

Europa alerta del riesgo de ciberataques a la fotovoltaica y reclama más controles sobre los inversores

- El grupo de expertos en ciberseguridad del SEEG advierte de que la manipulación remota de instalaciones solares podría comprometer la estabilidad de la red eléctrica y propone reforzar la protección de los equipos, controlar las actualizaciones de software y limitar los proveedores de alto riesgo.



Planta fotovoltaica de Atome.

<https://elperiodicodelaenergia.com/europa-alerta-del-riesgo-de-ciberataques-a-la-fotovoltaica-y-reclama-mas-c...>

Sandra Acosta

Lunes, 12 octubre 2026

El grupo de expertos en ciberseguridad del SEEG advierte de que la manipulación remota de instalaciones solares podría comprometer la estabilidad de la red eléctrica y propone reforzar la protección de los equipos, controlar las actualizaciones de software y limitar los proveedores de alto riesgo

La creciente digitalización de la generación fotovoltaica plantea nuevos retos para la ciberseguridad del sistema eléctrico europeo. La conexión de los inversores a internet y el uso de plataformas digitales para monitorizar y gestionar las instalaciones permiten controlar la producción solar de forma remota, pero también pueden abrir vías de acceso a posibles atacantes. Si estos consiguieran controlar un volumen suficiente de potencia fotovoltaica, **podrían provocar desequilibrios entre la oferta y la demanda de electricidad, congestión en las redes o alteraciones de tensión que, en un escenario extremo, podrían comprometer la continuidad del suministro.**

Ante estos riesgos, el grupo de trabajo de ciberseguridad del Grupo de Expertos en Energía Inteligente (SEEG, por sus siglas en inglés) propone reforzar la protección de los inversores fotovoltaicos y de las plataformas digitales asociadas. Entre sus recomendaciones figuran **controlar las comunicaciones de estos equipos con internet, someter las actualizaciones de software a una supervisión más estricta y restringir el uso de componentes y programas de proveedores**

considerados de alto riesgo. Los expertos también plantean cambios en la normativa europea para mejorar la verificación de los requisitos de seguridad y cubrir las lagunas regulatorias identificadas.

La advertencia se produce en un contexto de rápido crecimiento de la generación solar. La capacidad fotovoltaica instalada en la Unión Europea pasó de 86 GW en 2015 a 406 GW en 2025, y las previsiones de SolarPower Europe apuntan a que podría alcanzar los 718 GW en 2030. El aumento de la potencia conectada, unido a la posibilidad de gestionar numerosos equipos desde plataformas centralizadas, amplía el alcance potencial de una intrusión informática, aunque no implica por sí mismo que las instalaciones sean vulnerables ni que se haya producido un ataque.

Las conclusiones se recogen en el informe *Recommendations to address cybersecurity risk in photovoltaic generation*, publicado en su versión 1.1 el 1 de octubre de 2026. El documento analiza distintos escenarios de ataque sobre instalaciones residenciales, comerciales, industriales y de gran escala, y evalúa hasta qué punto la legislación europea permite prevenirlos. Sus recomendaciones reflejan el consenso de los expertos participantes en el SEEG, pero no representan necesariamente la posición oficial de la Comisión Europea.

Tres escenarios de riesgo elevado

El análisis identifica **tres escenarios** de riesgo alto. El primero son los ataques contra las plataformas de los fabricantes a las que se conectan los inversores, especialmente en instalaciones residenciales, comerciales e industriales. El segundo es la posible introducción deliberada de puertas traseras o backdoors por parte de un fabricante, bajo la influencia o por encargo de un actor estatal. El tercero afecta a las grandes plantas fotovoltaicas y contempla ataques a través de redes locales cuando el atacante consigue acceder a sistemas de acceso remoto y explotar vulnerabilidades de los equipos.

Las plataformas de los fabricantes concentran una parte importante de la preocupación porque permiten monitorizar la producción, modificar parámetros operativos y, en algunos casos, actualizar el firmware de los inversores de forma remota. Una vulnerabilidad en estas infraestructuras podría facilitar el acceso a numerosos equipos conectados al mismo servicio y, potencialmente, permitir que su funcionamiento se alterase de manera coordinada.

El informe cita investigaciones anteriores que han identificado vulnerabilidades en inversores y plataformas de gestión, entre ellas los análisis de Bitdefender sobre Solarman y el estudio SUN de Forescout. Los fallos detectados incluyen deficiencias en los mecanismos de autenticación y autorización, en las interfaces de programación de aplicaciones y en las comunicaciones entre los fabricantes y los dispositivos.

El documento recoge una estimación de Bitdefender según la cual la plataforma Solarman coordinaba 195 GW de potencia en todo el mundo. Esta cifra ilustra la escala potencial de una intrusión en una infraestructura compartida, pero no significa que toda esa capacidad estuviera comprometida ni que se haya producido un ataque de esas características.

