Capítulo tercero

La seguridad de los sistemas eléctricos europeos

Alberto Carbajo Josa

Resumen

La electricidad como tal no se puede almacenar, por eso hay que producir la misma cantidad que se consume y mantener un equilibrio en forma dinámica entre generación y demanda. En el reto del cambio climático, dada la mayor responsabilidad del sector energético, en cuanto a las emisiones de gases de efecto invernadero, debe procederse a un cambio de modelo energético. Afortunadamente los avances tecnológicos de las instalaciones de producción eléctrica con fuentes de energía renovable posibilitan esta transición energética. Sin embargo, su producción es aleatoria e imprevisible por lo que se precisa los servicios complementarios, para mantener el equilibrio mencionado y mantener la seguridad de suministro. Las fuentes de energías renovables se encuentran dispersas por el territorio por lo que habrá que desplegar redes que permitan la recolección de esta energía y el dotar al productor y al consumidor de un papel más activo en el suministro. Los avances tecnológicos de las comunicaciones, con equipos que reflejan la digitalización de vanguardia y dispositivos con redes inteligentes con un doble flujo de energía e información, serán la base sobre la cual se asentarán las decisiones de los consumidores. Los avances en digitalización y el incremento

de información facilitan este proceso, pero uno de los grandes riesgos a los se enfrenta la digitalización es la ciberseguridad en materia de protección de la información y vulnerabilidad de la infraestructura crítica ya que hablamos de una posible afectación a los servicios esenciales a la ciudadanía. Dejar sin luz durante unas pocas horas a una región o incluso un país es algo que, sin duda, tiene grandes repercusiones. El cibercrimen pretende atacar las infraestructuras críticas de organizaciones y Estados, debiendo abordar por éstos, costosos procesos de ciberseguridad.

Abstract

Electricity as such cannot be stored, that is why it is necessary to produce the same quantity as is consumed and keep a dynamic balance between generation and demand. A change in the energy model must be accomplished, as part of the climate change challenge, in view of the energy sector's larger responsibility for greenhouse gas emissions. Fortunately, technological breakthroughs affecting electricity production facilities using renewable energy sources make this energy transition possible. However, its production is random and unpredictable, so supplementary services are required to keep the aforementioned balance and guarantee the supply´s security. Renewable energy sources are scattered throughout the land, so networks will have to be laid that enable this energy to be collected, providing the producer and the consumer with a more active role in the supply. Technological breakthroughs in communications, with equipment that features state-of-the-art digitalisation and smart network devices with a dual flow of energy and information, will constitute the basis on which the consumers' decisions are made. Digitalisation breakthroughs and an increase in the information available make this process easier, but one of the major risks faced by digitalisation is cybersecurity in matters concerning data protection and vulnerabilities affecting critical infrastructure, because we are talking about the possibility of citizens' essential services being affected. Leaving a region, or even a whole country, without electricity for just a few hours undoubtedly has serious consequences. Cybercrime attempts to attack the critical infrastructures of organisations and States, which these then have to face through costly cybersecurity processes.

