La ciberseguridad en el sector energético

Ana I. Ayerbe | Directora del Área de Negocio TRUSTECH de Tecnalia | @AnaAyerbe

Tema

Nuestra economía y sociedad dependen del sector energético y debemos asegurar su resiliencia ante incidentes de ciberseguridad.

Resumen

Las economías desarrolladas dependen para su funcionamiento de la energía en sus diferentes formas. Por este motivo, el objetivo de las infraestructuras energéticas es ofrecer un suministro de energía continuo e ininterrumpido, y esto sólo puede lograrse si la cadena energética, desde la generación al suministro, funciona apropiadamente y de forma segura.

La resiliencia es un reto para cualquier organización, pero, dadas las características del sector de la energía y su importante papel en nuestra economía y sociedad, es de vital importancia la resiliencia del ecosistema energético ante ciberataques.

Análisis

Cuando hablamos de la energía, estamos hablando de la electricidad, el gas y el petróleo, fundamentalmente, y, si hablamos de la distribución de energía, estamos hablando de infraestructuras que ofrecen unos servicios que posibilitan el normal funcionamiento de otras industrias y de la vida ciudadana. No tenemos más que pensar en las redes eléctricas inteligentes (s*mart grid*s), que proporcionan suministro eléctrico a infraestructuras pertenecientes a otros sectores, como el de la salud, el transporte, las telecomunicaciones o la banca, entre otros.

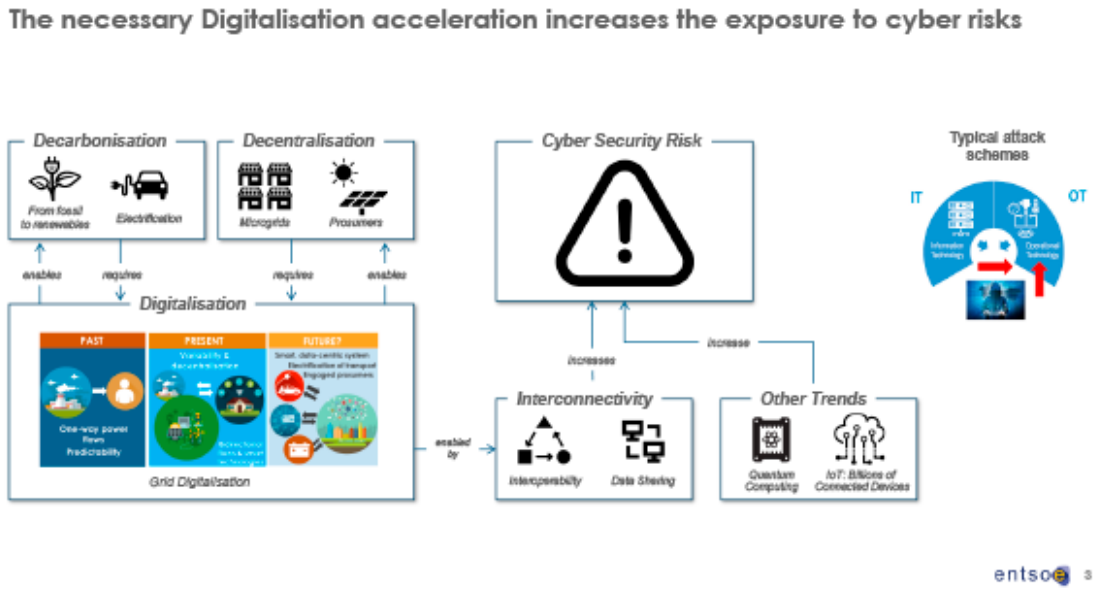
Una interrupción del suministro eléctrico puede dejarnos sin luz durante un determinado tiempo, con las consiguientes incomodidades, pero si se alarga la interrupción del servicio puede impactar en servicios ofrecidos por otros sectores. El efecto en cascada puede afectar no sólo a otros sectores, sino también a otras redes e incluso a otros países, dada la interconexión de las redes energéticas. En este efecto en cascada debe resaltarse la estrecha relación de interdependencia que existe entre las *smart grids* y las redes de telecomunicaciones, ya que, si las *smart grids* ofrecen a las redes la energía necesaria para su funcionamiento, las redes de telecomunicaciones son también necesarias para el buen funcionamiento de las *smart grids*, y esta relación será cada vez más dependiente a medida que la tecnología 5G vaya implantándose en el mundo industrial.

