

Expertos de la UE piden restringir el uso de proveedores solares de alto riesgo

- Expertos en ciberseguridad que asesoran a la Comisión Europea recomiendan restringir los componentes y el software fotovoltaicos procedentes de proveedores de terceros países considerados de alto riesgo en todos los segmentos del mercado, incluidos los sistemas enchufables, y someter los inversores a una...



<https://www.pv-magazine.es/2026/10/09/expertos-de-la-ue-piden-restringir-el-uso-de-proveedores-solares-de-...>

Pilar Sánchez Molina

Viernes, 09 octubre 2026

Un grupo de expertos que asesora a la Comisión Europea ha recomendado restringir los componentes y el software procedentes de proveedores de alto riesgo en todos los segmentos del mercado fotovoltaico de la Unión Europea, desde los sistemas enchufables hasta las plantas a escala comercial.

El informe *Recommendations to address cybersecurity risk in photovoltaic generation* fue elaborado por el grupo de trabajo de ciberseguridad del Smart Energy Expert Group (SEEG) de la Comisión Europea. El documento refleja el consenso de los expertos del grupo y “no representa la opinión de la Comisión Europea”.

Un subgrupo de 11 miembros realizó el análisis. Entre ellos había representantes de SolarPower Europe, Entso-E, Eurelectric, la Oficina Federal Alemana de Seguridad de la Información (BSI) y el Consejo de Reguladores Europeos de la Energía (CEER), así como dos miembros del European Solar Manufacturing Council (ESMC).

Los expertos señalaron que la capacidad fotovoltaica instalada en la Unión Europea pasó de 86 GW en 2015 a 406 GW en 2025. Según el informe, el riesgo se ha vuelto más urgente debido a las graves vulnerabilidades detectadas en inversores, al aumento de las tensiones geopolíticas y a “la fuerte dependencia de la UE de equipos fotovoltaicos de origen chino”. El informe no identifica a ningún país o empresa concreta como proveedor de alto riesgo.

Escenarios de amenaza

El informe evaluó los riesgos en cuatro segmentos: sistemas residenciales enchufables, residencial, comercial e industrial (C&I) y plantas a escala comercial. El impacto se midió en función de la cantidad de generación que podría controlar un atacante, en comparación con los 3.000 MW de reservas de contención de frecuencia de la red continental europea.

El análisis identificó tres riesgos elevados: ataques contra plataformas en la nube de fabricantes conectadas a un gran número de inversores; puertas traseras introducidas por los fabricantes en nombre de un Estado, un riesgo que, según el informe, afecta a todos los segmentos; y ataques contra plantas a escala comercial a través de redes locales.

Los expertos señalaron que hasta ahora no se ha producido en la práctica un ataque mediante una puerta trasera del fabricante, pero consideran que debe tomarse en serio por su posible impacto.

El informe también señaló como riesgo una “arquitectura operativa dividida”, en la que los paneles de monitorización están alojados en la Unión Europea, mientras que las actualizaciones de firmware, la firma digital y las funciones de control remoto se gestionan desde países identificados como jurisdicciones con riesgos significativos de ciberseguridad.

Restricciones a los proveedores

Los expertos recomiendan restringir los componentes y el software procedentes de proveedores sometidos a la jurisdicción de terceros países que planteen riesgos significativos de ciberseguridad, tomando como referencia los criterios incluidos en la propuesta de revisión de la Ley de Ciberseguridad de la Comisión Europea (CSA2). Esto afectaría tanto a los proveedores de componentes y software para fabricantes de inversores como a los propios fabricantes de inversores.

El informe introduce, no obstante, una salvedad: “Restringir el uso de proveedores de alto riesgo puede afectar seriamente al mercado si no existe una oferta alternativa suficiente. Por tanto, solo debería hacerse sobre la base de una evaluación exhaustiva del riesgo”. Los expertos reconocen que no realizaron dicha evaluación.

En virtud de la propuesta CSA2, publicada por la Comisión Europea en enero y todavía pendiente de aprobación, la Comisión podría designar a determinados terceros países como fuente de riesgos para la ciberseguridad y prohibir posteriormente el uso de componentes de proveedores establecidos en esos países o bajo su control.