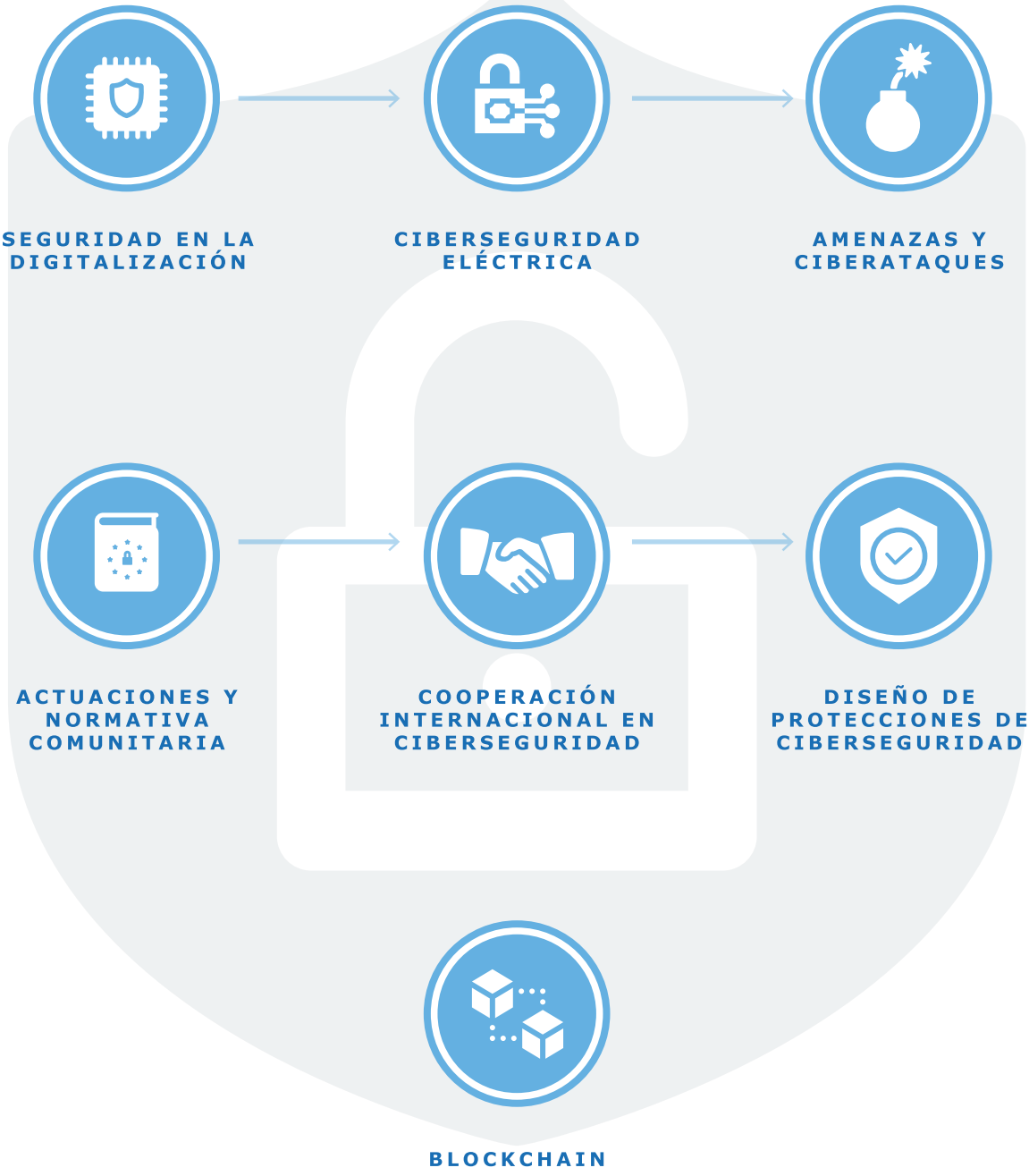
OPERACIÓN DEL SISTEMA ELÉCTRICO EUROPEO

DESCARBONIZACIÓN
ELIMINACIÓN DEL CO_2 RESULTANTE DE LA COMBUSTIÓN

DISTRIBUCIÓN
LA ENERGÍA RENOVABLE ESTÁ DISTRIBUIDA POR EL TERRITORIO

DIGITALIZACIÓN
FACILITA EL DESARROLLO DE LAS RENOVABLES, A LA VEZ QUE REPRESENTA RIESGOS

LOS RIESGOS CIBERNÉTICOS Y LA MITIGACIÓN DE LOS MISMOS



Primera parte

La seguridad del sector eléctrico en España

Introducción

En nuestra sociedad cada día más «electrificada», la garantía y fiabilidad del suministro eléctrico es un factor clave para el correcto funcionamiento de la misma. La interrupción del suministro eléctrico tiene un elevado coste económico y social y prueba de ello son las consecuencias de los últimos «apagones» registrados en grandes urbes.

La sociedad actual demanda índices de calidad de suministro cada vez más elevados, si bien es necesario valorar esto también desde el punto de vista económico y encontrar el óptimo entre la calidad de suministro y el coste económico, que en última instancia siempre repercute en los propios ciudadanos, por ello, hay que gestionar adecuadamente el binomio coste-fiabilidad.

El sistema eléctrico europeo es un sistema maduro y fiable, en el que son escasos los grandes incidentes, pero para ello, la garantía de suministro debe ser planificada y gestionada por las autoridades competentes en el largo, medio y corto plazo con adecuadas políticas energéticas que conlleven un suficiente plan de inversiones: la incorporación masiva de energía renovable en el sistema, cuyas fuentes primarias de energía no son gestionables por su alta variabilidad y su difícil previsión, es un factor de riesgo adicional al que tienen que hacer frente hoy en día los operadores del sistema; la moratoria nuclear alemana, consecuencia del incidente de la central nuclear de Fukushima, que conllevará el cierre de más de 8.000 MW de centrales nucleares, será sin duda un reto para el sistema eléctrico alemán que puede repercutir en su garantía de suministro y por tanto en el suministro eléctrico europeo; las medidas de ahorro energético y las actuaciones en el ámbito de la gestión de la demanda son actuaciones que mejorarán los márgenes de cobertura y, por ello, implicarán una mejora en los índices de garantía de suministro.

La disminución del margen de cobertura en el sistema no solo redunda en una disminución de la fiabilidad de suministro, sino también en un encarecimiento de la producción en el mercado eléctrico, al tener que disponer de las centrales más caras para cubrir las puntas de demanda.

La electricidad no es un bien almacenable (no al menos «a gran escala» y, de momento, no de forma económicamente viable). Eso implica que se necesite sobrecapacidad (necesitamos tener más capacidad de generar electricidad que consumo pico) y que su gestión se tenga que realizar en tiempo real (generación = consumo).

Esto supone que para el correcto funcionamiento del sistema eléctrico debe existir un equilibrio dinámico y permanente entre producción y consumo. Cualquier desequilibrio entre demanda y generación se traduce en un desvío de frecuencia respecto a su valor nominal, -50 Hz en Europa. Este desvío es tanto mayor cuanto mayor sea el desequilibrio generación-demanda y menor sea la inercia del sistema.

La electricidad se negocia en un mercado donde, diariamente y para cada hora, los generadores presentan ofertas de venta en el mercado eléctrico y los consumidores ofertas de compra. Este mercado es gestionado por el operador del mercado, en España, «OMIE» (Operador del Mercado Ibérico, polo español). El mercado tiene una sesión diaria, seis interdiarias y un intradiario continuo que funciona de forma similar a la bolsa de valores. En la sesión diaria, se negocia la mayor parte de la energía, mientras que, en las subastas intradiarias, se ajustan algunas cantidades programadas una vez ya fijado el mercado diario. Ambos tipos de sesión funcionan de forma similar. En el mercado eléctrico diario, los generadores (hidráulica, nuclear, térmica, renovables) presentan diariamente sus ofertas de venta para cada una de las horas del día siguiente. A su vez, comercializadoras y grandes consumidores (domésticos e industriales) presentan sus ofertas de compra, es decir, la energía que prevén consumir en cada una de esas horas. La capacidad de las interconexiones internacionales también se incluye como una variable más del mercado. Si nuestra energía es más cara que la francesa o la marroquí, importamos; si es más barata, exportamos.

