asociación de empresas de mantenimiento
de energías renovables

Ciberseguridad en el sector energético y vulnerabilidades en las instalaciones de energía renovable

#CIBERSEGURIDAD #TIC #SCADA #ENERGIASRENOVABLES
#CORONAVIRUS #COVID19

Mayo 2020

Alejandro Guillén Olague
Asesor Técnico AEMER
aguillen@aemer.org

Índice

Introducción

Uno de los principales desafíos de los sistemas de energía modernos son las vulnerabilidades de sus sistemas de control y gestión remota; además Internet es un medio inseguro y global. Y esa combinación es el campo perfecto para la ciberdelincuencia.

Un **ciberataque es un intento o incidente real** que usa tecnología informáticas y/o sus redes para comprometer o facilitar la comisión de delitos tradicionales, como fraude y falsificación (robo de identidad o datos) o un incidente dirigido a dispositivos de tecnologías de la información y/o operación **con la finalidad de interrumpir o dañar el acceso o cualquier otro aspecto de la funcionalidad**[1].

De acuerdo al VI Informe sobre Cibercriminalidad del Ministerio del Interior[2], en España se registraron 110.613 ciberataques durante 2018, siendo las Comunidades de Madrid, Andalucía y Valenciana las regiones donde estos incidentes fueron más recurrentes. En 2019, hasta 174 municipios españoles fueron afectados por campañas con el conocido virus ramsonware (software que «secuestra» la información, impidiendo el acceso a la misma, cifrándola, y solicitando un rescate).

Por lo general, los países toleran actividades maliciosas siempre que se mantengan en niveles "aceptables"; **medir el impacto exacto es complicado**. En la mayoría de los casos, los atacantes pueden comprometer una organización en cuestión de minutos, mientras que el tiempo de recuperación, por lo general requerirá considerablemente más tiempo.

Los sistemas de control industrial (**ICS**) y sistemas de Supervisión, Control y Adquisición de Datos (**SCADA**), permiten entre otras prestaciones monitorizar y operar en remoto; pero como advierte la organización ENISA (European Union Agency for Network and Information Security)[3] también **abren la puerta a nuevas brechas de ciberseguridad que pueden comprometer el correcto funcionamiento de estos sistemas**.

En este documento se abordará la evolución de los ciberataques por sectores productivos, la situación en la industria energética, ataques cibernéticos en el sector de las energías renovables, recomendaciones técnicas y una posible minoración de daños a través de pólizas específicas de seguros.

---

[1] https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-429-cyber-resilience-health-check/

[2] http://www.interior.gob.es/documents/10180/8736571/Informe+2018+sobre+la+Cibercriminalidad+en+Espa%C3%B1a.pdf/0cad792f-778e-4799-bb1f-206bd195bed2

[3] https://www.enisa.europa.eu/

1. Evolución cuantitativa de los ciberataques por sectores productivos

El Centro Nacional de Integración de Ciberseguridad y Comunicaciones (NCCIC)[4] que es parte del Departamento de Seguridad Nacional de los EE. UU., tiene un área denominada Equipo de respuesta a emergencias cibernéticas de **sistemas de control industrial** (ICS-CERT)[5], este departamento atiende, registra e intercambia información sobre incidentes de ciberseguridad y comunicaciones.

En el año 2015 presentó una comparativa de **ataques por sector productivo**, siendo **el área energética la que presentó más casos acumulados** desde el año 2011:

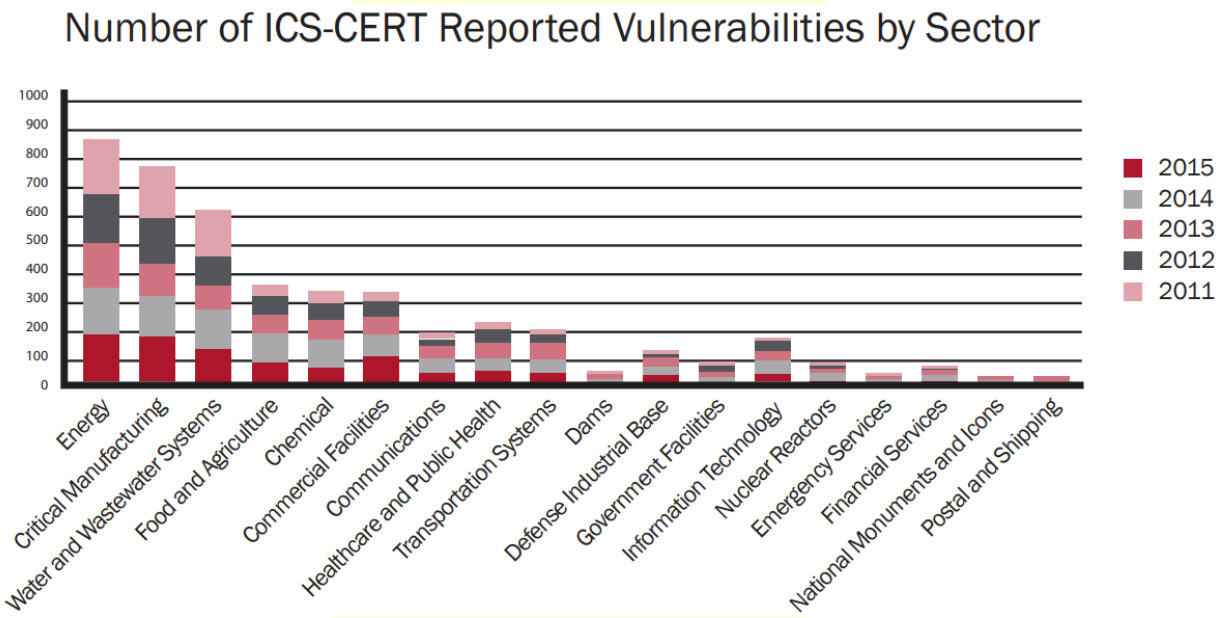

Ilustración 1: Ciberataques acumulados 2011-2015 por sector productivo. Fuente: ICS-CERT [6]

El principal vector de acceso fueron ataques "phishing" (técnica que consiste en engañar al usuario para robarle información confidencial), representando el 37% de los incidentes.

