**elperiodicodelaenergia.com**
Fecha Publicación: miércoles, 18 de febrero de 2026
Páginas: 3
Valor Publicitario: 2926,46 €
V. Únicos: 248263



# La armadura digital del sol: retos de ciberseguridad en la infraestructura fotovoltaica europea

- El Europa Solar Quality Summit, que se celebra esta semana en Barcelona, pone el foco en la vulnerabilidad de un sector altamente fragmentado. Expertos internacionales advierten de que la solar no necesita ataques sofisticados para comprometer la estabilidad de la red si no se refuerza la regulación y la…


La armadura digital del sol: retos de ciberseguridad en la infraestructura fotovoltaica europea

https://elperiodicodelaenergia.com/la-armadura-digital-del-sol-retos-de-ciberseguridad-en-la-infraestructura-fo…

Jaime Santisteban

**Miércoles, 18 febrero 2026**

## El Europa Solar Quality Summit, que se celebra esta semana en Barcelona, pone el foco en la vulnerabilidad de un sector altamente fragmentado. Expertos internacionales advierten de que la solar no necesita ataques sofisticados para comprometer la estabilidad de la red si no se refuerza la regulación y la gobernanza del hardware

La fotovoltaica ha dejado de ser un invitado secundario en el mix energético para convertirse en protagonista de la transición. Sin embargo, este crecimiento acelerado ha traído consigo una sombra que el sector ya no puede ignorar: la seguridad digital. En el marco del **Europa Solar Quality Summit** , la industria ha coincidido en que la resiliencia de las plantas no depende solo de la calidad de sus paneles, sino de la robustez de sus cortafuegos. En España, con una capacidad que ya sobrepasa los 48.000 MW, la energía solar fotovoltaica se sitúa **a la cabeza del mix eléctrico nacional** , una cifra que incluye los más de 8.500 MW aportados por el auge del autoconsumo.

El panel “ *Securing the future: cybersecurity priorities in modern PV systems* ” ha servido para constatar que la digitalización es un arma de doble filo. Mientras la inteligencia artificial y la monitorización remota optimizan el rendimiento, también abren miles de puertas traseras en una infraestructura que, por definición, está distribuida y atomizada. Ya no se trata solo de proteger una inversión financiera, sino de blindar la estabilidad del sistema eléctrico nacional.

**elperiodicodelaenergia.com**
Fecha Publicación: miércoles, 18 de febrero de 2026
Páginas: 3
Valor Publicitario: 2926,46 €
V. Únicos: 248263

La percepción del riesgo ha mutado. Si hace unos años la ciberseguridad se veía como un problema exclusivo de la banca o los sectores estratégicos pesados, hoy es una prioridad absoluta en el despliegue solar. La fragmentación de la industria, compuesta por multitud de pequeños actores y plantas dispersas, genera un ecosistema complejo de proteger.

## Una industria vulnerable por diseño

La naturaleza distribuida de la energía solar es, paradójicamente, una gran debilidad ante el cibercrimen. **Ryan Davidson** , principal for grid digitalisation and cyber security en **DNV** , subrayó que la solar es "una de las industrias más interesantes y vulnerables" precisamente por estar tan fragmentada. A diferencia del sector bancario, donde los escudos y los ataques requieren una sofisticación extrema (destacan las enormes inversiones en protección de países como EEUU e Israel), en el sector solar los atacantes no necesitan ser brillantes. "En la solar los ataques no son sofisticados porque no necesitan serlo", apuntó Davidson.

Esta falta de complejidad en el ataque contrasta con la gravedad de las amenazas. **Uri Sadat** , director general de **Solar Defend** , alertó de que los ataques entre estados "se están convirtiendo son ya hoy en día un hecho que merece atención". Según Sadat, el nivel de defensa en las plantas sigue siendo débil, y ya se observan ataques generados por IA y automatizados para golpear infraestructuras energéticas. En este sentido, **Paulo Moniz** , director senior de ciberseguridad y riesgos de **EDP** , incidió en que los cibercriminales son ya uno de los temas centrales en la agenda solar, aunque apuntó que propia IA puede ayudar a cerrar la brecha de talento y falta de especialistas en el sector.

## El dilema del inversor y la soberanía del hardware

Uno de los puntos críticos del debate fue el papel de los inversores fotovoltaicos, el "cerebro" de la instalación que convierte la energía y comunica los datos. La compra y establecimiento en Europa de plataformas manufacturadas fuera del continente plantea un desafío de soberanía. Al adoptar tecnología extranjera, se cede de facto la gobernanza de la plataforma a un tercero. Esto significa que el control del software, las actualizaciones y, en última instancia, la capacidad de desconexión o manipulación de la planta, queda en manos de entidades cuya jurisdicción y lealtades políticas podrían no alinearse con los intereses europeos.

Esta dependencia se agrava por la estructura de costes. **Calin Sas** , technical asset manager en **Sun Rock Netherlands** , definió la ciberseguridad como un "problema de CAPEX" (inversión de capital). Muchas empresas, ante la presión por la rentabilidad, relegan la seguridad a un segundo plano. Por ello, Sas recomendó centrarse en las *low hanging fruits* (soluciones sencillas y al alcance) para mejorar el desempeño, especialmente durante la fase de *commissioning* o puesta en marcha de las plantas.

## Regulación: del fallo de mercado a la directiva NIS2

Para Moniz, la situación actual de la ciberseguridad puede explicarse mediante el concepto de "fallo de mercado" de Adam Smith. “La mayoría de las empresas eligen no protegerse porque no tienen los medios económicos y muchas otras carecen de estadísticas para ser conscientes del riesgo real”,

**elperiodicodelaenergia.com**
Fecha Publicación: miércoles, 18 de febrero de 2026
Páginas: 3
Valor Publicitario: 2926,46 €
V. Únicos: 248263

explicó. Por esta razón, el consenso en Barcelona fue que la regulación es necesaria, aunque no suficiente por sí sola.

Esta diversidad regulatoria dibuja un mapa europeo heterogéneo donde cada país interpreta la seguridad bajo su propio prisma. **Alemania** , por ejemplo, posee un marco altamente prescriptivo a través de la *IT-Sicherheitsgesetz* que, pese a su exhaustivo detalle técnico, a veces cae en la microgestión y genera lagunas de interpretación al priorizar el cumplimiento de listas sobre la gestión real del riesgo. En el extremo opuesto se sitúa **Noruega** , que opta por un modelo funcional que traslada la responsabilidad de la estrategia de seguridad directamente al operador bajo el paraguas de la directiva NIS2. En este escenario, **España** se ubica en un punto intermedio definido por los expertos como un país de "cumplimiento auditado", situándose lejos de la autonomía de gestión noruega pero sin alcanzar el nivel de tutela técnica que caracteriza al modelo alemán.

El futuro pasa por la implementación del **EU Cybersecurity Act** para armonizar certificaciones de hardware y el nuevo **Código de Red sobre Ciberseguridad (NCCS)** , diseñado para blindar los flujos eléctricos transfronterizos. Como advirtió Davidson en una frase que resonó en la sala: "No necesitas que la energía solar o un actor en particular tengan una capacidad masiva para que, si hay disrupción, tengan un gran impacto en la red". La seguridad de uno es, cada vez más, la seguridad de todos.