A la importancia del sector energético para nuestra economía y sociedad hay que añadir que el mundo de las *utilities* y de las redes eléctricas se está enfrentando a retos de gran calado, como la descarbonización mediante la reducción al máximo de los combustibles fósiles, la descentralización mediante tecnologías de control descentralizadas y la digitalización en toda la cadena de valor, desde la generación y la distribución hasta llegar al consumidor. La generación renovable y distribuida en baja tensión, la energía solar fotovoltaica, el almacenamiento y el vehículo eléctrico, conectados todos ellos en los puntos de consumo, son auténticas tendencias del sector. A esto hay que añadir el nuevo papel de los consumidores, que ahora no sólo pueden consumir energía, sino también producirla, lo que implica cambios en la relación con las compañías y en el modelo de negocio de las distribuidoras, convirtiéndolas en facilitadores de mercado que explotan la gran cantidad de información de la que disponen y ofrecen nuevos servicios relacionados de alto valor añadido[1].

Merece especial atención la integración de los dispositivos inteligentes y la Internet de las Cosas (IoT), ya que el volumen de los dispositivos electrónicos que se integrarán o conectarán a las redes eléctricas inteligentes aumentará exponencialmente en los próximos años. Los vehículos eléctricos, que precisarán equipamiento específico que integrar en la infraestructura, como estaciones y puestos de recarga, y la generación eólica o la distribuida con paneles fotovoltaicos domésticos, entre otros, son algunos ejemplos. Y, ya que la conexión de dispositivos IoT aumentará los riesgos de las *smart grids*, debemos pensar en cómo considerar su seguridad desde el diseño para evitar ataques masivos desde dispositivos IoT provenientes, por ejemplo, de los sistemas de control de la humedad, el vapor y el aire acondicionado (HVAC) instalados en hogares y organizaciones.

[1] Ángel Díaz Gallo (2017), "La digitalización afecta a toda la cadena de valor de la distribución de energía". *INN* (Tecnalia), n.º 2, diciembre de 2017, https://www.tecnalia.com/images/stories/Tecnalia_INN/TECNALIA_INN_DICIEMBRE2017_CAST.pdf.

Figura 1. La digitalización acelera la exposición a ciberriesgos



Fuente: Nicolas Richet (CIO-ENTSO-E), "Cybersecurity & Energy in Europe", p. 3, https://energy-community.org/events/2019/04/CYBER.html.[2]

Garantizar la resiliencia de las empresas del sector energético ante diferentes tipos de incidentes que puedan producirse, tanto de seguridad física como de ciberseguridad o una combinación de ambos, es fundamental. Las organizaciones de inteligencia estadounidenses incluyeron los ciberataques a su red eléctrica como una de las mayores amenazas a la seguridad nacional a principios del 2019[3], año en el que estadounidenses y rusos han cruzado acusaciones relacionadas con intentos de hackeo de sus redes eléctricas[4], llegando a hablar de iniciar una ciberguerra[5]. Podríamos pensar que ya estamos en ese tipo de escenario si echamos un vistazo al histórico de ciberataques que se han venido produciendo en los últimos años en sistemas de control industrial del sector energético, según la Figura 2, de Deloitte.

