www.energias-renovables.com
Fecha Publicación: martes, 16 de junio de 2026
Páginas: 4
Valor Publicitario: 2368,51 €
V. Únicos: 53426

Cuatro de cada diez grandes ciberataques al sector energético proceden de actores Estados

energias-renovables.com/panorama/cuatro-de-cada-diez-grandes-ciberataques-al-20260616

Antonio Barrero F. June 15, 2026

El informe 2026 Energy Cybersecurity Outlook advierte que la "convergencia" entre las Tecnologías de la Información y las Tecnologías Operativas, la "inteligencia artificial ofensiva" y la creciente complejidad regulatoria enmarcan y determinan actualmente los riesgos de ciberseguridad de la industria energética. Los autores del estudio observan que la "superficie de exposición a las ciberamenazas" está creciendo debido a la transformación digital del sector energético y advierten que "mantener la seguridad de sus tecnologías operativas se ha convertido en un reto", en tanto en cuanto el sector está "conectando a la red sistemas que antes estaban aislados y creando un panorama energético mucho más distribuido". Esto abarca -señalan- desde estaciones de recarga de vehículos eléctricos hasta instalaciones de energía solar.

El informe de Fortinet también señala ciertas tecnologías emergentes, como la inteligencia artificial, los drones y la criptografía cuántica, que también plantean -sostiene- nuevos retos en materia de ciberseguridad. Todo ello, unido a las exigencias regulatorias, está configurando, según los autores de este estudio- un "nuevo escenario de riesgo" para operadores energéticos, utilities y compañías de infraestructuras críticas.

El estudio de Fortinet destaca que el coste medio de recuperación tras un incidente de ciberseguridad en el sector ya alcanza los 5,08 millones de dólares, mientras que el 39% de los grandes ciberataques registrados en 2025 fueron patrocinados por Estados, la cifra más alta registrada hasta la fecha.

La seguridad de los entornos OT (operational technology) constituye así -apuntan desde Fortinet- una de las principales preocupaciones para las organizaciones energéticas: "de hecho -avanza el informe-, el 57% de las compañías reconoce que sus defensas OT están menos desarrolladas que las de IT [Information Technology], y el 47% de las empresas de

energía y manufactura afirma estar encontrando desafíos de ciberseguridad durante sus procesos de modernización e integración tecnológica".

El informe también pone el foco en la irrupción de la inteligencia artificial como acelerador tanto de la defensa como de las amenazas: "el uso de IA permite a los atacantes crear campañas de phishing* altamente personalizadas, desarrollar malware** más adaptable e incluso emplear técnicas avanzadas de engaño para sortear controles de seguridad".

* El coloquialmente conocido como **phising** es una técnica utilizada por ciberdelincuentes para obtener información confidencial como contraseñas, números de tarjetas de crédito y otra información de carácter personal de los usuarios.

El **malware es un programa informático (software, en inglés) cuya principal característica es que se ejecuta sin el conocimiento ni autorización del propietario o usuario del equipo infectado y realiza funciones en el sistema que son perjudiciales para el usuario y/o para el sistema.

A todo ello -destaca el informe-, se suma la necesidad de prepararse para la era postcuántica. Según Fortinet, el 58% de los responsables de seguridad y TI de infraestructuras críticas ya está experimentando con criptografía postcuántica, anticipándose al impacto que la computación cuántica podría tener sobre los sistemas actuales de cifrado.

Sin embargo, la adopción de patrones de criptografía postcuántica sigue siendo baja: solo el 9% de los millones de sitios de la red más visitados ha adoptado patrones **PQC (criptografía postcuántica)**, "aunque la adopción -matizan los autores del informe- es mayor entre los líderes tecnológicos, ya que 5 de los 10 principales han tomado medidas al respecto".

En Europa, además, las compañías energéticas -aventura Fortinet, que tiene su sede en San Francisco (California)- deberán gestionar un entorno regulatorio cada vez más complejo marcado por (1) la implementación de **NIS2** (directiva europea relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión) y por (2) otras iniciativas orientadas a reforzar la resiliencia de las infraestructuras críticas.

"La diversidad en la aplicación nacional de estas normativas -advierte Fortinet- podría añadir nuevos retos de cumplimiento para las organizaciones con operaciones internacionales".

Ante este contexto, Fortinet identifica cinco prioridades para los responsables de ciberseguridad del sector energético. Son estas.

• integrar la seguridad en todo el ciclo de vida de los activos IT y OT (tecnologías de la información y tecnologías de la operación);

• reforzar la segmentación de redes;

• mejorar la detección y respuesta ante amenazas en tiempo real;

• avanzar en la soberanía de los datos y

• fomentar una mayor colaboración entre industria, reguladores y organismos públicos.

El informe concluye que la resiliencia de las infraestructuras energéticas dependerá cada vez más de la capacidad de las organizaciones para combinar visibilidad sobre sus activos, protección de entornos OT, automatización basada en IA y cumplimiento normativo en un escenario de amenazas cada vez más sofisticado.

Credenciales Fortinet Fundada en el Área de la Bahía de San Francisco en el año 2000, Fortinet es una compañía multinacional que opera en el sector de la ciberseguridad y en la convergencia de redes y seguridad. Según reza en su perfil corporativo, Fortinet posee 1.430 patentes globales (a 31 de marzo de 2026) y oferta una gama de más de 50 productos de nivel empresarial, "la oferta integrada más grande disponible", con "soluciones que se encuentran entre las más implementadas, patentadas y validadas de la industria". La compañía presume de tener una cartera de "más de 900.000 clientes".

Los principales **accionistas de Iberdrola** son el fondo soberano de Catar (Qatar Investment Authority), el fondo estadounidense BlackRock y el banco público Norges de Noruega.

El principal accionista del Grupo Enel, **propietario de Endesa**, es el Ministerio de Economía y Finanzas de Italia. El **segundo mayor accionista** de Enel es BlackRock.

EDP es el principal accionista de EDPR. Los **principales accionistas de EDP** son el estado chino, a través de la empresa estatal China Three Gorges Corporation (20,86%), la empresa asturiano-valenciana Oppidum Capital (6,82%), el fondo de inversiones estadounidense BlackRock (6,82) y el fondo de pensiones canadiense CCPIB (5,62%).

Los **principales accionistas de Naturgy** son Criteria Caixa, Global InfraCo, Corporación Financiera Alba y el estado argelino (a través de la compañía **Sonatrach**).

Informe **2026 Energy Cybersecurity Outlook: Regulatory Complexity, AI-Driven Threats, and OT Risk** (Fortinet)

Artículos relacionados
• **El Gobierno se prepara para repeler los ciberataques a infraestructuras energéticas estratégicas**

• **El ciberataque a Endesa reabre el debate sobre la seguridad de las infraestructuras críticas en España**

www.energias-renovables.com
Fecha Publicación: martes, 16 de junio de 2026
Páginas: 4
Valor Publicitario: 2368,51 €
V. Únicos: 53426