[4] https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center
[5] https://www.us-cert.gov/ics
[6] https://www.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202015_Annual_Vulnerability_Coordination_Report_S508C.pdf

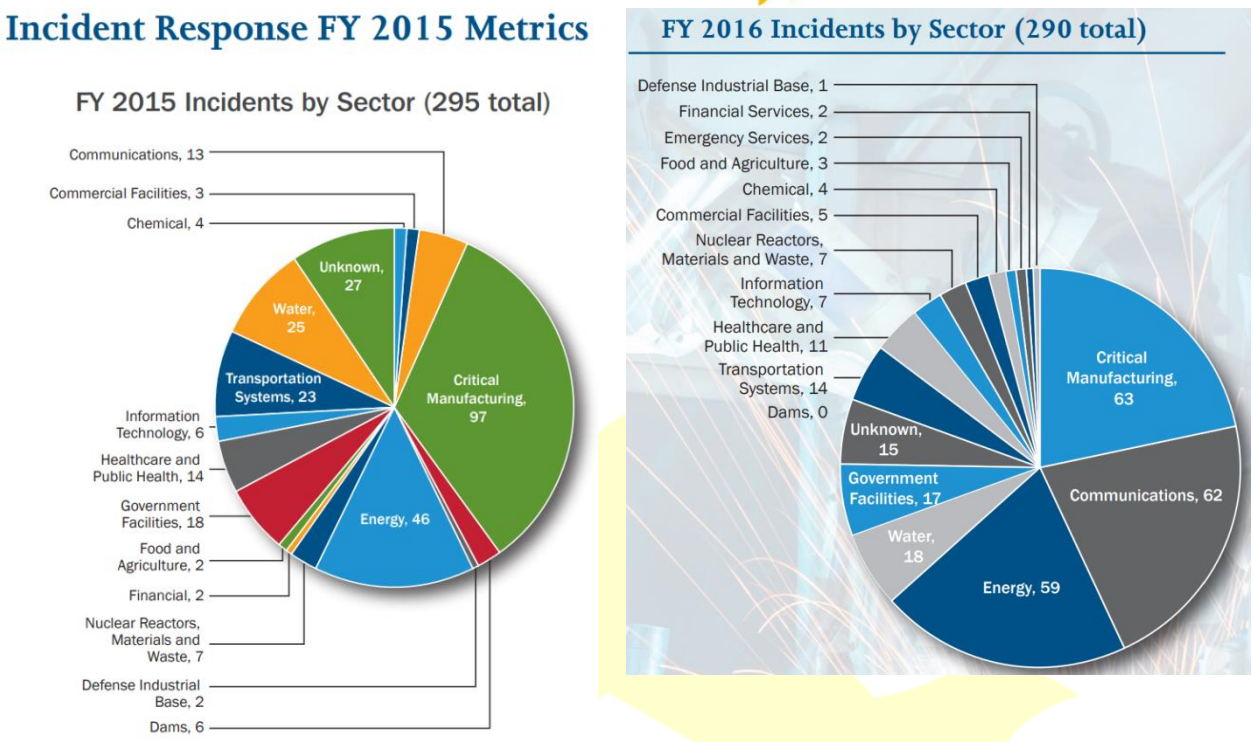

Ilustración 2: Incidentes de seguridad registrados por ICS-CERT por sector productivo. Fuente: ICS-CERT [7] [8]

2. Situación actual en la industria energética

El **sector energético** está experimentando **cambios a una escala y ritmo sin precedentes**. La nueva estructura energética contempla:

- basar el modelo en nuevas tecnologías energéticas como las energías renovables.
- generación y almacenamiento de electricidad en el mismo sitio.
- vehículos eléctricos que tendrán un amplio impacto social y económico.
- blockchain energético que pretende democratizar la producción y venta de la energía principalmente entre pequeños productores.

Este nuevo sistema de energía inteligente **requiere un uso significativamente mayor de las Tecnologías de Información y Comunicación** (TIC) en los rubros de la digitalización de la producción y distribución de la energía.

[7] https://www.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf
[8] https://www.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf

Esta revolución requiere una amplia expansión de dispositivos inteligentes, por tanto, el rango de posibles ataques **(o "vectores de amenaza") se multiplica dentro de los ecosistemas de la energía inteligente y renovable**.

Por este motivo, e**l sector energético ya es un objetivo claro y creciente para los ataques cibernéticos** y desde hace años se han tomado medidas especiales para blindarlos, pero los esfuerzos de protección se han centrado principalmente en las subestaciones y red de transmisión, dejando con **mayor vulnerabilidad los sistemas SCADA que gestionan los sistemas de generación eléctrica renovable**.

A lo largo de los últimos años, se han registrado una serie de **ataques cibernéticos en sistemas ICS-SCADA**. La severidad y consecuencias de los ataques varían. Cada vez se vuelven más sofisticados, experimentados y maliciosos. **Hasta ahora los grandes desastres se han evitado**.

Se podría partir de la premisa que la probabilidad de ciberataques catastróficos en sistemas SCADA es relativamente bajo y zanjar el tema de los riesgos ante un ataque; pero esto puede llevar a un falso sentido de seguridad, ya que **solo un pequeño número de incidentes de seguridad es reportado** y no es posible prever todos los posibles ataques dentro de un sistema SCADA.

El problema puede ser **más crítico cuando se involucran grandes sistemas renovables de potencia de generación de cientos de MW de potencia.** Una interrupción de vertido de electricidad en alguno de estos sistemas **puede causar daños en infraestructuras críticas interdependientes**. Esto conduciría a un desequilibrio importante de carga en la subestación de transmisión, desencadenando una falla en cascada a través de la red eléctrica.

Los atacantes encontrarán y aprovecharán cualquier vulnerabilidad en los dispositivos SCADA, el software que emplean, los componentes de la red, los medios de acceso, los protocolos de operación de los trabajadores o incluso los sistemas operativos de los ordenadores de administración y gestión.