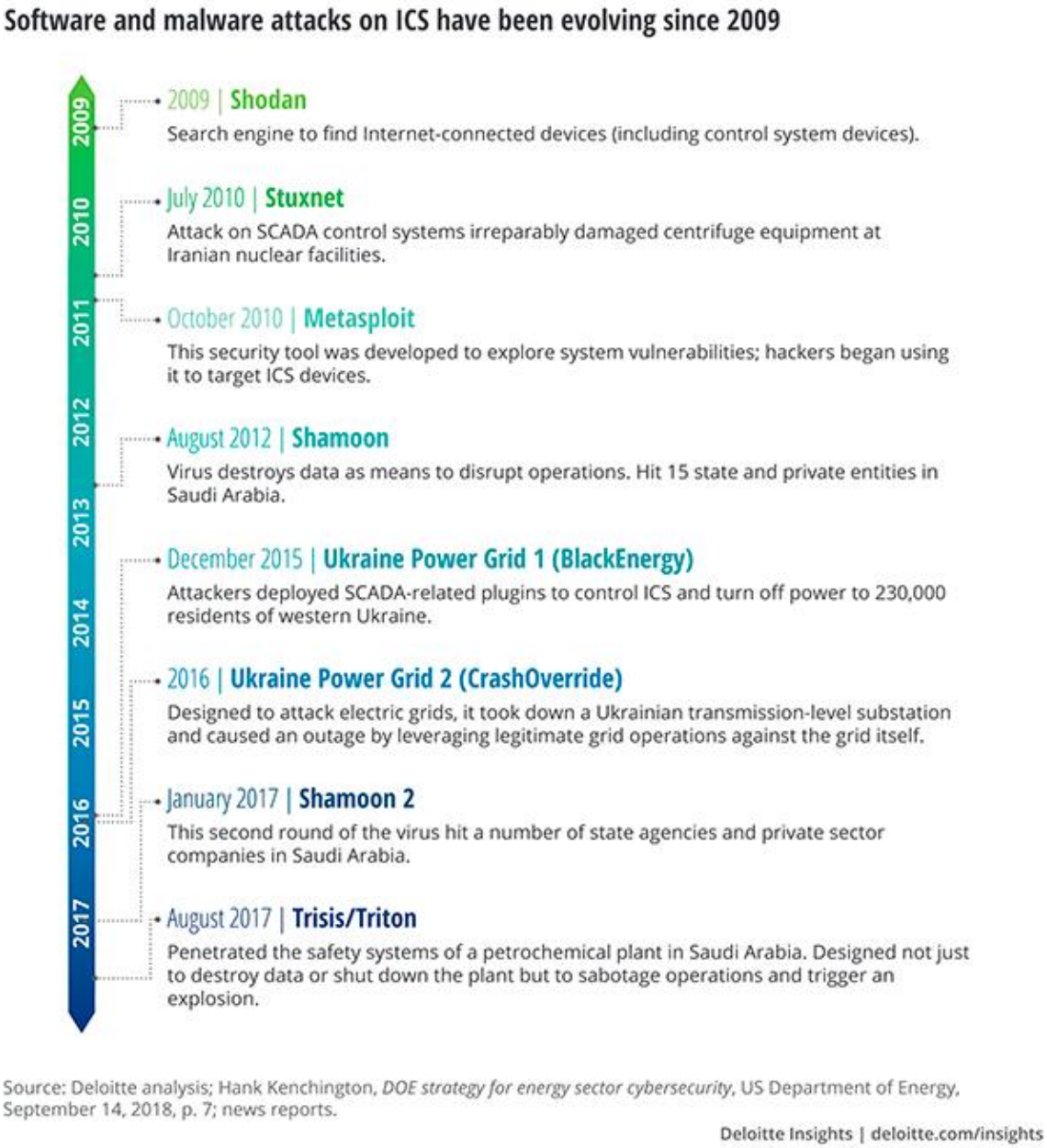
[2] Presentación realizada en el Cybersecurity Day in the Energy Community en Viena (Austria), 11 de abril de 2019, https://energy-community.org/news/Energy-Community-News/2019/04/12.html.

[3] Danny Bradbury (2019), "Electricity Grid Hacking Makes US Top Threat List", *Info Security*, 15/II/2019, https://www.infosecurity-magazine.com/infosec/electricity-grid-hacking-makes-us-1-1/.

[4] Andy Greenberg (2019), "The Highly Dangerous 'Triton' Hackers Have Probed the US Grid". *Wired*, 14/VI/2019, https://www.wired.com/story/triton-hackers-scan-us-power-grid/.

[5] Ivan Nechepurenko (2019), "Kremlim Warns of Cyberwar After Report of U.S. Hacking into Russian Power Grid". *The New York Times*, 17/VI/2019, https://www.nytimes.com/2019/06/17/world/europe/russia-us-cyberwar-grid.html.

Figura 2. Ciberataques en empresas energéticas



Fuente: Steve Livingston y otros (2019), “Managing Cyber Risk in the electric Power Sector”. *Deloitte Insights*, 31/I/2019, https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html.

¿Cuál es la situación en España?

Según un informe del Centro de Ciberseguridad Industrial (CCI) realizado en colaboración con Check Point, los sectores donde se conocen más tipos diferentes de incidentes son la electricidad, el gas y el petróleo (Figuras 3, 4 y 5)[6]. Por otro lado, un 41% de las organizaciones encuestadas piensan además que en el futuro un número importante de incidentes vendrán de dispositivos IoT comprometidos y, en menor medida, de los ataques multivector y del *ransomware* de operación.

