elperiodicodelaenergia.com
Fecha Publicación: lunes, 2 de febrero de 2026
Páginas: 4
Valor Publicitario: 2926,46 €
V. Únicos: 248263

Europa blinda su sector energético: así es el mayor escudo contra ciberataques de la historia

- La UE despliega una normativa sin precedentes para proteger su sistema energético. La propuesta, que abarca desde la generación eléctrica hasta el hidrógeno, impone la exclusión de proveedores tecnológicos considerados de alto riesgo para las infraestructuras críticas.

Imagen: Vicepresidenta Ejecutiva de Política Tecnológica y de Seguridad de la Comisión Europea, Henna Virkkunen

https://elperiodicodelaenergia.com/europa-blinda-su-sector-energetico-asi-es-el-mayor-escudo-contra-ciberata...

Jaime Santisteban
Sandra Acosta

Lunes, 02 febrero 2026

La Unión Europea avanza hacia un refuerzo sin precedentes de la ciberseguridad en el sector energético, con una propuesta normativa que **amplía y endurece los requisitos de protección digital** para prácticamente toda la cadena de valor: desde grandes infraestructuras críticas hasta operadores de menor tamaño. El objetivo es blindar uno de los pilares estratégicos de la economía europea en un contexto marcado por la tensión geopolítica, la digitalización acelerada y el auge de las amenazas híbridas.

Este impulso regulatorio se enmarca en una maniobra más amplia de Bruselas para vetar a proveedores tecnológicos considerados de alto riesgo, como los gigantes chinos Huawei y ZTE, de sectores críticos, comenzando por el despliegue de las redes 5G. La estrategia, inspirada en la "Caja de Herramientas del 5G", se extiende ahora al corazón del sistema energético, permitiendo evaluaciones de riesgo, restricciones o prohibiciones a escala de la UE para **proteger 18 sectores críticos** . El objetivo declarado es eliminar vulnerabilidades en las cadenas de suministro de tecnologías de la información y la comunicación (TIC) y blindar infraestructuras esenciales frente a posibles injerencias de terceros países, un paso que refleja la creciente preocupación por la seguridad y la autonomía estratégica europea.

elperiodicodelaenergia.com
Fecha Publicación: lunes, 2 de febrero de 2026
Páginas: 4
Valor Publicitario: 2926,46 €
V. Únicos: 248263

La propuesta legislativa de la Comisión Europea, que enmienda los Anexos de la Directiva (EU) 2022/2555, busca blindar infraestructuras críticas mediante la exclusión obligatoria de proveedores de "alto riesgo". Su alcance, definido en el **anexo** , es técnico y sectorialmente específico. En energía, cubre a todos los productores de electricidad (según la Directiva (EU) 2019/944), con la excepción únicamente de aquellos con capacidad total inferior a 1 MW, un umbral tan bajo que engloba prácticamente toda la estructura de generación comercial.

De manera crucial, **extiende la protección al sector del gas y el hidrógeno emergente** , integrando a las empresas de hidrógeno para producción comercial, y a los operadores de almacenamiento y red de transmisión de hidrógeno (definidos en la Directiva (EU) 2024/1788). Finalmente, también incluye a los proveedores de Sistemas Inteligentes de Transporte (Directiva 2010/40/EU). Estos cambios reflejan una voluntad de proteger los vectores energéticos actuales y futuros, así como infraestructuras de transporte vitales, más allá del foco inicial en telecomunicaciones.

La vicepresidenta ejecutiva de Política Tecnológica y de Seguridad de la Comisión Europea, **Henna Virkkunen** , declaró que no estaba satisfecha con cómo los Estados miembros habían estado implementando la "Caja de Herramientas 5G" de la UE, admitiendo que aún había proveedores de alto riesgo en partes críticas de las redes. En este sentido, anunció que ahora se establecerían normas más estrictas sobre el asunto.

Afirmó que las capitales de la UE estaban invirtiendo fuertemente en defensa y seguridad, y que no se podía permitir la presencia de esos proveedores en una parte crítica de la infraestructura. Virkkunen aportó cifras alarmantes, calculando que **los cuatro mayores ciberataques en la UE entre 2020 y 2025 habían tenido un coste de 307.000 millones de euros** y que el 28% de los incidentes se originaban en vulnerabilidades de la cadena de suministro tecnológico.

Sector energético convencional avala el blindaje

Desde el sector gasista, la valoración es claramente positiva. **Sedigas** considera que el impulso de la Comisión Europea supone un paso coherente y necesario al reconocer las infraestructuras energéticas como activos críticos, que deben ser protegidos de forma prioritaria. En un escenario internacional cada vez más complejo, la asociación subraya que la ciberseguridad ya no puede desligarse de la seguridad de suministro ni de la resiliencia del sistema energético, tanto a escala nacional como europea.

Uno de los elementos clave que destaca el sector es la necesidad de un enfoque integral. “La ciberseguridad **no puede dejar huecos** en la cadena de valor”, señalan desde Sedigas, alertando de que un único eslabón vulnerable puede provocar impactos sistémicos con consecuencias económicas, operativas y sociales de gran alcance. De ahí la importancia de que el marco europeo sea homogéneo y coordinado, abarcando desde las grandes redes e infraestructuras hasta los operadores más pequeños.