De forma horaria, el operador del mercado OMIE ordena las ofertas de generación de menor a mayor según el precio de venta (oferta) y de mayor a menor según el precio de compra (demanda). El precio de la electricidad y la cantidad de energía que va a vender y/o comprar cada uno de los agentes se determina a partir de un punto de equilibrio entre la oferta y la demanda. El encargado de calcular ese punto de equilibrio para cada una de las horas del día siguiente y teniendo en cuenta todas las variables

(incluyendo interconexiones con el resto de mercados europeos) es un algoritmo llamado EUPHEMIA. Como dato importante cabe resaltar que el mercado eléctrico es un mercado marginalista, es decir, independientemente del precio al que haya ofertado un productor, éste recibirá el precio del último productor que haya entrado en el mercado.

Este sistema, desde el punto de vista físico, funciona en tiempo real mediante un principio de solidaridad que las leyes físicas imponen entre los diferentes subsistemas —países— que lo componen, minimizando la repercusión de los posibles incidentes al apoyarse mutuamente entre ellos. En todo este sistema síncrono el valor de la frecuencia es el mismo.

Ante un incidente eléctrico, los generadores síncronos de todos los países vecinos reaccionan, automáticamente, modificando su producción para compensar las variaciones sufridas en el país donde tuvo lugar el incidente. Transcurrido un tiempo establecido corresponde a las instalaciones de este país asegurar, nuevamente, el equilibrio de generación – demanda.

Los servicios de ajuste y servicios complementarios

Para mantener el equilibrio citado, que puede verse alterado por variaciones en el sistema de producción o en el consumo, en la operación del sistema eléctrico, en cada momento, se dispone de las resoluciones de las restricciones técnicas (se producen por las limitaciones técnicas del sistema que no hacen factible el programa de casación obtenido en el mercado eléctrico) y de los servicios complementarios, todo ello comporta lo que se llama los servicios de ajuste.

Los servicios complementarios, gestionados por el operador del sistema, tienen por finalidad adaptar los programas de producción resultantes de la contratación de energía para garantizar el cumplimiento de las condiciones de calidad y seguridad requeridas para el suministro de energía eléctrica.

Los procedimientos de operación, que son resoluciones administrativas, recogen respectivamente las características de los servicios complementarios de regulación primaria, secundaria y terciaria en el sistema eléctrico, que se diferencian entre otras cuestiones en los distintos periodos de tiempo de actuación, que consiguen mantener ese equilibrio y por tanto el valor de la frecuencia.

En España, de acuerdo con lo establecido en el Real Decreto 1454/2005, los servicios de ajuste del sistema están constituidos por: la resolución de restricciones técnicas, identificadas en los programas resultantes de la contratación bilateral física y los mercados de producción (diario e intradiario), así como todas aquellas restricciones técnicas que puedan presentarse durante la propia operación en tiempo real, y por los servicios complementarios, que son aquellos servicios necesarios para asegurar el suministro de energía eléctrica en las condiciones de seguridad, calidad y fiabilidad requeridas y que se clasifican en:

- los asociados a la regulación frecuencia-potencia (reserva primaria, secundaria y terciaria),
- el control de tensión de la red de transporte,
- la reposición del servicio post incidente.

El proceso de gestión de los desvíos entre generación y consumo, como medio imprescindible para garantizar el equilibrio entre la producción y la demanda, debe asegurar la disponibilidad en todo momento de las reservas de regulación requeridas. En términos económicos, el conjunto de servicios de ajuste del sistema tiene una incidencia muy reducida sobre el coste del suministro eléctrico, sin embargo, como ya se ha comentado, son vitales para garantizar la seguridad y la calidad del suministro eléctrico.

Regulación primaria

Tiene por objeto la corrección automática de los desequilibrios instantáneos que se producen entre la generación y el consumo. La regulación primaria es aportada por los reguladores de velocidad con los que están equipados los generadores. Su horizonte temporal de actuación alcanza hasta los 30 segundos. Es un servicio complementario de carácter obligatorio y no retribuido de forma explícita.

La regulación primaria de los grupos generadores debe permitir establecer un estatismo en su regulador de manera que puedan variar su carga en un 1,5 % de la potencia nominal. La variación de potencia resultante debe realizarse en quince segundos ante perturbaciones que provoquen desvíos de frecuencia inferiores a 100 megaherziops (mHz) y linealmente entre quince y treinta segundos para desvíos de frecuencia entre 100 y 200 mHz. La insensibilidad de los reguladores de los grupos debe ser inferior a ±10 mHz y la banda muerta voluntaria nula (ver figura 1).

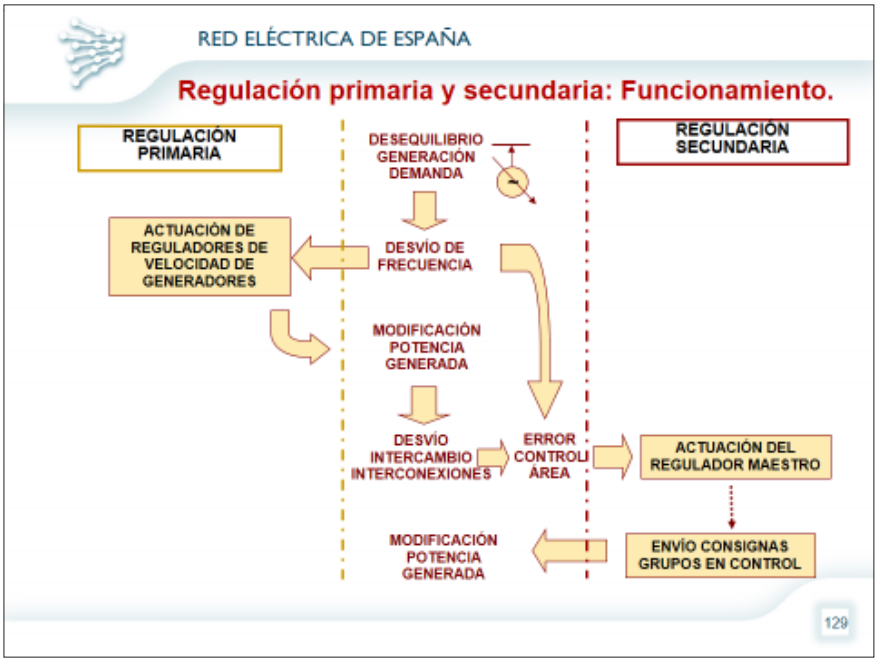


Figura 1. Funcionamiento de la regulación primaria y secundaria.