Figura 3. Tipos de incidentes

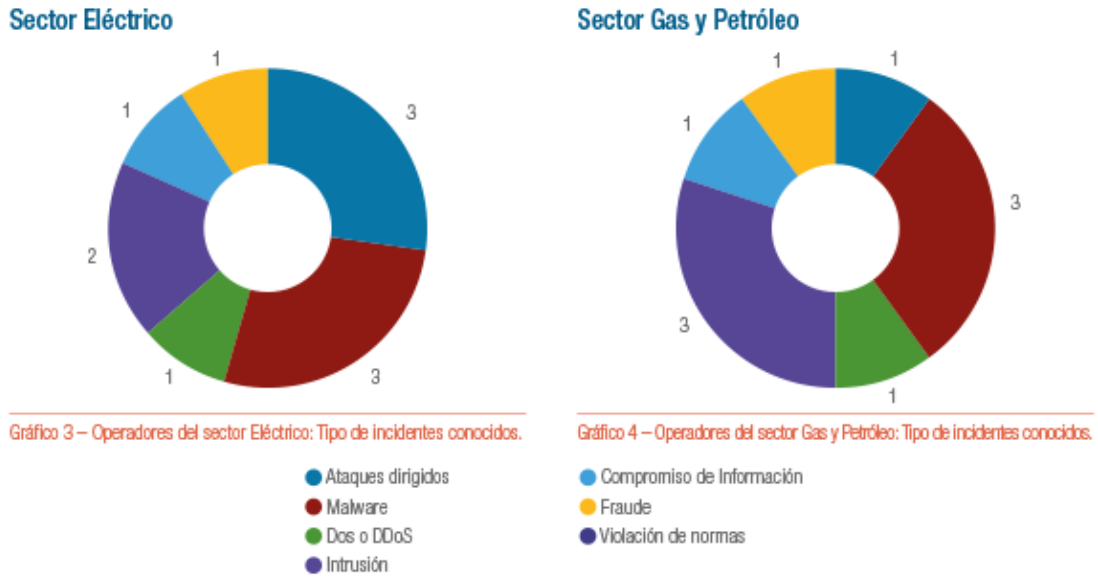
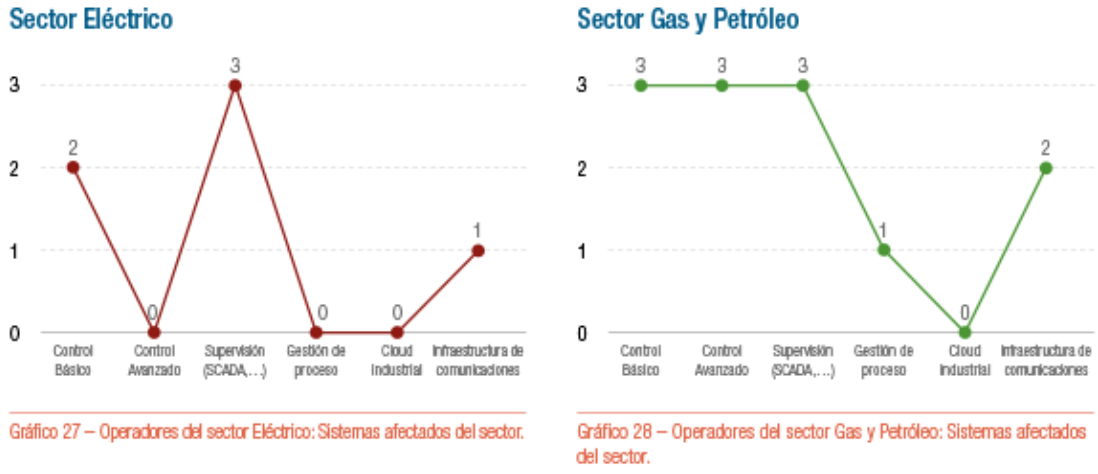


Figura 4. Sistemas afectados por incidentes



[6] CCI y Check Point Software Technologies, "Incidentes de Ciberseguridad Industrial en Servicios Esenciales de España", mayo de 2019, https://cybersecuritynews.es/wp-content/uploads/2019/10/Check-Point_Informe-incidentes-de-ciberseguridad-en-infraestructuras-cri%CC%81ticas-en-Espan%CC%83a.pdf.

Según dicho informe, casi un 30% de los profesionales encuestados consideran que una de las principales consecuencias de un incidente de ciberseguridad puede ser la pérdida de un servicio esencial, dado que las tecnologías industriales que operan los servicios esenciales no han incorporado requisitos de ciberseguridad, lo que las hace vulnerables a comportamientos no esperados.