El gas natural y, cada vez más, los gases renovables forman parte de infraestructuras esenciales para el funcionamiento de la economía y el bienestar de los ciudadanos. En este sentido, elevar el nivel de exigencia, armonizar estándares y reforzar la prevención, detección y respuesta frente a ciberataques es, a juicio de Sedigas, plenamente coherente con el carácter estratégico del sector.

elperiodicodelaenergia.com
Fecha Publicación: lunes, 2 de febrero de 2026
Páginas: 4
Valor Publicitario: 2926,46 €
V. Únicos: 248263

Además, recuerda que **las empresas gasistas ya operan bajo marcos muy estrictos de seguridad operativa y digital** y que llevan años trabajando en esta materia, por ejemplo, mediante su participación en iniciativas de intercambio de información y buenas prácticas como el ES-ISAC Energía, impulsado junto con el Instituto Nacional de Ciberseguridad (INCIBE).

No obstante, el refuerzo regulatorio tendrá impacto en las inversiones. El sector gasista da por hecho que la nueva consideración formal de infraestructuras críticas **implicará destinar más recursos** a tecnología, procesos y capacitación, especialmente en ámbitos como la protección de sistemas industriales, redes, centros de control, comunicaciones y gestión de incidentes. Aun así, insiste en que no se parte de cero: la digitalización de redes, la automatización de instalaciones y el aumento del riesgo asociado al conflicto en Ucrania ya han llevado a intensificar las inversiones en los últimos años. Más que un cambio radical, se tratará de reforzar y homogeneizar los niveles de protección existentes, alineándolos con los nuevos estándares europeos.

Una visión similar comparte el sector eléctrico. Desde **Aelec** valoran de forma positiva que la Unión Europea impulse el refuerzo de la ciberseguridad en todo el ámbito energético y recuerdan que la protección de las infraestructuras eléctricas es esencial para garantizar la seguridad del suministro y la resiliencia del sistema. En un entorno cada vez más digitalizado y con una mayor complejidad geopolítica, la ciberseguridad se ha convertido en un elemento estructural de la seguridad energética.

Las compañías eléctricas llevan años realizando inversiones continuas y aplicando estándares muy exigentes en esta materia, por lo que muchas de las medidas planteadas por Bruselas **ya forman parte de su operativa habitual.** Sin embargo, Aelec reconoce que la ampliación del marco regulatorio europeo puede traer nuevas obligaciones que requieran inversiones adicionales para adaptar y actualizar los sistemas. En este contexto, el sector considera fundamental contar con un marco retributivo estable y con seguridad jurídica que permita recuperar las inversiones necesarias.

De cara al futuro, tanto el gas como la electricidad coinciden en señalar que la ciberseguridad será un pilar estratégico, no solo desde el punto de vista del cumplimiento normativo, sino como garantía de continuidad del suministro, confianza de los consumidores y resiliencia del sistema. La creciente penetración de las energías renovables, la gestión en tiempo real de la energía y la mayor interconexión del sistema hacen imprescindible una operativa digital robusta y segura.

Por su parte, **INCIBE** ha optado por la prudencia. Al tratarse todavía de una propuesta en fase de desarrollo, el organismo no se pronuncia sobre el contenido concreto de la iniciativa europea, aunque ha agradecido el interés y el contacto de los agentes del sector.

La visión del sector renovable y los nuevos operadores digitales

El sector solar fotovoltaico también acoge con satisfacción el enfoque de la Comisión. Dries Acke, director general adjunto de **SolarPower Europe** , señala: "Es muy positivo que la Comisión Europea se tome en serio los temas de ciberseguridad. Como subrayamos en nuestro informe 'Soluciones para los riesgos cibernéticos de la FV para la estabilidad de la red' con DNV, una economía del siglo XXI exige una seguridad del siglo XXI". Acke insiste en que "la clave sigue siendo contar con normas y protocolos de ciberseguridad sólidos y aplicables en toda la UE que se apliquen a todos los

elperiodicodelaenergia.com
Fecha Publicación: lunes, 2 de febrero de 2026
Páginas: 4
Valor Publicitario: 2926,46 €
V. Únicos: 248263

componentes digitales y empresas activas en el mercado energético europeo". La asociación espera seguir cooperando con las instituciones europeas a medida que avanza la evaluación de riesgos específica para la energía solar.

Desde **WindEurope** , la perspectiva es de cauteloso apoyo. La asociación eólica describe la introducción de una disposición sobre "proveedores de alto riesgo" como "un paso significativo y de gran alcance", que refleja la tendencia de la UE a eliminar riesgos de sus cadenas de suministro. Advierten, sin embargo, de las implicaciones operativas si las normas incluyen la posibilidad de retirar equipos ya instalados, un mecanismo regulatorio "sin precedentes". WindEurope subraya que cualquier transición debería ser "gradual, basada en el riesgo y proporcionada para evitar interrupciones no deseadas", especialmente dada la ya crítica congestión de las redes. En última instancia, creen que la propuesta "podría acelerar el despliegue de la energía eólica" al eliminar vulnerabilidades de ciberseguridad que podrían amenazar su expansión.

Desde el lado de los nuevos agregadores y comercializadoras digitales, la visión es pragmática y confiada. Una portavoz de **Octopus Energy** afirma que la directiva "no debe verse como un freno, sino como una oportunidad para fortalecer la resiliencia de nuestra infraestructura". La compañía, que opera con su propia plataforma tecnológica (Kraken), asegura no prever "un impacto negativo en los plazos ni en los costes", gracias a una planificación previa y una cartera de proveedores diversificada que ya cumple con los más altos estándares. Octopus enfatiza que controlar su propio software le otorga mayores garantías de seguridad frente a las vulnerabilidades en cascada que puede generar la dependencia de terceros, posicionándose como un actor clave para construir un ecosistema tecnológico europeo seguro y competitivo.