Los sistemas de energía inteligente que actualmente se están implementando dependen completamente de la convergencia de la Tecnología de la información (**TI**) y la Tecnología de la Operación (**TO**). Históricamente, estos dos dominios han estado separados, pero ahora ya es el momento de **analizarlos conjuntamente para aumentar la protección de los sistemas**.

Hasta hace pocos años, la infraestructura energética en Europa estaba dominada por las grandes plantas generadoras, los operadores de sistemas de distribución y el gestor de red. La red presentaba un flujo de energía unidireccional relativamente simple.

Cualquier amenaza y riesgo para la estabilidad y seguridad del sistema estaban contenidos dentro de un pequeño número de activos operativos.

Ahora se tienen sistemas de generación más distribuidos debido al gran número de sistemas de generación renovable; estos activos distribuidos **crean nuevos desafíos en términos de equilibrio y funciones de gestión**. Pasan a ser un sistema más inteligente que depende de las comunicaciones y del software, es decir, un aumento significativo de las vulnerabilidades potenciales y particularmente desde el punto de vista de la seguridad cibernética.

Cabe señalar que un sistema energético más distribuido y descentralizado también proporciona beneficios de seguridad, ya que es más fácil aislar los impactos de un ataque a una parte del sistema.

De acuerdo a un informe de la empresa Analysys Mason[9], en el mejor de los casos, **la transición a nuevos sistemas de red inteligentes dará como resultado mayores costos debidos a mantener múltiples políticas y medidas de seguridad adicionales durante la transición**. En el peor de los casos, expondrá el sistema a numerosos vectores de amenazas adicionales.

En el sector energético, las amenazas por ciberataques pueden crear un daño considerable si se hacen a una escala significativa o cuando se combinan con otros ataques. Además, se debe considerar la mayor cantidad de ataques combinados.
La principal amenaza está en el número de los diferentes tipos y direcciones de ataque que podrían producirse, algunos de los cuales pueden identificarse hasta después del ataque, aumentando la vulnerabilidad del sistema en un punto específico de la red.

3. Principales ataques cibernéticos en el sector energético

Ha habido numerosos **ataques cibernéticos contra el sector energético** en las últimas décadas, **muchos de ellos se conocieron después de muchos años** y no todos fueron el trabajo de atacantes sofisticados; algunos incidentes fueron solo daños colaterales causados por infecciones de malware o problemas de mala configuración. Estos incidentes resaltan el hecho de que tales ataques pueden ocurrir y que pueden tener consecuencias importantes.

A continuación se resaltan los más importantes:

[9] https://www.analysysmason.com/

Año 2000: funcionarios rusos confirman que la compañía de extracción de gas natural más grande del país fue atacada. Los agresores utilizaron un troyano para obtener acceso al control de los gasoductos.

Año 2001: se produjo un ataque contra el centro de distribución de energía de California, que controla la operación y los flujos de la red. Debido a una configuración de seguridad aparentemente deficiente, el atacante pudo comprometer dos servidores Web. La incursión se detuvo antes de que pudieran atacar sistemas conectados a la red de transporte.

Año 2003: el sistema de monitorización de la seguridad de la central nuclear de Ohio se desconectó durante varias horas debido a una infección informática del gusano Slammer. Afortunadamente, la planta de energía estaba fuera de línea por mantenimiento y el gusano no afectó el sistema de monitoreo de respaldo secundario.
A principios de ese año, en una terminal marítima en Venezuela un grupo atacante logró obtener acceso a la red SCADA de la maquinaria de carga de buques petroleros y sobrescribieron con módulo de programa vacío los controladores lógicos programables (PLC). Esto detuvo la maquinaria, evitando que los petroleros pudieran cargar durante ocho horas hasta que el código de respaldo se reinstaló en los PLC.

Año 2008: un alto funcionario de la Agencia Central de Inteligencia (CIA) informó a representantes de compañías de servicios públicos que se habían registrado ataques cibernéticos procedentes de fuera de los EEUU que habían inutilizado equipos de energía en varias ciudades. En algunos casos, el atacante intentó extorsionar a las compañías de energía, amenazándolas con más apagones.

Año 2012: RasGas de Qatar, uno de los mayores productores mundiales de gas natural, fue golpeado por un virus que se infiltró en 30.000 de sus estaciones de trabajo informáticas. La compañía aisló todos sus sistemas informáticos del acceso externo, lo que obligó a los comerciantes de petróleo a volver a comunicarse por fax y télex, ya que incluso los servicios externos de correo electrónico de la compañía eran inoperantes.

Año 2013: parte de la red eléctrica austriaca y alemana casi queda inoperativa debido al desvió de entrega accidental de un comando de control. Un paquete de comando de solicitud de estado, que fue transmitido desde una compañía de gas alemana como prueba para su nueva sucursal de red instalada, se abrió camino en los sistemas de la red austriaca de control y monitorización de energía. Una vez allí,

el mensaje generó miles de mensajes de respuesta, lo que generó aún más paquetes de datos, que a su vez inundaron la red de control. Para detener el ataque parte de la red de monitorización y control tuvo que ser aislada y desconectada. La situación se resolvió sin cortes de energía.

En EEUU, un virus informático atacó un sistema de control de turbina en una compañía eléctrica después de que un técnico insertó una unidad USB infectada en una computadora en la red. El incidente mantuvo una planta fuera de línea durante tres semanas [10].

Año 2014: Symantec destacaba en un informe que debido al crecimiento en la cantidad de sistemas ICS, redes SCADA y tecnologías similares de gestión distribuida; los riesgos de los ciberataques solo podrían ir en aumento[11].

En diciembre de 2014, Corea del Sur informó sobre un ciberataque contra el operador de sus plantas de energía nuclear. Los atacantes divulgaron en línea información sensible y confidencial (incluidos los diseños y manuales para los equipos de la planta).

Año 2015: Un informe de Motorola Solutions indicaba que en cualquier punto donde se haya implementado un dispositivo inteligente, existe el riesgo de que se use como un punto de entrada no autorizado y se tome el control con una intención maliciosa[12].