Figura 5. Impacto de los incidentes

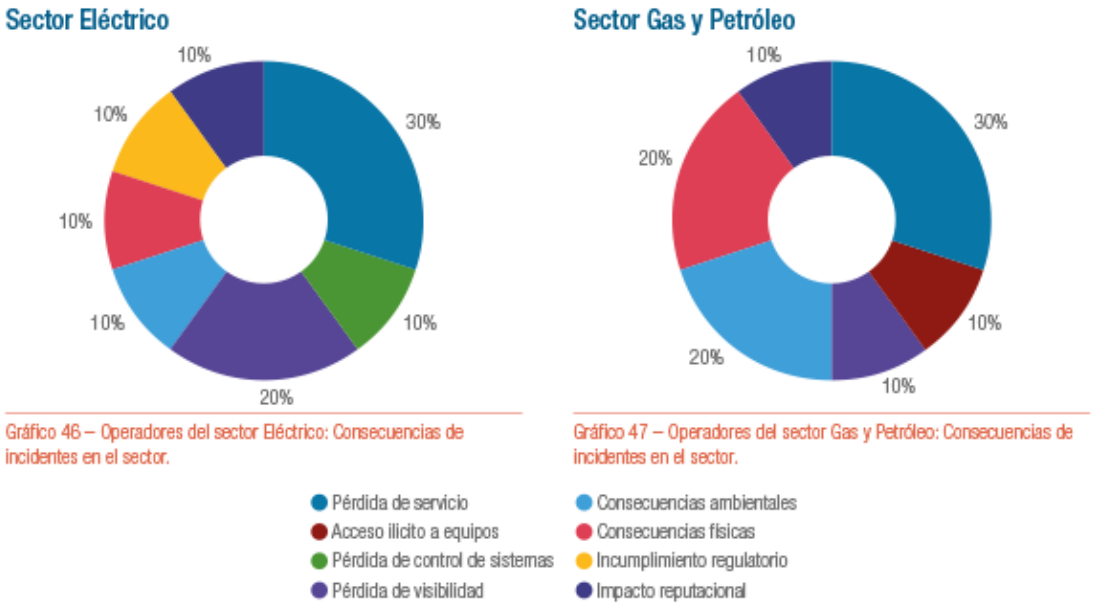


Gráfico 46 – Operadores del sector Eléctrico: Consecuencias de incidentes en el sector.

Gráfico 47 – Operadores del sector Gas y Petróleo: Consecuencias de incidentes en el sector.

¿Están preparadas las empresas del sector para un ciberataque?

El sector energético está expuesto a ciberataques de distinta índole, que van desde el *malware* a ataques basados en web o de aplicaciones web, ataques de denegación de servicio, patrones estándar de ataques a través de amenazas avanzadas persistentes (APT) o verse envueltos en una guerra híbrida y sufrir ataques patrocinados por Estados. Los ciberatacantes pueden perseguir objetivos como la obtención de dinero mediante su robo, el secuestro de datos o de servicios y la consiguiente petición de rescate, el robo de datos de los clientes, realizar algún tipo de daño a la imagen de la empresa, provocar interrupciones del negocio o del servicio y, en los casos más graves, la destrucción de la infraestructura o la pérdida de vidas humanas. Detrás de los ciberataques nos podemos encontrar con ataques oportunistas provenientes de activistas, *script kiddies* y cibercriminales deseosos de obtener dinero a través del secuestro o robo de datos y con ataques dirigidos provenientes de Estados nación, trabajadores descontentos o ciberterroristas. Digamos que las empresas del sector energético están expuestas a los ataques habituales de cualquier empresa industrial, a los que debemos añadir, en el caso de las empresas consideradas como infraestructuras esenciales, los posibles ataques nación o terroristas.

Para hacer frente a los ciberataques, estas empresas presentan problemas ligados a la cultura empresarial, dado que la preocupación principal del sector venía siendo la seguridad física de las infraestructuras y la disponibilidad de la red, y la ciberseguridad es un nuevo escenario de juego al que hay que adaptarse. Por otro lado, cuentan con

sistemas de control industrial del que, en su mayoría, venían siendo propietarios y fueron diseñados e instalados sin tener en consideración la ciberseguridad y que han pasado de estar aislados a estar conectados. Lo mismo puede decirse de la gran cantidad de aplicaciones legadas instaladas. A esto hay que añadir que la continuidad de las operaciones industriales dificulta la actualización de los sistemas, además de obligar a pasar por nuevas certificaciones en ciertos casos. También hay aspectos organizativos, ya que es posible utilizar sistemas de diferentes empresas como puerta de entrada a los sistemas de control industrial por los canales de comunicación existentes entre diferentes entidades de la empresa.