Regulación secundaria

Tiene por objeto el mantenimiento del equilibrio generación-consumo, corrigiendo los desvíos respecto a los programas de intercambio previstos en la interconexión entre España y Francia, y las desviaciones de la frecuencia, respecto al valor de consigna establecido. Es un servicio complementario de regulación frecuencia-potencia centralizado que actúa entre los 20 segundos y 15 minutos del desbalance. En este punto los «generadores» ya no hacen «la guerra por su cuenta» como en la regulación primaria, sino que la consigna de regulación es calculada por un sistema central llamado RCP (regulación compartida peninsular) gestionado por Red Eléctrica SAU, que tiene como misión mantener la frecuencia objetivo de la red y los intercambios de energía programados en las interconexiones internacionales con otros países.

La regulación secundaria es aportada por los generadores, cuyas ofertas son seleccionadas mediante mecanismos competitivos. La consigna de regulación necesaria a nivel peninsular para ajustar la frecuencia y el balance con Francia y Portugal se reparte en diferentes valores (CRR en la figura 2) entre diferentes agrupa-

ciones de productores dentro de lo que se denominan zonas de regulación (AGC en la figura 2). Cada zona está constituida por una agrupación de centrales con capacidad de prestar el servicio de regulación secundaria. Las zonas son comandadas por el regulador maestro del operador del sistema, denominado RCP. Cada una de estas zonas reparte a su vez la consigna de regulación del regulador maestro para cumplir con las solicitudes en el tiempo requerido. El requerimiento de respuesta dinámica de cada zona de regulación es el correspondiente a una constante de tiempo de 100 seg. La demanda, por el momento, no participa en este servicio.

El día anterior al suministro y tras el mercado diario y el proceso de restricciones técnicas, los productores habilitados ofertan su banda de fluctuación de potencia disponible, obteniendo una retribución por ella. El coste de la provisión de la banda de regulación secundaria recae sobre la demanda y es uno de los principales costes de los servicios de ajuste del sistema. El uso de esa potencia que se utiliza lo pagan la demanda y generadores que causan la necesidad por desviarse respecto a lo programado en el mercado. El servicio de regulación secundaria es complementario de carácter potestativo, retribuido por dos conceptos: disponibilidad (banda) y utilización (energía).

Disponibilidad o banda de regulación

Cada día, el operador del sistema publica los requerimientos de reserva de regulación secundaria, tanto a subir como a bajar, para la programación del día siguiente. Los productores ofertan una banda de regulación para cada unidad de programación habilitada para la prestación de este servicio complementario. Se asignan las ofertas, aplicando criterios de mínimo coste, hasta cubrir los requerimientos, estableciéndose un precio marginal de banda en cada hora.

Energía utilizada de regulación secundaria

El uso de esa potencia también se le retribuye al productor. La utilización de energía de regulación secundaria se realiza, de forma automática, basándose en la asignación de banda establecida por el del el día anterior a través del correspondiente mercado.

La energía de regulación secundaria utilizada como consecuencia del seguimiento en tiempo real de los requerimientos de regula-

ción se valora, al precio marginal de la energía de regulación terciaria que hubiera sido necesario programar en cada hora, tanto a subir como a bajar, para sustituir a la energía.

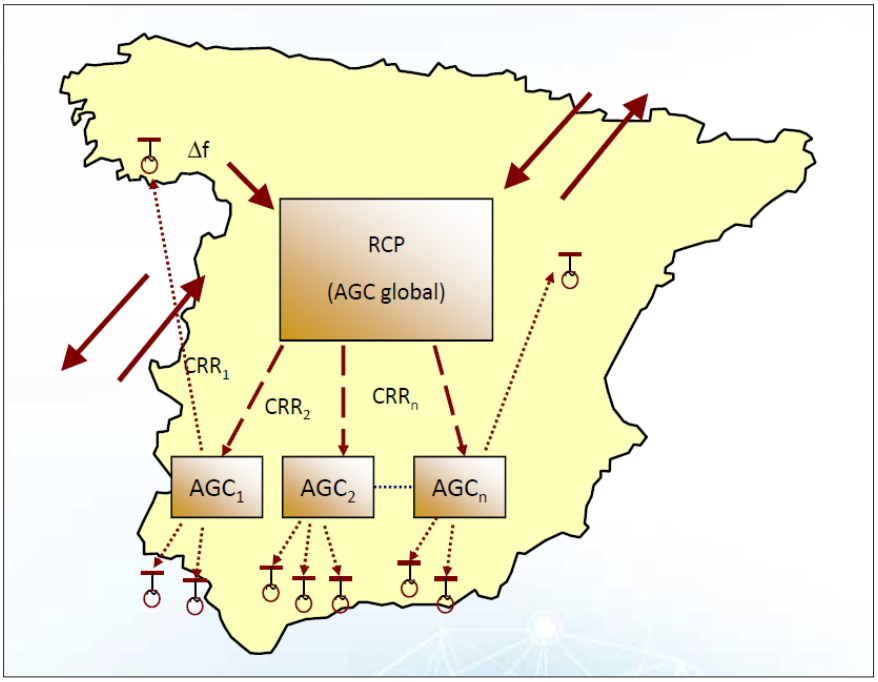


Figura 2. Regulación compartida peninsular.

