidad. Se espera que la aprobación formal del Consejo tenga lugar en abril; el texto jurídico se publicará en el Diario Oficial poco después.

([2]) COM(2016) 861 final.

([3]) COM(2016) 862 final.

([4]) Reglamento (UE) 2017/1938 del Parlamento Europeo y del Consejo, de 25 de octubre de 2017, sobre medidas para garantizar la seguridad del suministro de gas y por el que se deroga el Reglamento (UE) n.º 994/2010 (DO L 280 de 28.10.2017, p. 1).

([5]) JOIN(2013) 1.

([6]) 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).

(4) Al aplicar medidas de preparación en materia de ciberseguridad, las partes interesadas, como los operadores de servicios esenciales en el ámbito de la energía a que hace referencia la Directiva SRI, deben tener en cuenta las directrices del Grupo de cooperación establecido por el artículo 11 de la Directiva SRI. El Grupo de cooperación, compuesto por representantes de los Estados miembros, de la Agencia de la Unión Europea para la Ciberseguridad («ENISA») y de la Comisión, ha adoptado documentos de orientación sobre medidas de seguridad y notificación de incidentes. En junio de 2018, el Grupo creó una línea de trabajo específica sobre la energía.

(5) La Comunicación conjunta de 2017 sobre la ciberseguridad ([7]) reconoce la importancia de las consideraciones sectoriales específicas y de los requisitos a escala de la Unión, también en el sector de la energía. La ciberseguridad y las posibles implicaciones estratégicas han sido objeto de un amplio debate en la Unión en los últimos años. Todo ello quiere decir que hay mayor conciencia de que cada sector de actividad económica se enfrenta a problemas específicos de ciberseguridad, por lo que tiene que desarrollar sus propios enfoques sectoriales en el marco más amplio de las estrategias generales de ciberseguridad.

(6) La confianza y el intercambio de información son elementos clave de la ciberseguridad. La Comisión pretende aumentar el intercambio de información entre las partes interesadas organizando actos específicos, tales como la mesa redonda (Roma, marzo de 2017) o la conferencia de alto nivel (Bruselas, octubre de 2018) sobre ciberseguridad en el sector la energía. La Comisión también desea mejorar la cooperación entre las partes interesadas y entidades especializadas, como el Centro europeo de puesta en común y análisis de la información energética.

(7) El Reglamento relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad» ([8])), reforzará el mandato de la Agencia de Ciberseguridad de la UE con el fin de prestar un mejor apoyo a los Estados miembros en la lucha contra las amenazas y los ataques de ciberseguridad. También crea un marco europeo de ciberseguridad para la certificación de productos, procesos y servicios que será válido en toda la Unión y reviste especial interés para el sector de la energía.

(8) La Comisión ha presentado una Recomendación ([9]) relativa a la ciberseguridad de la 5.ª generación de tecnologías de red («redes 5G»), que contiene orientaciones sobre medidas nacionales apropiadas de análisis y gestión de riesgos, el diseño de un análisis de riesgos coordinado a escala europea y el establecimiento de un procedimiento para desarrollar herramientas comunes con las mejores medidas de gestión. Una vez que sean operativas, las redes 5G constituirán el esqueleto de una amplia gama de servicios esenciales para el funcionamiento del mercado interior y el desempeño de funciones vitales para la sociedad y la economía, tales como la energía.

(9) La presente Recomendación aspira a proporcionar una orientación no exhaustiva a los Estados miembros y las partes interesadas, en particular a los operadores de redes y proveedores de tecnología, destinada a lograr un mayor nivel de ciberseguridad teniendo en cuenta los requisitos específicos de tiempo real del sector energético, los efectos en cascada y la combinación de tecnologías tradicionales y de vanguardia. Esta orientación tiene por objeto ayudar a las partes interesadas a tener en cuenta los requisitos específicos del sector de la energía al aplicar normas de ciberseguridad reconocidas internacionalmente ([10]).

(10) La Comisión se propone revisar periódicamente la presente Recomendación sobre la base de los progresos realizados en la Unión, en concertación con los Estados miembros y las partes interesadas. La Comisión continuará sus esfuerzos para reforzar la ciberseguridad en el sector de la energía, en particular a través del Grupo de cooperación SRI, que garantiza la cooperación estratégica y el intercambio de información entre los Estados miembros en materia de ciberseguridad.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

OBJETO

1) La presente Recomendación establece las principales cuestiones relacionadas con la ciberseguridad en el sector de la energía: requisitos de tiempo real, efectos en cascada y combinación de tecnologías tradicionales y de vanguardia, y determina las principales acciones que deben llevarse a cabo para aplicar medidas de preparación en materia de ciberseguridad en el sector de la energía.

([7]) JOIN(2017) 450.

([8]) El Parlamento Europeo adoptó el Reglamento de Ciberseguridad en marzo de 2019. Se espera que la aprobación formal del Consejo tenga lugar en abril; el texto jurídico se publicará en el Diario Oficial poco después.