Años 2015 y 2016: Ucrania presento varias interrupciones en su sistema eléctrico, los fallos se atribuyeron a un ciberataque durante un período de 30 minutos (apagando decenas de subestaciones de 110kV y 35kV) y provocaron cortes de energía que afectaron a cientos de miles de personas que se quedaron sin electricidad en el clima invernal de diciembre[13]. Los atacantes obtuvieron acceso y control ilegales de las computadoras de las compañías y de los sistemas SCADA ligados a las subestaciones. Estos ciberataques son muy significativos porque fueron los primeros incidentes reconocidos públicamente de un ataque contra los sistemas de OT de una nación que dieron como resultado un amplio apagón.

[10] http://www.reuters.com/article/us-cyber security-powerplants-idUSBRE90F1F720130116

[11] https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf

[12] Cyber security: A growing threat to the energy sector – An Australian perspective - March 2016

[13] https://www.powerengineeringint.com/articles/2018/10/protecting-europe-s-grids.html

El 27 de abril de 2016, una planta de energía nuclear alemana (Gundremmingen) fue infectada con virus informáticos. Los virus fueron descubiertos en un sistema informático asociado a equipos de monitorización de barras de combustible[14].

Año 2017: se registraron intentos de ataques a las redes eléctricas en algunos países europeos y un ataque muy importante a instalaciones nucleares en los EE. UU. Estos ataques fueron hechos aparentemente por el llamado grupo Dragonfly. Este grupo parece estar interesado en aprender cómo operan las instalaciones de energía y obtener acceso a los sistemas operativos, atacaron a socios vulnerables de la cadena de suministro y trabajaron aguas arriba para obtener acceso a servicios públicos (obtener credenciales de red e instalar puertas traseras en las computadoras)[15].
En julio de ese año, Cisco advierte sobre ataques basados en correo electrónico dirigidos al sector de la energía utilizando un conjunto de herramientas llamado Phishery[16].

Ilustración 3: Resumen de las actividades del grupo Dragonfly en el sector energético. Fuente: Symantec

Año 2018: los investigadores de ESET Anton Cherepanov y Robert Lipovsky publicaron un estudio en el que se revelan detalles de un nuevo actor malicioso apodado GreyEnergy, quien al parecer es el sucesor de BlackEnergy. El primer

[14] http://uk.reuters.com/article/us-nuclearpower-cyber-germany-idUKKCN0XN2OS
[15] https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
[16] https://blog.talosintelligence.com/2017/07/template-injection.html

ataque de este grupo lo habría registrado una compañía eléctrica de Polonia a finales de 2015, pero la mayoría de ciberataques se han concentrado en Ucrania, al igual que ocurrió con BlackEnergy. Además del sector eléctrico, otras infraestructuras críticas, como el transporte público, se habrían visto afectadas[17].

Año 2019: Expertos en ciberseguridad de la firma FireEye[18] publicaron un informe explicando que el malware Triton había sido utilizado de nuevo, después del ataque de 2017, para comprometer una instalación de infraestructura crítica, aún no revelada. La amenaza está diseñada para explorar las redes del objetivo y sabotear sus Sistemas de Control Industrial, a menudo utilizados en centrales eléctricas y refinerías de petróleo y, de esta manera, obtener control en las operaciones de la instalación[19].

Año 2020: En el mes de abril, el grupo energético EDP sufrió un ataque informático[20]. El periódico Jornal de Notícias comentó que los atacantes declararon haber extraído 10 terabytes de información de los servidores del grupo empresarial, y para demostrarlo publicaron algunas imágenes de los archivos. La compañía tuvo que desactivar el acceso a su red privada virtual (VPN) como medida preventiva. Los cibercriminales pidieron a EDP 10 millones de euros a pagar en bitcoins para no hacer pública la información que le habrían robado.

Además de estos incidentes, ha habido más ataques bien documentados contra el sector energético; algunos de los virus, malware y demás acciones intrusivas detectadas se describen el documento de Symantec: Targeted Attacks Against the Energy Sector[21].

Las amenazas de ciberataques no solo se registran en las redes de transporte y distribución eléctrica; **se tienen grandes desafíos en las redes inteligentes y los medidores inteligentes**. Estos últimos permiten medir la energía de consumo a un nivel más granular, creando mejores patrones de flujo y permitiendo diferentes precios para cada perfil de consumo.

---

[17] https://www.welivesecurity.com/la-es/2018/10/17/greyenergy-actores-maliciosos-peligrosos-arsenal-actualizado/

[18] https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html

[19] https://www.dailymail.co.uk/sciencetech/article-6913775/Experts-warn-hackers-murderous-malware-Triton-targeting-critical-infrastructure.html

[20] https://cincodias.elpais.com/cincodias/2020/04/14/companias/1586887179_127560.html

[21] https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf

Además del problema de asegurar estos dispositivos, las redes inteligentes producen una gran cantidad de datos que, dependiendo de las reglamentaciones, deberá mantenerse para las auditorías. Algunos de estos datos pueden ser confidenciales y podrían generar problemas de privacidad si no se protegen adecuadamente. Esto podría convertirse fácilmente en petabytes de datos que deberán almacenarse y administrarse de forma segura.

De acuerdo a la revista PVTECH, se ha calculado que una **planta fotovoltaica**, con una capacidad instalada de **500 MW,** con los actuales sistemas de control y monitorización genera casi **8 GB de datos por segundo**[22].

De acuerdo a Symantec, **los ataques no pueden atribuirse a un solo grupo o región geográfica**. Algunos de los ataques han sido puramente oportunistas, buscando cualquier información valiosa disponible. Los atacantes tienden a buscar información valiosa, incluidos mapas de nuevos campos de gas o investigaciones sobre la eficiencia en generadores fotovoltaicos.

Las amenazas se detectan principalmente en los siguientes sistemas:

- Sistemas de Tecnología de la Información (TI) que soportan funciones administrativas y de negocios de "back office".
- Los sistemas de Tecnología de la Operación (OT) que monitorizan y administran las redes de energía, incluidas las fuentes de generación, redes de transmisión y distribución y también activos energéticos basados en el consumidor, incluidos los puntos de carga domésticos y contadores inteligentes.
- Los sistemas de comunicaciones que proporcionan inteligencia en red a través de OT, IT y que a menudo también están interconectados con otras redes de comunicaciones públicas y privadas.