Cabe destacar, dentro de la apuesta de la Unión Europea por la integración real y efectiva de mercados y la implantación del mercado único europeo, que se está trabajando muy activamente dentro de las organizaciones europeas de reguladores —ACER— y Operadores del Sistema —ENTSO-E— en el establecimiento de mecanismos transfronterizos de energías de balance y reserva entre los Estados miembros que redunden en un mercado eléctrico más competitivo. Los servicios transfronterizos de balance permitirán, entre otras cosas, una mayor y más segura integración de energías renovables.

Regulación terciaria

Tiene por objeto la restitución de la reserva de regulación secundaria que haya sido utilizada. Es aportada mediante la actuación manual de subida o bajada de potencia de las centrales de generación o de consumo de bombeo que la oferten al menor precio,

en el caso de energía a subir, o a un mayor precio de recompra en el caso de energía a bajar. La reserva terciaria se define como la variación máxima de potencia que puede efectuar una unidad de producción o de consumo de bombeo en un tiempo no superior a 15 minutos, y que puede ser mantenida durante, al menos, 2 horas. La regulación terciaria es un servicio complementario de oferta obligatoria y retribuido a través del correspondiente mercado de operación. En caso de resultar necesario, se asigna el servicio de regulación terciaria con base en las ofertas enviadas a tal fin por las unidades de producción; el precio del servicio es fijado por la última oferta asignada en cada dirección, subir y bajar, en cada hora.

Gestión de desvíos

Tiene por objeto resolver los desvíos entre generación y consumo que pudieran aparecer con posterioridad al cierre de cada sesión del mercado intradiario y hasta el inicio del horizonte de efectividad de la siguiente sesión.

La gestión de desvíos cumple una función de nexo entre la regulación terciaria, y los mercados intradiarios, dotando al operador del sistema de un mecanismo de mayor flexibilidad para poder solventar los desequilibrios entre generación y demanda, sin poner en riesgo la disponibilidad de las reservas de regulación secundaria y terciaria requeridas. Para ello, antes de cada hora se evalúan los desvíos comunicados y/o previstos en el horizonte hasta la próxima sesión del mercado intradiario y, en caso de identificarse desvíos de magnitud superior a 300 MWh, mantenidos varias horas, se convoca el correspondiente mercado de gestión de desvíos.

La asignación se basa en las ofertas de incremento y reducción de generación y de consumo de bombeo presentadas a dicha convocatoria. La valoración de las modificaciones programadas para la resolución de los desvíos se realiza al precio marginal de las ofertas asignadas en cada periodo horario.

Control de tensión de la red de transporte

Tiene por objeto garantizar el adecuado control de la tensión en los nudos de la red de transporte, de forma que la operación del sistema se realice en las condiciones de seguridad y fiabilidad requeridas, el suministro de energía a los consumidores finales

se efectúe con los niveles de calidad exigibles y las unidades de producción puedan funcionar en las condiciones establecidas para su operación normal. Son proveedores de este servicio complementario los grupos generadores, de potencia neta no inferior a 30 MW y con conexión directa, o a través de línea dedicada, a nudos de la red de transporte, las empresas transportistas, los consumidores cualificados no acogidos a tarifa, con potencia contratada no inferior a 15 MW y conectados directamente a la red de transporte, y los gestores de las redes de distribución.

Reposición del servicio

Tiene por objeto reponer el suministro en caso de una perturbación de ámbito nacional o regional. Se basa en la capacidad que tienen determinados grupos generadores para arrancar sin alimentación exterior en un tiempo determinado tras un cero de tensión general en la instalación y mantenerse generando de forma estable durante el proceso de reposición del servicio, o bien de mantenerse en funcionamiento en isla sobre sus servicios auxiliares, preparados para servir de punto de envío de tensión y energización tras la perturbación. Este servicio complementario está aún en fase de desarrollo.

Recientemente, ocho operadores de sistemas eléctricos (TSO) europeos han lanzado la plataforma europea de energías de balance TERRE que permite gestionar de forma coordinada en el ámbito europeo el equilibrio entre la generación y la demanda de electricidad, tras los ajustes de los programas en el mercado intradiario.

Esta plataforma apoyada en las interconexiones internacionales, permitirá una gestión aún más eficiente de las energías de balance, al sustituir los mercados nacionales de balance y los mecanismos bilaterales de intercambio de energías de balance entre sistemas interconectados vecinos, por un sistema multilateral de ámbito europeo.

Su uso contribuirá a reducir el precio final de la energía y optimizará la integración de la generación renovable en Europa. Supone así, un paso decisivo en la implantación del mercado interior de la electricidad en Europa.

En resumen, los mercados de ajuste gestionados por el operador del sistema tienen por finalidad adaptar los programas de producción resultantes de la contratación bilateral física y de los

mercados diario e intradiario para garantizar el cumplimiento de las condiciones de calidad y seguridad requeridas para el suministro de energía eléctrica.

Las protecciones eléctricas

El sistema eléctrico está constituido por una serie de instalaciones, la mayoría de intemperie, conectadas de superficie, sobre el territorio y por ello está sometido a continuas agresiones algunas de ellas accidentales, como caída de rayos o de árboles que producen cortocircuitos que necesitan ser aislados para que no afecten al suministro de los consumidores o por el contrario, malintencionadas provocadas para causar averías que afecten de forma generalizada al suministro.

Por ello, los sistemas se dotan de unos mecanismos denominados protecciones, cuya misión es o bien proteger al personal o a la aparamenta de las consecuencias de los cortocircuitos o bien aislar la zona donde éste se ha producido para evitar que las consecuencias se propaguen a lo largo de toda la red.