A esto hay que añadir un confuso escenario legal y la carencia de una regulación europea común y un marco de certificación en ciberseguridad. Aunque se han definido algunos estándares de ciberseguridad para sistemas industriales y de potencia, se echa de menos una regulación unificada y un marco de certificación a nivel europeo para los operadores de red y los proveedores de tecnología que ayude a los operadores a saber qué deben pedir y a los fabricantes qué deben desarrollar. Aunque ENISA está trabajando en la definición de una regulación unificada para el sector eléctrico, esta debería ser más ágil para acelerar la necesaria armonización a nivel europeo. Además, las empresas del sector energético también se enfrentan a una falta de recursos financieros para abordar la ciberseguridad y una escasez de recursos humanos capacitados en ciberseguridad y, en el caso de las infraestructuras esenciales, pueden llegar a sufrir disputas territoriales.

En este complejo contexto, debemos pensar en los diferentes agentes de la cadena de valor del sector energético, ya que cada uno debe enfocarse hacia la ciberseguridad y privacidad por defecto y desde el diseño teniendo en cuenta sus especiales características y requisitos:

- Operadores: mejorar la resiliencia de sus instalaciones para que no se produzca una interrupción del servicio o un accidente ante un ciberincidente. Utilizar estándares para la operación, gestión y mantenimiento. Formar a sus empleados en medidas higiénicas de ciberseguridad.

- Proveedores de equipamiento: proporcionar sistemas *hardware*, *software* y empotrados seguros y, a poder ser, certificables. Establecer nuevos procedimientos para la actualización segura de sistemas (gestión del ciclo de vida de equipos seguros). Adaptar/asegurar los sistemas legados

- Otros proveedores de equipamiento, como los de vehículo eléctrico y estaciones de recarga o dispositivos IoT *plug & play*: proporcionar sistemas ciberseguros compatibles.

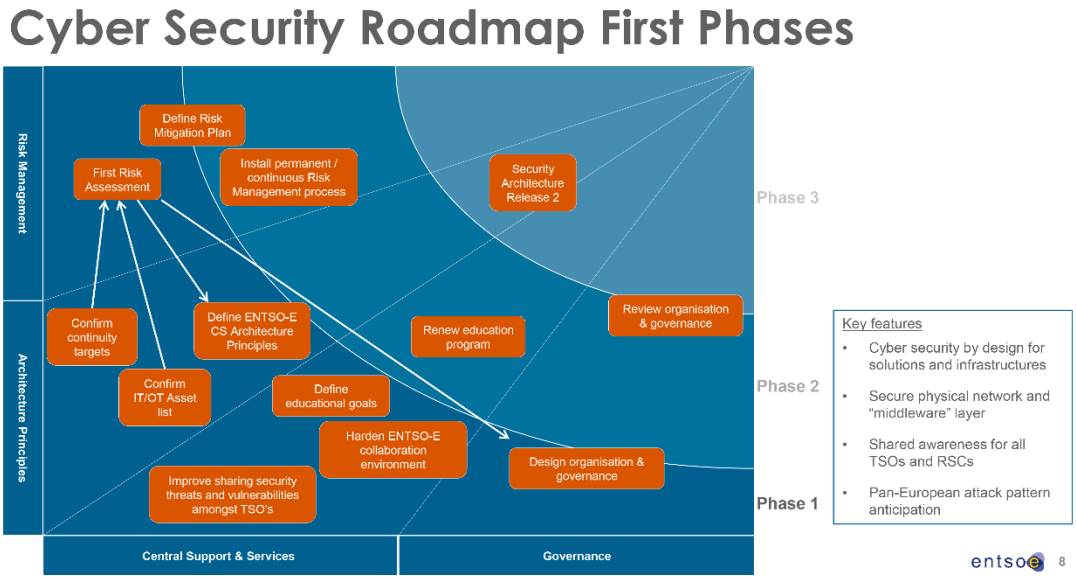
- Compañías de ingeniería e integración: utilizar arquitecturas seguras y aplicar estándares.

- Proveedores de soluciones de ciberseguridad: desarrollar tecnologías y soluciones para la detección temprana de ciberataques y anomalías teniendo en cuenta los requisitos de tiempo real de muchas partes de las instalaciones. Monitorizar y controlar el nivel de seguridad de la red.

- Consultoras y empresas de servicios de ciberseguridad: apoyar en la aplicación e implantación de políticas y estándares.