([9]) C(2019) 2335.

([10]) Las organizaciones internacionales de normalización han publicado diversas normas de ciberseguridad (ISO/IEC 27000: Tecnología de la información) y de gestión de riesgos (UNE-ISO 31000: Gestión del riesgo. Directrices). Una norma específica para el sector de la energía (ISO/IEC 27019: Controles de seguridad de la información para la industria de servicios energéticos) se publicó en octubre de 2017 como parte de la serie ISO/IEC 27000.

2) Al aplicar la presente Recomendación, los Estados miembros deben animar a las partes interesadas a que adquieran conocimientos y competencias relacionados con la ciberseguridad en el sector de la energía. Cuando proceda, los Estados miembros también deben incluir estas consideraciones en su marco nacional de ciberseguridad, en particular mediante estrategias, leyes, reglamentos y demás disposiciones administrativas.

REQUISITOS DE TIEMPO REAL DE LOS COMPONENTES DE LA INFRAESTRUCTURA ENERGÉTICA

3) Los Estados miembros deben velar por que las partes interesadas, como los operadores de redes de energía y los proveedores de tecnología, y en particular los operadores de servicios esenciales a que hace referencia la Directiva SRI, apliquen las medidas de preparación en materia de ciberseguridad relacionadas con los requisitos de tiempo real en el sector de la energía. Algunos elementos del sistema energético tienen que funcionar «en tiempo real», es decir, reaccionar en milisegundos, lo que hace difícil o incluso imposible introducir medidas de ciberseguridad por falta de tiempo.

4) En particular, los operadores de redes de energía deben:

a) aplicar las normas de seguridad más recientes para las nuevas instalaciones cuando sea adecuado y estudiar medidas complementarias de seguridad física cuando los mecanismos de ciberseguridad no puedan proteger suficientemente el conjunto de las instalaciones antiguas;

b) aplicar normas internacionales de ciberseguridad y normas técnicas específicas adecuadas para una comunicación en tiempo real segura en cuanto los productos estén disponibles en el mercado;

c) tomar en consideración las restricciones de tiempo real en el concepto general de seguridad de los activos, especialmente en la clasificación de activos;

d) sopesar recurrir a redes privadas para programas de teleprotección con el fin de garantizar el nivel de calidad del servicio requerido para las restricciones de tiempo real; al utilizar las redes públicas de comunicación, los operadores deben plantearse garantizar una asignación de banda específica, requisitos de latencia y medidas de seguridad de la comunicación;

e) dividir el sistema general en zonas lógicas y, dentro de cada zona, definir restricciones de tiempo y procesos que permitan aplicar medidas de ciberseguridad adecuadas o estudiar métodos de protección alternativos.

5) Cuando sea posible, los operadores de redes de energía también deben:

a) elegir un protocolo de comunicación segura, teniendo en cuenta los requisitos de tiempo real, por ejemplo entre una instalación y sus sistemas de gestión (sistema de gestión de la energía/sistema de gestión de la distribución);

b) introducir un mecanismo de autenticación adecuado para la comunicación de máquina a máquina, en el que se aborden los requisitos de tiempo real.

EFECTOS EN CASCADA

6) Los Estados miembros deben velar por que las partes interesadas, como los operadores de redes de energía y los proveedores de tecnología, y en particular los operadores de servicios esenciales a que hace referencia la Directiva SRI, apliquen las medidas de preparación en materia de ciberseguridad relacionadas con los efectos en cascada en el sector de la energía. Las redes eléctricas y los gasoductos están fuertemente interconectados en toda Europa y un ciberataque que provoque una disrupción o la interrupción de una parte del sistema energético podría desencadenar importantes efectos en cascada en otras partes del mismo.

7) Al aplicar la presente Recomendación, los Estados miembros deben evaluar la interdependencia y la criticidad de los sistemas de generación de electricidad y de demanda flexible, las subestaciones y líneas de transmisión y distribución, y las correspondientes partes interesadas que se verán afectadas (también en situaciones transfronterizas) si se produce un ciberataque o un ciberincidente. Los Estados miembros también deben velar por que los operadores de redes de energía dispongan de un marco de comunicación con las partes interesadas para compartir señales de alerta temprana y cooperar en la gestión de crisis. Debe haber canales de comunicación estructurados y formatos acordados para compartir información sensible con las partes interesadas, los equipos de respuesta a incidentes de seguridad informática y las autoridades competentes.