El Operador del Sistema establece, con la colaboración de los agentes afectados, los criterios de coordinación de los sistemas de protección de la red gestionada, así como de éstos con los sistemas de protección de las instalaciones de distribución conectadas directamente a la dicha gestionada. La red de transporte está interconectada con la red mallada de distribución de AT en múltiples puntos, mediante transformadores transporte (220, 400 kV) – distribución mallada (30, 45, 50, 66, 110 y 132 kV, típicamente), que son el elemento frontera. Por otra parte también hay transformadores entre la red de transporte y la red de distribución no mallada o también llamada radial. En cuanto a los sistemas de protección, para aislar las faltas mencionadas, se pueden distinguir dos grandes grupos. En un primer grupo se encuadran aquellos sistemas cuyo objetivo es la protección unitaria o de funcionamiento «cerrado» (protecciones sensibles única y exclusivamente a faltas eléctricas ubicadas entre transformadores de intensidad) cuya naturaleza, a efectos de coordinación, les confiere independencia total respecto al resto de sistemas de protección. Tales sistemas no precisan análisis de coordinación propiamente dicho. El segundo grupo lo constituyen los sistemas de protección de funcionamiento «abierto», sensibles a faltas eléctricas ubicadas tanto en el propio elemento a proteger como más allá del mismo. Su característica principal es la interdepen-

dencia y, por tanto, estos sistemas requieren coordinación entre ellos para obtener la selectividad necesaria.

Para cada elemento del sistema eléctrico analizado, líneas y cables, transformadores, barras y acoplamientos de barras, hay que establecer los criterios básicos de coordinación, para cada uno de los diferentes tipos de falta eléctrica, así como los intervalos de ajuste admisibles. Para cada función se formulan los límites, inferior y superior impuestos a los ajustes en función de la ubicación de la falta, es decir, si actúa como protección principal o protección de apoyo remoto.

La transición energética

El cambio climático consiste, entre otras manifestaciones, en el calentamiento global de la tierra debido al efecto invernadero provocado por la elevada concentración de CO_2 alcanzada en la atmósfera. En esta elevada concentración influye de manera notable la utilización de combustibles fósiles en la generación de electricidad y en el transporte y movilidad.

En la Unión Europea, la necesidad de protección medioambiental y la política energética ha llevado a establecer en el paquete «Energía limpia para todos los europeos», del también llamado «paquete de invierno», los siguientes objetivos para el horizonte del año 2030:

- Reducción del 40 % de las emisiones de CO_2 con relación a las habidas en el año 1990.
- Presencia en el mix de energía final de 32 % de energía procedente de fuentes renovables.
- Incremento de la eficiencia energética del 32,5 %.

La nueva Comisión Europea está en la línea de profundizar en los objetivos de reducción de CO_2, pero esta mayor ambición va a necesitar de una más alta flexibilidad para poder alcanzar lo propuesto ya que, por primera vez, la obligación política va por delante de la tecnología.

La consecución de estos objetivos precisará de un incremento profundo de la electrificación de la economía para conseguir un modelo energético híbrido basado en la electrificación y la utilización de gases descarbonizados y/o renovables (siempre que los avances tecnológicos hagan viable económicamente la producción de hidrógeno y la captura y confinamiento de CO_2).

Para ello, se presentan ya unas tendencias claras hacia la generación renovable y el almacenamiento de energía a través de bombeos y baterías, a la respuesta de la demanda, a la generación de respaldo (tan limpia como sea posible) y a las interconexiones energéticas. Es necesario un amplio consenso para definir el trayecto hacia un mix de generación más sostenible.

La penetración de la electricidad en la economía se verá algo mitigada con los resultados que se obtengan de la aplicación de medidas de eficiencia energética, pero si hay crecimientos de demanda eléctrica importantes, el cierre paulatino de las centrales de generación basada en el carbón, que debe tender a su desaparición, deberá conciliarse con la necesidad de potencia firme por los incrementos de demanda.

En el sector de la movilidad, otro sector que se encuentra entre los principales responsables de las emisiones contaminantes, la utilización del automóvil eléctrico y del vehículo con gases descarbonizados será la clave para poder reducir de una manera drástica el nivel de las mismas, siempre que la producción de la electricidad se realice mediante fuentes no emisoras de CO_2.

Por otra parte, los Estados han venido basando los objetivos de reducción de emisiones de CO_2 fundamentalmente en la actividad de generación eléctrica, sector en el que el coste marginal de reducción es más elevado y el riesgo de deslocalización más reducido. Pero también se exige reducción de emisiones a sectores de la industria básica que sí están sujetos a ese riesgo, por lo que se aplican compensaciones por los costes de adquisición de derechos de emisión para reducir el riesgo de deslocalización.

Para conseguir una reducción de emisiones en el sector eléctrico y en el sector industrial, se ha establecido un mercado de emisiones de modo que se asignan unas determinadas cantidades de emisiones permitidas, que son llamados derechos de emisión, que son decrecientes en el tiempo. Si las emisiones reales de cada instalación son superiores a sus derechos, puede acudir al mercado a aprovisionarse de los derechos faltantes donde estarán los derechos excedentarios de CO_2 de las empresas con emisiones reales inferiores a la cantidad asignada.

La electricidad es, pues, un vector energético que por sus características desempeña un papel fundamental con participación creciente en el consumo final de energía. La producción de electricidad se ha de desenvolver en un triple compromiso entre seguridad de suministro, sostenibilidad medioambiental y competitividad eco-

nómica. En efecto, la producción de electricidad tiene unas implicaciones medioambientales cuyo análisis riguroso requiere evaluar estas, en todas y cada una de las fases del ciclo de vida del kWh. Nos centramos aquí exclusivamente en las emisiones contaminantes resultado de la actividad de generación eléctrica.

Las principales emisiones contaminantes derivadas de la actividad de generación eléctrica son resultado de la utilización, mediante combustión, en las centrales de combustibles fósiles. Las emisiones de gases de CO_2 tienen un efecto global, aunque inocuo para la salud humana, uno de los principales causantes del efecto invernadero. Las emisiones de gases acidificantes y eutrofizantes como los NOx (gases precursores del ozono troposférico), el SO_2 y las emisiones de partículas sólidas tienen efectos locales y regionales.