- Entidades de I+D: investigar en nuevas tecnologías como inteligencia artificial, *machine learning*, *deep learning* y criptografía avanzada para apoyar el desarrollo de nuevas soluciones para la prevención de ciberincidentes, la detección temprana, la gestión y respuesta ante incidentes y el desarrollo de equipamiento con ciberseguridad y privacidad por defecto y desde el diseño.

Figura 6. Fases para una hoja de ruta de la ciberseguridad



Fuente: Nicolas Richet (CIO-ENTSO-E), "Cybersecurity & Energy in Europe", p. 8.

Por otro lado, la infraestructura es solo una parte del sistema completo. Las personas siguen siendo el eslabón más débil en la cadena de la ciberseguridad. Esto hace que sea necesario concienciar a los empleados en medidas higiénicas de ciberseguridad, pero también a la gran cantidad de personal externo subcontratado que suele trabajar en esas instalaciones. Dada la creciente participación de los consumidores en los nuevos modelos de negocio, también se hace necesaria su formación en ciberseguridad.

El papel de los consumidores

La Organización de Consumidores Europeos (BEUC) en su informe "The Future of Energy Consumers"[7] plantea que la relación entre los consumidores y la energía está cambiando drásticamente, ya que podrán elegir el momento de realizar el consumo de una forma más automatizada, participar activamente en el mercado vendiendo su energía y acceder a productos y servicios más sofisticados. Este cambio, en principio beneficioso para los consumidores, supone riesgos asociados con la protección de datos. Por este motivo, desde la organización se plantea la necesidad de seguir criterios de privacidad por defecto y desde el diseño, y que se fijen reglas para el acceso a los datos. También solicitan que todos los proveedores de energía y de servicios sean conformes a la Directiva NIS y que sean considerados por los Estados miembros como operadores de servicios esenciales con independencia de su tamaño.

Si tenemos en cuenta que los datos provenientes de contadores inteligentes, los puntos de recarga del vehículo eléctrico en el hogar u otros productos ligados al consumo en el hogar pueden proporcionar una gran cantidad de información acerca de las preferencias de uso y hábitos de sus usuarios, pudiendo ser utilizados de formar monopolística por algunas empresas de energía, desde BEUC sugieren que la gobernanza de los datos debe estar centrada en el consumidor para evitar la concentración de los datos en unas pocas manos. En cuanto a la utilización de la inteligencia artificial para modificar el modo en el que consumimos energía o en el que funciona el sistema energético, BEUC pide transparencia respecto al funcionamiento de los algoritmos y que las empresas que los utilizan puedan demostrar que han sido diseñados para cumplir con la legislación vigente.

El papel de la Unión Europea en el sector energético

Desde Europa se han planteado diferentes iniciativas relacionadas con el sector energético y que incluyen la ciberseguridad:

- Cybersecurity Act, que ENISA materializará en diferentes certificaciones.
- Directiva NIS en su Grupo de Cooperación con Estados Miembros (Work Stream 8 sobre Energía). En España la Directiva NIS ha sido completamente transpuesta en el Real Decreto Ley 12/2018.
- Intercambio de información a nivel técnico en el grupo de trabajo sobre *smart grids* del European Energy-Information Sharing & Analysis Centre (EE-ISAC).
- Regulación sobre la preparación para riesgos eléctricos.
- Regulación sobre la seguridad del suministro de gas.

[7] The European Consumer Organization, "The Future of Energy Consumers – Bright or Burdensome?", 4 de octubre de 2019, https://www.beuc.eu/publications/beuc-x-2019-055_the_future_of_energy_consumers.pdf

- Acciones de concienciación y de movilización en colaboración con la Red Temática de Protección de Infraestructuras Críticas (TNCEIP) y la Infraestructura Europea de Gas (GIE), involucrada en la construcción de la infraestructura energética europea.

- Recomendación de la Comisión Europea sobre la ciberseguridad en el sector energético.

Esta última plantea una serie de acciones para considerar las particularidades que presenta el sector de la energía, como los efectos en cascada, los requisitos de tiempo real, que plantean retos para las soluciones estándares de ciberseguridad, y la combinación de tecnología con dispositivos que fueron implementados y puestos en funcionamiento cuando no había requisitos de ciberseguridad o nuevos dispositivos de la IoT que tampoco han sido diseñados o instalados considerando la ciberseguridad, lo que implica retos en cuanto a la gestión del ciclo de vida de los productos e instalaciones. Debemos tener en cuenta que las soluciones de ciberseguridad que se implanten lo harán sobre una infraestructura antigua y geográficamente dispersa con miles de dispositivos legados en un contexto en el que la vida media de los productos se reducirá drásticamente y serán necesarias revisiones continuas de vulnerabilidades que afectarán a la fabricación, la actualización y los procesos de certificación.