Estas medidas se aplicarían únicamente a las entidades cubiertas por la directiva NIS2. Por ello, los expertos consideran que la prohibición también debería extenderse a la venta a consumidores de inversores procedentes de proveedores de alto riesgo.

El informe también cita la propuesta de Ley de Aceleración Industrial de la Comisión Europea. Sus considerandos establecen que los proveedores de alto riesgo identificados en el marco de la CSA2 deberían quedar excluidos del suministro de componentes críticos a licitadores en subastas de

energías renovables, participantes en concursos de contratación pública y productos respaldados mediante intervenciones gubernamentales.

Otras medidas

Para las plantas a escala comercial, los expertos recomiendan documentar, cifrar y autenticar todo el tráfico de Internet de los inversores, limitar las conexiones salientes a servidores autorizados ubicados en la Unión Europea o en jurisdicciones equivalentes y bloquear las comunicaciones entrantes procedentes de fuera de la red local.

Para las instalaciones C&I y a escala comercial, proponen sustituir las actualizaciones automáticas de firmware activadas por el fabricante por actualizaciones manuales controladas realizadas por proveedores de mantenimiento cualificados. El objetivo es, entre otros, reducir los riesgos en instalaciones que ya utilizan equipos de proveedores considerados de alto riesgo.

El informe también propone clasificar los inversores fotovoltaicos como productos importantes de Clase II en virtud de la Ley de Ciberresiliencia (CRA). Esto exigiría una evaluación independiente de conformidad por parte de un organismo notificado, además de una norma armonizada de ciberseguridad específica para inversores.

Actualmente, los inversores se encuentran en la categoría por defecto de la CRA, que permite a los fabricantes realizar una autoevaluación.

El informe recuerda que los requisitos de producto de la CRA solo se aplicarán a los productos introducidos en el mercado a partir del 11 de diciembre de 2027 y no al parque instalado.

Entre las demás recomendaciones figuran establecer plazos obligatorios para la aplicación de parches de seguridad en las plataformas de los fabricantes, fijar requisitos mínimos de cualificación en ciberseguridad para los instaladores en el marco del código de red sobre requisitos para generadores y establecer un umbral común de 1 MW para aplicar la directiva NIS2 y el código de red de ciberseguridad eléctrica a las plantas solares.

La posición de los fabricantes

El ESMC, que promueve la fabricación solar europea y representa a unas 70 empresas y organizaciones de investigación, estuvo representado en el subgrupo por su director de políticas, Jens Holm, y por Thomas Rührlinger, responsable de asuntos públicos y regulatorios del fabricante austriaco de inversores Fronius.

“El informe supone un importante paso adelante hacia unos estándares de ciberseguridad más sólidos para la energía solar fotovoltaica en Europa”, afirmó el secretario general del ESMC, Christoph Podewils. “Ahora esperamos que sus recomendaciones se incorporen a las políticas de la UE y de los Estados miembros, especialmente en la actual revisión de la Ley de Ciberseguridad (CSA2)”.

La recomendación del informe de que los servicios web y SSH de los inversores no estén directamente expuestos a Internet coincide con una investigación publicada esta semana por la empresa neerlandesa Modat y el Centro Nacional de Ciberseguridad de los Países Bajos. El estudio

identificó 7.942 sistemas accesibles desde Internet en parques solares de 34 países europeos que, según los investigadores, no deberían haber estado disponibles en línea.

En abril, la Comisión Europea publicó unas directrices para restringir la financiación de proyectos fotovoltaicos que utilicen inversores de proveedores considerados de alto riesgo, con un periodo transitorio para los proyectos que ya se encontraban en desarrollo.

Lituania prohibió en noviembre de 2024 el acceso remoto de empresas chinas a instalaciones solares, eólicas y de almacenamiento de más de 100 kW, mientras que la agencia de ciberseguridad de Chequia advirtió en septiembre de 2025 de que los inversores chinos utilizados en pequeñas plantas solares podían representar un riesgo potencial para la seguridad.