Las consecuencias dependerían de la potencia que consiguiera controlar el atacante y de la capacidad del sistema para compensar las alteraciones. Una desconexión simultánea de numerosas

instalaciones podría obligar a los operadores a recurrir a sus reservas para equilibrar la oferta y la demanda. Si el desequilibrio superase los recursos disponibles, podría afectar a la frecuencia de la red. También podrían producirse sobrecargas en líneas y transformadores o problemas de tensión que exigieran actuaciones correctivas para mantener la seguridad del sistema.

Las puertas traseras y la dependencia de proveedores

El grupo de expertos presta especial atención a la **posibilidad de que un fabricante introduzca deliberadamente una puerta trasera en sus equipos o programas**. Este escenario se considera de alto riesgo para todos los segmentos fotovoltaicos analizados, aunque el informe precisa que no se han producido casos confirmados de este tipo en la práctica.

Una puerta trasera podría incorporarse a la plataforma central del fabricante, al firmware del inversor o incluso a su hardware. En los supuestos más sofisticados, un mecanismo de comunicación integrado en el dispositivo podría permitir mantener el acceso remoto incluso después de desconectarlo de internet. Los expertos consideran que esta posibilidad merece atención por su impacto potencial, especialmente si un actor estatal tuviera capacidad para influir en un fabricante o en sus proveedores.

La preocupación está vinculada al **aumento de las tensiones geopolíticas** y a la **concentración de la cadena de suministro fotovoltaica**. El documento destaca la dependencia europea de equipos fabricados fuera de la Unión Europea, particularmente en China, y advierte de que la ubicación de los servidores no siempre refleja dónde se encuentran las funciones más sensibles de los sistemas.

Algunos fabricantes utilizan arquitecturas en las que las plataformas de monitorización están alojadas en servidores europeos, mientras que las actualizaciones del firmware, la autenticación de los dispositivos o los mecanismos de control remoto siguen gestionándose desde terceros países. Según los expertos, esta configuración puede ofrecer una apariencia de control europeo sin garantizar que las funciones críticas estén sometidas a una jurisdicción equivalente.

Por ello, el informe recomienda restringir el uso de componentes y programas de proveedores considerados de alto riesgo tras una evaluación rigurosa. La valoración debería tener en cuenta la jurisdicción a la que está sometido cada proveedor, la información disponible sobre posibles actividades maliciosas y el riesgo de influencia por parte de actores estatales. Los autores advierten de que estas restricciones podrían tener un impacto significativo en el mercado si no existe suficiente oferta alternativa y subrayan la necesidad de fundamentarlas en una evaluación exhaustiva.

Más control sobre las comunicaciones y las actualizaciones

Para reducir los riesgos identificados, los expertos plantean **reforzar los procedimientos de detección y corrección de vulnerabilidades en las plataformas de los fabricantes**. Las empresas deberían buscar activamente fallos de seguridad, responder a los comunicados por investigadores externos y establecer plazos claros para aplicar parches en función de su gravedad. El informe también recomienda fomentar programas de recompensas por la identificación de errores, conocidos como bug bounty.

Otra de las medidas prioritarias consiste en controlar las actualizaciones del firmware. Para las instalaciones comerciales, industriales y de gran escala, el documento propone sustituir las actualizaciones automáticas activadas por los fabricantes por procedimientos manuales, ejecutados por proveedores de mantenimiento cualificados después de comprobar el contenido de los archivos. En las instalaciones críticas, también plantea estudiar el código o recurrir a técnicas de ingeniería inversa para tratar de detectar posibles puertas traseras.

Los autores reconocen que estas medidas no eliminarían por completo el riesgo, especialmente si un fabricante contase con el apoyo técnico de un actor estatal, pero consideran que dificultarían la introducción y explotación de mecanismos maliciosos. En las instalaciones residenciales, en cambio, estiman que las actualizaciones automáticas pueden seguir siendo necesarias para garantizar que los parches de seguridad se instalen de forma fiable y a tiempo.

El control de las comunicaciones constituye otra de las prioridades. El informe recomienda documentar los canales, puertos, protocolos y servidores con los que se comunica cada inversor, y bloquear las conexiones que no estén expresamente autorizadas. Los equipos deberían estar protegidos mediante cortafuegos o routers correctamente configurados y actualizados, sin servicios de acceso entrante directamente expuestos a internet.

Además, las comunicaciones permitidas deberían estar cifradas y autenticadas. Para las instalaciones de mayor tamaño, los expertos proponen restringir las conexiones salientes a servidores autorizados ubicados en la Unión Europea o en jurisdicciones que ofrezcan un nivel de seguridad equivalente, así como impedir las comunicaciones entrantes desde fuera de la red local. También reclaman reforzar la autenticación de los accesos remotos utilizados por los proveedores de mantenimiento.

El informe completa estas recomendaciones con la aplicación de **criterios de seguridad desde el diseño y por defecto**. Entre ellos figuran evitar contraseñas predeterminadas compartidas, cerrar servicios y puertos innecesarios y garantizar la autenticación de los servicios habilitados. Asimismo, pide mejorar la protección de los sistemas que utilizan instaladores y mantenedores para acceder a los equipos y reforzar la formación de estos profesionales en la configuración segura de los inversores, la gestión de credenciales y la prevención de ataques informáticos.