Esta misma recomendación insta a los agentes relevantes, como operadores de la red de energía, proveedores tecnológicos y especialmente a los operadores de servicios esenciales, a que tomen las medidas apropiadas en relación con la ciberseguridad en el sector de la energía, recomendando estándares como el ISO/IEC 27001/27019, IEC62443, IEC62351 y ISO/IEC31000. Entre las acciones que considera, cabe mencionar:

Figura 7. Acciones recomendadas por la Comisión Europea

Requisitos de tiempo real	Efectos en cascada	Combinación tecnológica
• Utilizar estándares internacionales • Aplicar medidas físicas • Clasificar/gestionar los elementos • Tener en cuenta las redes de comunicación de propiedad privada o considerar medidas específicas • Dividir el sistema en zonas lógicas • Escoger comunicación y autenticación segura	• Evaluar interdependencias • Asegurar un marco de comunicación para alertas tempranas y para cooperar en casos de crisis • Asegurar niveles de seguridad para nuevos dispositivos • Tener en cuenta los sistemas ciberfísicos • Establecer criterios de diseño para una red resiliente	• Seguir una aproximación de ciberseguridad al conectar los dispositivos • Utilizar estándares internacionales • Establecer capacidades de monitorización y análisis • Llevar a cabo un análisis de riesgos para las instalaciones existentes • Colaborar con los suministradores de tecnología • Actualizar el *hardware* y *software*

Fuente: Nicolas Richet (CIO-ENTSO-E), “Cybersecurity & Energy in Europe”.

Además de aplicar la recomendación, se está preparando la implementación de los Códigos de Red Europeos (CdR) para la electricidad en cooperación con la Asociación Europea de Transportistas y Operadores del Sistema (ENTSO-E), los distribuidores europeos de energía (EU DSO) y la Agencia para la Cooperación de los Reguladores de la Energía (HACER), de acuerdo con la nueva regulación eléctrica publicada en mayo/junio. El art. 59(2) tiene un acto delegado que habla de "reglas específicas del sector para aspectos de ciberseguridad de los flujos de electricidad transfronterizos, incluyendo reglas sobre requisitos comunes mínimos, planificación, monitorización, reporte y gestión de crisis".

A finales del 2019, ENISA ha organizado un taller para tratar de identificar las necesidades de certificados de ciberseguridad europeos para los productos, procesos y servicios de energía que sean válidos a través de toda la Unión Europea. Muchos aspectos deben tenerse en cuenta a la hora de definir el proceso de certificación para el sector de la energía, pero en cualquiera de los casos tendrá que ser un esquema ágil y que tenga en cuenta las necesidades de actualización de los dispositivos a lo largo de su ciclo de vida.

Conclusiones

El sector energético es fundamental en una economía y sociedad desarrolladas, por lo que debe asegurarse la resiliencia del ecosistema energético ante diferentes tipos de amenazas o accidentes de seguridad, entre los que se cuenta la ciberseguridad.

Al tratarse de un sector en profunda transformación con la digitalización, la IoT y el nuevo papel de los consumidores, es necesario asegurar el buen funcionamiento y la resiliencia de las infraestructuras existentes que puedan considerarse esenciales teniendo en cuenta los equipos y sistemas legados instalados y analizando cómo minimizar los riesgos asociados. Al mismo tiempo, las nuevas instalaciones y equipos que se desarrollen e instalen deberán hacerse bajo principios de ciberseguridad y privacidad desde el diseño y a lo largo de toda la cadena de suministro, así como de su ciclo de vida. En este sentido, es fundamental la definición y seguimiento de estándares claros y de un marco de certificación que aporte seguridad a usuarios, fabricantes y operadores.

Integrar la ciberseguridad y privacidad desde el diseño implica fomentar una cultura de ciberseguridad en las organizaciones, de forma que puedan definir y gestionar políticas de ciberseguridad, capacitar a las personas, adoptar ciclos de vida ciberseguros para el desarrollo de los equipos y pensar en las respuestas ante posibles incidentes. Ante el nuevo papel de los consumidores como generadores de energía, también debemos pensar en qué formación en ciberseguridad pueden llegar a necesitar.
No debemos olvidar considerar la ciberseguridad en las nuevas interrelaciones y dependencias que se irán estableciendo entre los diferentes servicios ligados a la utilización de nuevas tecnologías como la 5G, así como la aplicación responsable de la inteligencia artificial.