A medida que los ataques cibernéticos contra el sector energético aumentan tanto en frecuencia como en destructividad**, las energías renovables se convierten en un objetivo**. Las energías renovables tendrán que enfrentar la realidad de sus vulnerabilidades y reconocer la importancia de invertir en defensa cibernética.

Descartar estas inversiones financieras como perjudiciales para su competitividad podría provocar pérdidas catastróficas.

[22] https://store.pv-tech.org/store/big-data-and-predictive-maintenance-in-pv-the-state-of-the-art/

4. Ataques cibernéticos en el sector de las energías renovables

Los sistemas de control de supervisión y adquisición de datos (**SCADA**) responsables de monitorizar y controlar las instalaciones de energía renovable a menudo tienen **vulnerabilidades** que los hacen susceptibles a los ataques cibernéticos. Estas vulnerabilidades permiten a los atacantes inmiscuirse en los parques eólicos y fotovoltaicos.

De acuerdo a un artículo de la empresa DNV GL[23], investigadores de la Universidad de Tulsa informaron que les tomó menos de un minuto abrir las cerraduras de la puerta de una turbina sin supervisión y obtener acceso al servidor no seguro. A través del servidor de esa turbina accedieron instantáneamente a las direcciones IP de todas las turbinas conectadas a la red. Indican que los parques eólicos en alta mar son más vulnerables a los ataques informáticos.

En una publicación reciente, la revista PVMAGAZINE, indica que dentro de las instalaciones **fotovoltaicas**, los equipos **inversores son un punto débil** de acceso[24]. "Son un objetivo principal de un pirata informático, porque son accesibles y realizan muchas funciones inteligentes para mantener la estabilidad y la eficiencia"… "son el corazón del sistema fotovoltaico" o dicho de otra forma, **son el eslabón más débil**. Se pueden apagar, sobrecargar las baterías si el sistema cuenta con almacenamiento de energía o causar importantes inestabilidades de la red. Los investigadores también creen que un ataque cibernético en una planta solar con almacenamiento podría conducir a la destrucción o un daño irreparable de las baterías, lo que a su vez podría provocar un incendio.

Por otra parte, la publicación señala que los inversores de "string" no son necesariamente más vulnerables que los inversores centrales. Los hackers escriben código para hacer "ping[25]" al sistema en general e intentan encontrar el punto más débil. Por tanto, recorrerán toda la red hasta encontrar la puerta de entrada más conveniente para sus fines.

Respecto a la protección de los inversores ante ciberataques, apuntan que no hay estándares sobre ello, pero que the Solar Energy Technologies Office of the Department of Energy está invirtiendo recursos en esta investigación. Quieren hacer avanzar a la industria en este aspecto mientras también mantienen bajos los costes.

[23] https://www.dnvgl.com/article/why-windfarms-need-to-step-up-cyber-security-128082
[24] https://pv-magazine-usa.com/2020/04/21/solar-inverters-vs-cyberattacks/
[25] https://es.wikipedia.org/wiki/Ping

Hay muchas instalaciones de energía renovable antiguas, en especial parques eólicos con sistemas de comunicación que fueron diseñados sin contemplar una "seguridad en el diseño de la red". En el caso de los parques fotovoltaicos con antigüedad alrededor de los 10 años, quizá sea mejor esperar a una pronta renovación de los inversores para actualizar la seguridad de estos.

También la seguridad física a menudo no se ha cubierto lo suficiente en el diseño de las instalaciones, lo que resulta en deficientes sistemas de vigilancia, mala calidad de las cerraduras, además, el acceso remoto de los proveedores no siempre se gestiona correctamente, los enlaces de comunicación se contratan a diferentes proveedores y se tienen protocolos de comunicación obsoletos sin mejoras de seguridad y/o actualización de los ordenadores.

5. Auditorías y herramientas de protección

Gran parte de las empresas no conocen sus vulnerabilidades ante ciberataques, hasta que una empresa especializada audita sus sistemas, redes de datos y arquitecturas de comunicación.

GE Renewable Energy[26] indica que al auditar a sus clientes ha encontrado lo siguiente:

- ✓ El 96% tenía al menos un equipamiento con un sistema operativo vulnerable.
- ✓ El 92% presentó al menos un sistema con una solución de punto final expirado.
- ✓ El 88% no tenía implementada las mejores prácticas de acceso de usuarios..
- ✓ El 96% contaba al menos con un sistema de "doble alojamiento" (eludiendo el firewall).
- ✓ El 8% tenía al menos un sistema donde se detectó malware.
- ✓ El 0% contaba con un sistema efectivo de monitoreo de ciberseguridad.
- ✓ 12 años fue el periodo de mayor duración que no se cambió la contraseña del administrador.

En recientes fechas, **AEMER** organizó un Coloquio Virtual Gratuito con el título: **Ciberseguridad Operativa en servicios remotos y Cobertura de riesgos existentes**[27]. Los temas que se desarrollaron fueron: Empresa ALTRAN - modelado PILAR (niveles de riesgo, identificación y clasificación de activos críticos), políticas y procesos y estrategia de gestión de crisis; Empresa ENIGMEDIA - herramientas para proteger dispositivos y redes en infraestructuras críticas. Recomendamos visitar la página de **AEMER** (www.aemer.org) para visualizar las interesantes exposiciones.

[26] https://www.ge.com/power/services/automation-controls/cyber
[27] https://www.youtube.com/watch?v=0xMcJ0izjCg

En dicho Coloquio se resaltó la importancia de analizar los sistemas desde un enfoque holístico (los sistemas y sus propiedades deben ser inspeccionados en su conjunto y no sólo a través de las partes que los componen), ya que puede proporcionar una validación técnica eficiente desde una perspectiva de extremo a extremo. Empezando por los dispositivos conectados a Internet y especialmente los que tienen acceso remoto.