La normativa europea presenta lagunas

El análisis jurídico concluye que el marco europeo ofrece instrumentos para mejorar la seguridad de las instalaciones fotovoltaicas, pero no garantiza una aplicación suficiente de todas las medidas propuestas. El documento examina cuatro normas: el Reglamento de Ciberresiliencia (CRA), la directiva NIS2, el código de red de ciberseguridad eléctrica (NCCS) y el código de red sobre requisitos para generadores (RfG).

Una de las principales limitaciones identificadas afecta al CRA. Aunque este reglamento contempla los productos con elementos digitales, incluidos los inversores fotovoltaicos, **estos no están clasificados como productos importantes o críticos en el marco analizado**. Por ello, los fabricantes pueden demostrar su conformidad mediante un procedimiento de control interno, sin una verificación independiente por parte de un organismo notificado.

Para corregir esta situación, los expertos proponen **desarrollar una norma armonizada de ciberseguridad específica para los inversores y clasificarlos como productos importantes de clase II en el marco del CRA**. Este cambio permitiría exigir una evaluación de conformidad por terceros o una certificación europea de ciberseguridad, reforzando la comprobación independiente de los requisitos.

El informe considera que la directiva NIS2 y el NCCS pueden desempeñar un papel relevante en la protección de las grandes instalaciones y de determinados proveedores de servicios, pero reclama simplificar y armonizar los umbrales de aplicación de ambas normas. Como opción, plantea establecer un umbral común de 1 MW, en línea con la clasificación de instalaciones de generación del código RfG, para facilitar la supervisión de las plantas de mayor tamaño.

En cuanto al RfG, que regula los requisitos de conexión de los generadores a la red, el documento subraya que actualmente no incorpora exigencias específicas de ciberseguridad. Los expertos proponen introducir requisitos mínimos verificables de cualificación en esta materia para los instaladores, de manera que quienes configuren y conecten los inversores dispongan de los conocimientos necesarios para protegerlos.

El grupo también pide **mejorar la coordinación entre las autoridades responsables de la ciberseguridad energética y las de otros sectores**. Muchas instalaciones fotovoltaicas comerciales e industriales pertenecen a empresas cuya actividad principal no es la generación eléctrica, como industrias, hospitales o entidades financieras. Sus obligaciones de ciberseguridad pueden proceder de otras normas, pero sus propietarios y supervisores podrían no ser plenamente conscientes de las consecuencias que un ataque a sus instalaciones solares tendría sobre el sistema eléctrico.

La cadena de suministro, otro frente regulatorio

Los expertos consideran que las normas examinadas no bastan para abordar de manera completa el riesgo de puertas traseras introducidas deliberadamente por los fabricantes. Para cubrir esta laguna, apuntan a la propuesta de revisión de la Ley de Ciberseguridad europea, publicada por la Comisión el 20 de enero de 2026, y al proyecto de Ley de Aceleración Industrial (IAA).

La propuesta de revisión de la Ley de Ciberseguridad contempla mecanismos para identificar países que planteen riesgos para la seguridad de las cadenas de suministro tecnológicas y, sobre esa base, restringir determinados componentes procedentes de proveedores considerados de alto riesgo. Los expertos sostienen que estas medidas deberían poder extenderse también a los equipos residenciales, incluidos los sistemas fotovoltaicos enchufables, dado que su capacidad agregada podría tener relevancia para la estabilidad de la red.

El documento señala, además, que la Ley de la Industria de Cero Emisiones Netas (NZIA) ya incorpora algunos criterios de ciberseguridad para determinadas **subastas** renovables, aunque considera insuficientes sus mecanismos actuales para excluir a proveedores de alto riesgo. En este contexto, plantea aprovechar el futuro marco de aceleración industrial para reforzar las condiciones de las subastas renovables, la contratación pública y otras formas de apoyo público.

Mientras se desarrollan estos cambios normativos, el informe propone medidas que pueden aplicarse de forma voluntaria. Entre ellas, que los distribuidores de electricidad establezcan requisitos de seguridad para los inversores conectados a sus redes, cuando la legislación nacional lo permita, y que las administraciones impulsen campañas de concienciación dirigidas a instaladores, mantenedores y propietarios de instalaciones.

Los expertos advierten, no obstante, de que incluso la aplicación de las medidas propuestas dejaría un riesgo residual. La existencia de equipos ya instalados, las dificultades para mantener actualizada toda la base de inversores y la elevada potencia que pueden controlar fabricantes, agregadores y proveedores de servicios impiden garantizar una protección absoluta.

Por ello, recomiendan **incorporar los escenarios de ciberataque contra la generación fotovoltaica a las evaluaciones de riesgos del sistema eléctrico**, incluidas las contempladas en la normativa de preparación frente a riesgos y en las directrices de operación del sistema. El objetivo es que los operadores puedan anticipar las consecuencias de una intrusión, limitar su impacto y reducir la posibilidad de que una alteración de la generación solar comprometa la continuidad del suministro.