Las emisiones de carácter ácido, SO_2 y NOx, se pueden controlar de manera casi total empleando combustibles más limpios y, sobre todo, instalando plantas limpiadoras de gases. El único problema es el incremento de los costes de producción debido a los costes de inversión y de los productos a adicionar con la consiguiente pérdida de competitividad relativa.

Las energías renovables

El desarrollo de energías renovables constituye uno de los puntos principales en la política energética en España, marcada por la necesidad de disminuir la dependencia energética del exterior (importamos un 80 % de nuestras necesidades en energía primaria, mientras que la media europea está en el entorno del 55 %), así como de disminuir las emisiones de carbono y de cumplir con los compromisos medioambientales y de eficiencia contraídos (Kioto y objetivos 20-20-20 motivados por la Directiva 28/CE/2009) y del paquete «Energía limpia para todos los europeos».

Las energías renovables se han implantado de manera significativa en el sistema eléctrico español, en especial la generación eólica, que con una potencia instalada a finales del año 2019 de 25.310 MW es la segunda tecnología con mayor potencia instalada en el sistema eléctrico peninsular español, tan solo por detrás de las centrales de gas de ciclo combinado. Por otra parte, no hay que olvidar que la generación hidráulica convencional, con una potencia instalada a finales del año 2019 de 17.085 MW es la tercera tecnología de generación en potencia instalada, aunque no ha ha-

bido aumentos significativos en los últimos años y a la que habría que sumar 3.329 MW de hidráulica de bombeo. Otras tecnologías renovables, a finales del año 2019, como la solar fotovoltaica con 8.454 MW de potencia instalada o la solar térmica con 2.304 MW, han adquirido relevancia en el parque generador. El resto de tecnologías renovables implantadas en España tienen mucho menor peso en el mix de producción. Estas tecnologías son la biomasa, la mini-hidráulica o la incineración de residuos de naturaleza renovable. La capacidad de generación de origen renovable permitió que el 38,9 % de la generación neta anual península en el año 2019 (247.002 GWh) fuese renovable, contribuyendo la eólica en un 21,5 %, la hidráulica convencional en un 10,0 %, la solar en un 5,7 %, y el resto de renovables en un 1,5 %. La energía producida sin emisiones de CO_2 ha ascendido a 151.918 GWh lo que supone el 61,5 del total. Se espera que en el año 2030 cerca del 40 % de la energía primaria consumida sea de origen renovable.

El objetivo de estas tecnologías, eólica y solar fotovoltaica, es transformar en energía eléctrica el máximo producible con las condiciones de sol o viento disponibles, y lo hacen con independencia de las necesidades del sistema eléctrico en ese momento. Desde el punto de vista de la integración en el sistema eléctrico, la característica principal es que su régimen de funcionamiento depende exclusivamente de las condiciones meteorológicas existentes en cada momento en el emplazamiento.

Estas condiciones meteorológicas locales son muy variables, lo que se traduce en que la generación que depende de ellas es también variable. Un parque eólico puede permanecer parado debido a la falta de viento y pocas horas más tarde puede producir su potencia nominal debido a un aumento del viento. Esto ocurre con mayor regularidad en el caso de la generación solar fotovoltaica, que durante la noche no produce energía y en días soleados produce prácticamente su potencia máxima en las horas centrales del día. Una consecuencia de este comportamiento es que el factor de utilización de estas tecnologías, como relación entre la energía producida durante un periodo de tiempo determinado y la energía que se hubiera producido si la instalación hubiera generado a plena potencia durante el mismo periodo de tiempo, es bajo. En el caso de la generación eólica es de alrededor del 25 % en los parques españoles y también, con los avances tecnológicos, en la fotovoltáica es de alrededor del 25 %.

Un factor de utilización bajo implica que para conseguir una penetración determinada en términos de energía se debe instalar

una potencia más alta que para tecnologías con factor de utilización alto. Sin embargo, en determinadas situaciones, dada la alta potencia instalada, se producirá una simultaneidad en la producción de una tecnología, momentos con situaciones de alto viento en toda la península para la generación eólica o días soleados de verano para la energía solar fotovoltaica, con lo que la producción a integrar en esos momentos será muy alta pudiendo dificultar esta integración, especialmente si la demanda es reducida, como puede ocurrir en horas nocturnas o en las mañanas de determinados domingos o festivos.

Las tecnologías de generación se clasifican fundamentalmente dependiendo de su gestionabilidad. La definición de gestionabilidad se establece en el RD 661/2007, estableciendo como generación no gestionable «aquella cuya fuente primaria no es controlable ni almacenable y cuyas plantas de producción asociadas carecen de la posibilidad de realizar un control de la producción, siguiendo instrucciones del operador del sistema, sin incurrir en un vertido de energía primaria, o bien la firmeza de la previsión de producción futura no es suficiente para que pueda considerarse como programa». En principio, y tal como se establece en el anexo XI del mencionado Real Decreto, se consideran como no gestionables los generadores de régimen especial con tecnología eólica, solar (térmica y fotovoltaica), geotérmica, de las olas y mareas, de las rocas calientes y secas, oceanotérmica, de las corrientes marinas, así como los generadores hidráulicos fluyentes con potencia instalada inferior a 50 MW, salvo valoración específica gestionable, a realizar por el operador del sistema, de una planta generadora con la consecuente aplicación de los requisitos o condicionantes asociados a dicha condición.