Los parques fotovoltaicos y eólicos son administrados por sistemas de control industrial que interconectan equipos inversores o turbinas individuales, subestaciones y otros equipos a unas cuantas computadoras. Muchos de estos sistemas fueron **diseñados teniendo en cuenta la eficiencia, pero no la seguridad informática**.

Asimismo, cada vez se incorporan **dispositivos IoT** (Internet de las cosas) a estas redes de gestión, lo que permite tener una red "más inteligente" y más rentable, pero también **aumenta su vulnerabilidad** a los piratas informáticos.

La red de telefonía 5G tendrá una amplia cobertura progresivamente y será la responsable de la "explosión del mercado IoT". Un informe de la Agencia de Ciberseguridad de la UE (ENISA) advierte que las **redes 5G** estarán más basadas en software que las anteriores generaciones. Esto significa que podrían tener **más vulnerabilidades** derivadas de una mala praxis en el desarrollo del programa.

Existen productos de **protección de activos de energía renovable que aseguran los puntos de entrada de los parques eólicos y FV, las redes SCADA y los controladores de equipos.** Son productos que están diseñados para proteger de amenazas internas y externas. En el mercado se pueden encontrar diferentes servicios de protección, que van desde actualizaciones mínimas de seguridad hasta reemplazos de hardware a gran escala.

Principalmente se ofrece:

- ✓ reducir el riesgo del tiempo de inactividad.
- ✓ prevenir daños a la reputación y el robo de propiedad intelectual.
- ✓ mantener el rigor operativo para lograr las mejores prácticas.
- ✓ actualizaciones que los sistemas que detectan amenazas de intrusión.
- ✓ actualización de hardware en servidores y redes SCADA.

La siguiente ilustración muestra un esquema general de las redes SCADA de gestión y monitorización de un parque eólico, pero puede aplicar también para uno fotovoltaico:

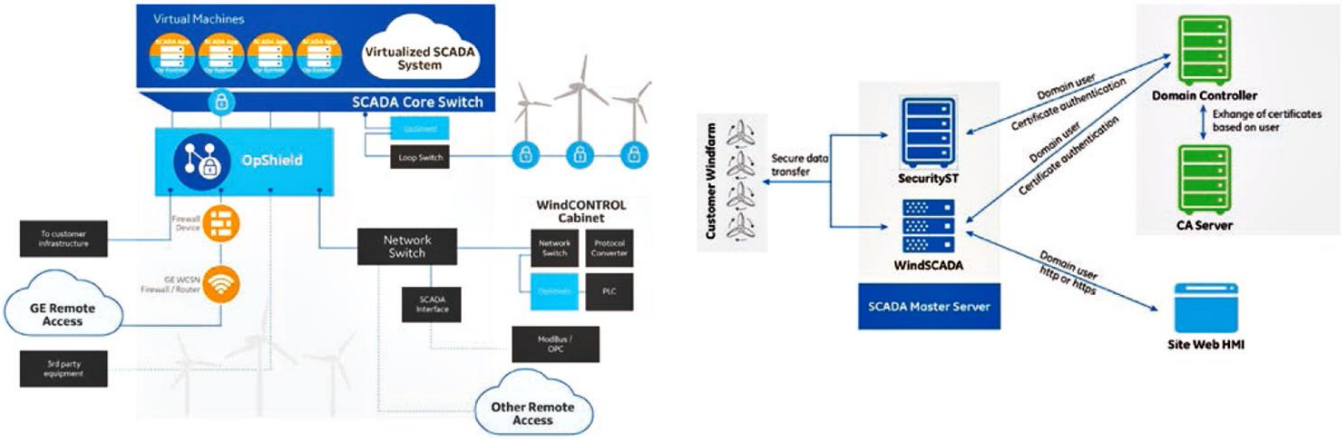

Ilustración 4: WindSCADA Secure Fuente: GE Renewable Energy

No hay una única solución para lograr una protección total contra los ataques cibernéticos. La red inteligente sigue siendo una red de máquinas de IT / OT con flujos de datos entre ellas.

La industria de las energías renovables también necesita trabajar más estrechamente con las instituciones gubernamentales para protegerse contra los ataques. La mayoría de las redes de energía están en manos privadas y es crucial construir asociaciones público-privadas para abordar la dimensión cibernética de la seguridad energética.

En el Coloquio Virtual Gratuito **AEMER**: Ciberseguridad Operativa en servicios remotos y Cobertura de riesgos existentes[28], la Correduría de seguros Campos&Rial expuso las siguientes **recomendaciones en el teletrabajo**:

- Utilizar, siempre que sea posible, dispositivos de empresa, con sus limitaciones correspondientes, con antivirus instalado y actualizado y todo el software actualizado.
- VPN Red privada virtual (Túnel entre oficina y viviendas de los empleados, con información cifrada y autenticación de doble factor, ej. código SMS a móvil).
- Contraseñas robustas, privadas y con cambios periódicos.
- Redes WiFi privadas (nunca públicas), cambiar el nombre del router y la contraseña que vienen por defecto.
- Copias de seguridad periódicas (diarias, semanales) almacenadas en otros servidores fuera de la propia red o en la nube.
- Actualizaciones periódicas de software.

[28] https://www.youtube.com/watch?v=0xMcJ0izjCg

Las **principales consecuencias de un ciberataque** son:

- Contratación de expertos que mitiguen el daño.
- Pérdida de datos.
- Pérdida de beneficios por interrupción parcial o total del sistema informático de la empresa.
- Pago de rescates.
- Servicios de control de identidad.
- Costes de notificación.
- Gastos de investigación.
- Sanciones.
- Reclamaciones de terceros (Gastos de defensa, indemnizaciones).
- Gastos para restaurar la pérdida de imagen y reputación.