8) En particular, los operadores de redes de energía deben:

a) velar por que los nuevos dispositivos (como los del internet de las cosas) tengan y mantengan un nivel de ciberseguridad adecuado a la criticidad de cada sitio;

b) tener debidamente en cuenta los efectos ciberfísicos al establecer y revisar periódicamente los planes de continuidad de las actividades;

c) establecer criterios de diseño y una arquitectura para una red resiliente, lo que puede conseguirse:

— estableciendo medidas de defensa en profundidad en cada sitio, adaptadas por emplazamiento, adaptadas a su criticidad;

— identificando los nodos cruciales, tanto en términos de capacidad de producción de energía como de repercusión para el cliente; las funciones esenciales de una red deben diseñarse de modo que se mitiguen los riesgos que puedan producir efectos en cascada, teniendo en cuenta la redundancia, la resistencia a las oscilaciones de fase y la protección contra cortes de carga en cascada;

— colaborando con otros operadores y proveedores de tecnología para evitar efectos en cascada, gracias a medidas y servicios adecuados;

— diseñando y creando redes de comunicación y control que permitan confinar los efectos de los posibles fallos de equipos y sistemas a partes limitadas de las mismas, y garantizando medidas de mitigación adecuadas y rápidas.

COMBINACIÓN DE TECNOLOGÍAS TRADICIONALES Y DE VANGUARDIA

9) Los Estados miembros deben velar por que las partes interesadas, en particular los operadores de redes de energía y los proveedores de tecnología, y más concretamente los operadores de servicios esenciales identificados en virtud de la Directiva SRI, apliquen las medidas de preparación en materia de ciberseguridad relacionadas con la combinación de tecnologías tradicionales y de vanguardia en el sector de la energía. En efecto, en el sistema energético actual coexisten dos tipos de tecnologías: una tecnología más antigua, de una vida útil de 30 a 60 años, diseñada antes de que comenzasen las consideraciones de ciberseguridad, y equipos modernos, que reflejan la digitalización de vanguardia, y dispositivos inteligentes.

10) Al aplicar la presente Recomendación, los Estados miembros deben animar a los operadores de redes de energía y a los proveedores de tecnología a seguir, siempre que sea posible, las normas internacionalmente aceptadas en materia de ciberseguridad. Por su parte, las partes interesadas y los clientes deben adoptar un enfoque de ciberseguridad al conectar dispositivos a la red.

11) En particular, los proveedores de tecnología deben aportar soluciones ya experimentadas a los problemas de seguridad, tanto en tecnologías tradicionales como de vanguardia, de forma gratuita y tan pronto como se tenga conocimiento del problema.

12) En particular, los operadores de redes de energía deben:

a) analizar los riesgos de conectar dispositivos tradicionales con otros del internet de las cosas, y ser conscientes de las interfaces internas y externas y de sus vulnerabilidades;

b) tomar las medidas necesarias contra ataques malintencionados procedentes de muchos dispositivos o aplicaciones de consumo que están controlados de forma maliciosa;

c) establecer una capacidad automatizada de seguimiento y análisis de problemas de seguridad en entornos tradicionales y del internet de las cosas, tales como intentos fallidos de iniciar sesión, alarmas de apertura de puertas u otros;

d) realizar periódicamente análisis específicos del riesgo para la ciberseguridad en todas las instalaciones tradicionales, especialmente cuando se conectan tecnologías antiguas y nuevas; dado que las instalaciones tradicionales suelen tener un gran número de activos, el análisis del riesgo puede realizarse por clases de activos;

e) actualizar el *software* y el *hardware* de los sistemas tradicionales y del internet de las cosas con la versión más reciente, siempre que sea procedente; al hacerlo, deben plantearse adoptar medidas complementarias, como la segregación del sistema o la adición de barreras de seguridad externas cuando convenga instalar un parche o hacer una actualización pero no sea posible, por ejemplo, con productos que no reciben soporte;

f) pensar en la ciberseguridad al redactar licitaciones: pedir información sobre las características de seguridad, exigir que se cumplan las normas vigentes de ciberseguridad, asegurarse de recibir de forma continua alertas, parches y propuestas de mitigación si se descubren vulnerabilidades, y aclarar la responsabilidad del vendedor en caso de ataques o incidentes cibernéticos;

g) colaborar con los proveedores de tecnología para sustituir los sistemas tradicionales cuando sea preciso por razones de seguridad, pero teniendo en cuenta las funcionalidades cruciales del sistema.

SEGUIMIENTO

13) Los Estados miembros deben comunicar a la Comisión, antes de transcurridos 12 meses desde la adopción de la presente Recomendación, y posteriormente cada dos años, información detallada sobre el estado de aplicación de la presente Recomendación a través del Grupo de cooperación SRI.

REVISIÓN

14) Sobre la base de la información presentada por los Estados miembros, la Comisión revisará la aplicación de la presente Recomendación y evaluará si se requieren otras medidas, según proceda, en concertación con los Estados miembros y las partes interesadas.

DESTINATARIOS

15) Los destinatarios de la presente Recomendación son los Estados miembros.

Hecho en Bruselas, el 3 de abril de 2019.

Por la Comisión
Miguel ARIAS CAÑETE
Miembro de la Comisión