6. Minoración de daños a través de pólizas de seguros.

Un **seguro de Ciberriesgos cubre a las empresas frente** a:

- Ataques cibernéticos o vulneraciones de seguridad: Recuperación de los datos y reparación o sustitución del software.
- Robo de datos: Investigación del origen y alcance de la divulgación no autorizada de datos, recuperación de datos y gestión del incidente, si se trata de información sensible o confidencial.
- Responsabilidad civil frente a terceros: por divulgación no autorizada de datos confidenciales o de carácter personal o por publicación de contenido digital a través de cuentas hackeadas.
- Paralización del negocio: Actuación de emergencia y contingencia por la interrupción parcial o total del sistema informático de la empresa, causada por un ataque cibernético o vulnerabilidad en los propios sistemas o también en los sistemas de proveedor externo tecnológico.
- Extorsión: Gestión del incidente (secuestro, suplantación web, ransomware) y desbloqueo de equipos.
- Fraude: Robo o suplantación de identidad, fraude o ataque al CEO, acceso a cuentas bancarias (Ciberdelito), hacking telefónico.

Para conocer con más detalle las coberturas y primas, recomendamos visitar la página de AEMER (www.aemer.org) para visualizar dicho Coloquio.

7. El teletrabajo incrementa la vulnerabilidad de las empresas

La implementación "temporal" del trabajo a distancia como medida gubernamental para prevenir la propagación del coronavirus (Covid-19) ha incrementado la vulnerabilidad de las empresas ante **amenazas cibernéticas que ya estaban latentes previamente**. Este esquema laboral del **teletrabajo podría quedarse instaurado** en una parte importante de la fuerza laboral; si no en toda la jornada laboral, si en momentos en los cuales el beneficio de evitar el transporte a la oficina sea más rentable.

Este esquema de trabajo llegó de forma intempestiva y su precipitada instauración, se traduce en **acciones de implementación a contrarreloj**, en que la gran mayoría de los empleados no tienen a su disposición las herramientas de protección necesarias y muchas veces utilizan para trabajar equipos personales con mínima o nula defensa ante ataques cibernéticos; en el mejor de los casos emplean ordenadores de la empresa que interactúan con sistemas neurálgicos de la compañía a través de redes inalámbricas domésticas, sin una configuración robusta de cortafuegos, con una arquitectura de red endeble, sin procesos de encriptación de datos, ni validación de credenciales y por tanto, **una alta vulnerabilidad a los ciberataques**. Es decir, se pierde o complica el control del entorno de trabajo del usuario.

También se evidenció que es **necesario actualizar las "políticas, prácticas y metodologías" de acceso remoto a la empresa y/o sistemas de gestión remota con multiusuarios bajo diversas circunstancias de conexión**. Algunas empresas olvidan contemplar estos procesos en los planes de continuidad de negocio y eso aumenta el riesgo de fuga y quiebra de información.

8. Ciberataques dentro de la pandemia Covid-19

Lamentablemente **durante la pandemia del Covid-19 ha habido una gran cantidad de ciberataques.** En España, a finales de marzo, la Policía Nacional detectó un ciberataque al sistema informático de los hospitales, se bloquearon ordenadores mediante el envío al personal sanitario de correos electrónicos con un virus ransomware (Netwalker) que pretendía "romper" el sistema informático de los centros médicos en plena crisis sanitaria.

El 12 de marzo hubo un ataque contra una organización sanitaria en Illinois (Estados Unidos), Champaign Urbana Public Health District, que les bloqueó la página web y

debieron crear una alternativa. Este ransomware fue encontrado también en febrero en un ciberataque contra Toll Group, una empresa australiana de logística.

A inicios de abril, varias organizaciones gubernamentales a nivel mundial advirtieron sobre la vulnerabilidad cibernética de la popular aplicación de videoconferencia 'Zoom', utilizada por decenas de miles de profesionales que trabajan desde su casa; se advirtió que el uso en ese momento era inseguro ya que permitía a los ciberdelincuentes acceder a información confidencial como detalles de reuniones y conversaciones. A las 24 hrs, la aplicación Zoom respondió que la vulnerabilidad de los enlaces UNC se había resuelto.

También en abril, la Organización Mundial de la Salud informó que unas 450 direcciones de correo electrónico y contraseñas activas de la OMS se filtraron en línea junto con miles de otras personas que trabajan en la nueva respuesta de coronavirus. También advirtieron de estafadores que suplantan a la OMS en correos electrónicos (campañas de phishing) para canalizar las donaciones a un fondo ficticio.

A finales de abril, en España se advertía por las autoridades, que debido al temor y la incertidumbre de la crisis económica, los usuarios son más susceptibles de confiar en mensajes o correos electrónicos que antes pasarían inadvertidos. Los delincuentes enviaron cientos de emails haciéndose pasar por el Organismo Estatal de Inspección de Trabajo y Seguridad Social (ITSS) comunicando a las empresas una falsa investigación de la Inspección de Trabajo. También se hicieron pasar por el Servicio Público de Empleo Estatal (SEPE) y enviaron mensajes a dispositivos móviles comunicando la aprobación de un ERTE en la empresa del usuario y solicitando información bancaria, como el número de cuenta, para completar la gestión.

Conclusiones

El **sector energético** está experimentando **cambios a una escala y ritmo sin precedentes**. El nuevo sistema de energía inteligente **requiere un uso significativamente mayor de las Tecnologías de Información y Comunicación** (TIC) en los rubros de la digitalización de la producción y distribución de la energía.

Esta revolución requiere una amplia expansión de dispositivos inteligentes, por tanto, el rango de posibles ataques **(o "vectores de amenaza") se multiplica dentro de los ecosistemas de la energía inteligente y renovable**. El **sector energético es un objetivo claro y creciente para los ataques cibernéticos,** presentando **mayor vulnerabilidad los sistemas SCADA** que gestionan los sistemas de generación eléctrica renovable.

Los ataques cibernéticos contra el sector energético aumentan tanto en frecuencia como en destructividad, **muchos de ellos se conocieron después de muchos años.** Ataques cibernéticos a grandes instalaciones de energía renovable **pueden causar daños considerables en infraestructuras críticas interdependientes** si se hacen a una escala significativa o cuando se combinan con otros ataques.. Esto podría conducir a un desequilibrio importante de carga en las subestaciones de transmisión, desencadenando una falla en cascada a través de la red eléctrica.

También hay que tener en cuenta que las redes de gestión producen una gran cantidad de datos que pueden ser confidenciales y podrían generar problemas de privacidad si no se protegen adecuadamente. Una **planta fotovoltaica**, con una capacidad instalada de **500 MW,** con los actuales sistemas de control y monitorización genera casi **8 GB de datos por segundo.**

Las energías renovables se convierten en un objetivo y tendrán que enfrentar la realidad de sus vulnerabilidades y reconocer la importancia de invertir en defensa cibernética.

Los parques fotovoltaicos y eólicos son administrados por sistemas de control industrial, muchos de ellos son antiguos y fueron **diseñados teniendo en cuenta la eficiencia, pero no la seguridad informática**.

Asimismo, cada vez se incorporan **dispositivos IoT** (Internet de las cosas) a estas redes de gestión, lo que permite tener una red "más inteligente" y más rentable, pero también **aumenta su vulnerabilidad**.

La seguridad física a menudo no se ha cubierto lo suficiente en el diseño de las instalaciones, lo que resulta en **deficientes sistemas de vigilancia** y se tienen sistemas obsoletos sin mejoras de seguridad y/o actualización de los ordenadores.

También es **necesario actualizar las "políticas, prácticas y metodologías" de acceso remoto a la empresa y/o sistemas de gestión remota con multiusuarios bajo diversas circunstancias de conexión**. Algunas empresas olvidan contemplar estos procesos en los planes de continuidad de negocio y eso aumenta el riesgo de fuga y quiebra de información.

Además de las inversiones en infraestructuras técnicas más robustas, se pueden proteger los activos renovables y las empresas de gestión con pólizas de seguro que ofrecen una amplia cobertura ante daños y perjuicios de un ciberataque.

Finalmente, la mayoría de las redes de energía están en manos privadas y es crucial construir asociaciones público-privadas para abordar la dimensión cibernética de la seguridad energética.

Los ciberdelicuentes no reducen sus acciones mientras el mundo industrial para o reduce sus actividades, al contrario, saben que muchos sistemas son vulnerables desde hace tiempo, pero bajo el contexto operativo del teletrabajo, se incrementan las posibilidades de hacerse con el control, interrumpir o dañar la funcionalidad de los sistemas informáticos. Por ello, el sector energético, pero en especial el de las energías renovables, debe de redoblar esfuerzos para proteger las instalaciones, tanto antiguas como todas las que están en operación a partir de este nuevo boom energético distribuido, renovable e inteligente.

ANEXO - Iniciativas de seguridad cibernética en España

En el año 2012, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) que se creó en el año 2006 con la misión era impulsar y desarrollar proyectos de innovación en el sector de las Tecnologías de la Información y la Comunicación, focalizó su actividad en el ámbito de la ciberseguridad de forma específica, para pasar en 2014 a denominarse Instituto Nacional de Ciberseguridad (INCIBE)[29], a raíz de la evolución de los riesgos globales y de las ciberamenazas. INCIBE es una sociedad dependiente del Ministerio de Economía y Empresa, a través de la Secretaría de Estado para el Avance Digital, es la entidad de referencia en el desarrollo de la ciberseguridad y la confianza digital de ciudadanos y empresas, especialmente aquellas que gestionan infraestructuras críticas. También es el motor de transformación social y oportunidad para la innovación, formando parte de la Estrategia de Ciberseguridad Nacional orientada a la protección del ciberespacio.

Actualmente, INCIBE a través de su portal pone a disposición de empresarios y empleados de pymes así como de colectivos específicos, asociaciones y colegios profesionales, **herramientas de ciberseguridad**[30] enfocadas a la prevención, detección y respuesta a incidentes.

Asimismo se cuenta con el CCN-CERT [31], que es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y su misión, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Por otro lado, existe el Foro CSIRT.es [32], que es una plataforma independiente de confianza y sin ánimo de lucro compuesto por aquellos equipos de respuesta a incidentes de seguridad informáticos cuyo ámbito de actuación o comunidad de usuarios en la que opera, se encuentra dentro del territorio español.

[29] https://www.incibe.es/
[30] https://www.incibe.es/protege-tu-empresa/herramientas
[31] https://www.ccn-cert.cni.es/
[32] https://www.csirt.es/index.php/es/

Finalmente, España cuenta con el Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC)[33]. Este Centro custodiará y actualizará el Plan de Seguridad de Infraestructuras Críticas y el Catalogo Nacional de Infraestructuras Críticas. Ante una situación de crisis: El operador designado del CNPIC comunicara a las unidades de inteligencia competentes y en caso de crisis ante el equipo de respuesta ante emergencias (CERT).

Entre estas instalaciones sensibles destacan las centrales y redes de energía, las comunicaciones, las finanzas, el sector sanitario, la alimentación, el agua -embalses, almacenamiento, tratamiento y redes-, los transportes -aeropuertos, puertos, etc-, monumentos nacionales, así como la producción, almacenamiento y transporte de mercancías peligrosas, como material químico, biológico o nuclear.

Acerca de AEMER

AEMER es la Asociación de Empresas de Mantenimiento de Energía Renovable que se consolida como un punto de encuentro de expertos vinculados a los servicios de O&M, con la misión de impulsar el debate, desarrollar estándares, homogenizar procesos - prácticas y ofrecer alternativas de crecimiento ante los nuevos desafíos. Cada día trabaja para posicionarse dentro del sector renovable como referente a nivel técnico y fomentar la calidad en toda la cadena de valor de los servicios de mantenimiento.

AEMER tiene entre sus principales objetivos elaborar documentos, guías sobre procedimientos de diagnóstico y buenas prácticas, fomentar el intercambio de experiencias e información entre sus socios y los agentes del sector en general a través de diferentes seminarios y jornadas técnicas. Actualmente AEMER cuenta con más de 30 asociados en un contexto de creciente importancia de la actividad de mantenimiento.

Para más información contacte:

Nacho Hernández - info@aemer.org +34 687 725 011

Alejandro Guillén Olague – aguillen@aemer.org +34 671 604 132

[33] https://www.intelpage.info/centro-nacional-de-proteccion-de-infraestructuras-criticas8.html