Es decir, para la integración de las energías renovables, por su alta variabilidad y su difícil predictibilidad se precisan, para asegurar en todo momento el equilibrio dinámico entre la generación y el consumo, de instalaciones que puedan almacenar la energía excedentarias en momento de menor demanda y recurrir a ellas cuando la demanda fuera mayor que la energía que, en ese momento, ofrezcan las plantas de energías renovables. Estas instalaciones de almacenamiento son o bien de bombeo o, cuando la tecnología ofrezca soluciones de almacenamiento no solo diario si no también estacional, de baterías, que hoy están alcanzando un gran desarrollo a la espera de su escalación cuando alcance la viabilidad económica. A este respecto, puede jugar un papel im-

portante el H_2 cuando su producción con los diferentes métodos que hoy se están investigando, la hagan viable.

Entre tanto, además de los bombeos y baterías, la variabilidad de las renovables puede ser compensada con generación firme pero flexible, es decir, de respuesta rápida, donde las plantas hidroeléctricas y las centrales de ciclo combinado consumiendo gas natural (con menor emisión específica de CO_2 que las actuales centrales de carbón) jugaran un papel muy importante durante las primeras décadas de la transición energética pudiendo ser desplazadas cuando los almacenamientos (bombeos y baterías) hayan alcanzado su viabilidad económica y estén operativos.

El sistema eléctrico europeo

El sistema eléctrico peninsular español forma parte del sistema interconectado europeo que abarca la mayor parte de la Europa Continental hasta Polonia y Grecia, y también está conectado con Marruecos, Argelia y Túnez a través de dos cables submarinos de 400 kV bajo el estrecho de Gibraltar. Dentro de esta área regional el sistema eléctrico europeo es conducido por los operadores de los sistemas (TSO) que están asociados en ENTSO-E, cuyas áreas fundamentales de cooperación son el desarrollo de la red europea de infraestructuras eléctricas y la coordinación del sistema eléctrico europeo así como el trabajo conjunto en materia de innovación y desarrollo tecnológico. Además, a esta asociación se le ha confiado por la Comisión de la Unión Europea, el desarrollo de los códigos de red actualmente en vigor y es el principal grupo asesor técnico en materia de energía eléctrica por las instituciones europeas. Su implicación es fundamental para afrontar los retos que plantea la reducción de emisiones, la integración de energías renovables a gran escala, la flexibilidad o las nuevas tecnologías.

Datos de tamaño del sistema (2018)

Sistemas eléctricos	*Potencia MW instalada*	*Generación neta TWh*	*Producción con bombeo TWh*	*Demanda TWh*
ENTSO-E	1.083.705,0	3.659,20	46,3	3.328,80
Continental	868.944,5	2.913,85	41,7	2.862,55
Nórdico	100.328,5	385,95		381,05
Báltico	9.214,0	20,00	0,7	28,20
G. Bretaña	90.207,0	285,80	3,4	304,00

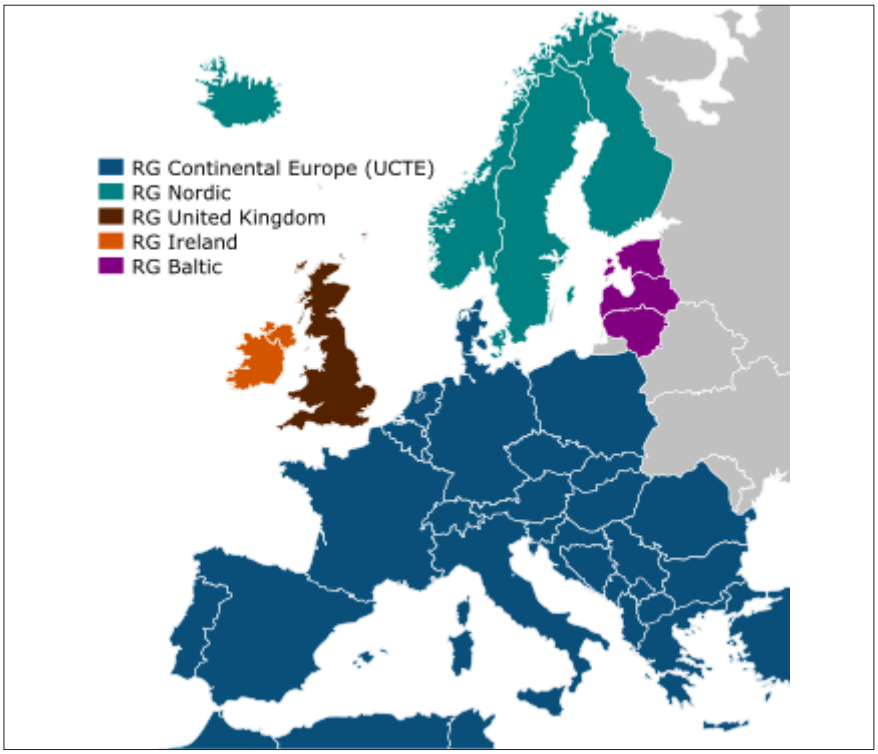


Figura 3. Alcance de los sistemas eléctricos europeos.

Las interconexiones eléctricas

Las interconexiones internacionales que se representan en la figura 3 generan una serie de ventajas en los países conectados. La principal es la contribución a la seguridad y a la continuidad del suministro eléctrico en los sistemas interconectados, gracias a los intercambios de energía en caso de necesidad. Las interconexiones son el respaldo instantáneo más significativo a la seguridad de suministro.

La segunda ventaja de las interconexiones, que se ve supeditada a la primera, es el aumento de la eficiencia de los sistemas interconectados. Con la capacidad que queda vacante en las líneas, después de la capacidad ocupada por razones de seguridad de los sistemas eléctricos de los países, se establecen diariamente intercambios comerciales de electricidad aprovechando las diferencias de precios de la energía entre los sistemas eléctricos. Estos intercambios permiten que la generación de electricidad se realice con las tecnologías más efi-

cientes fluyendo la energía desde donde es más barata hacia donde es más cara.

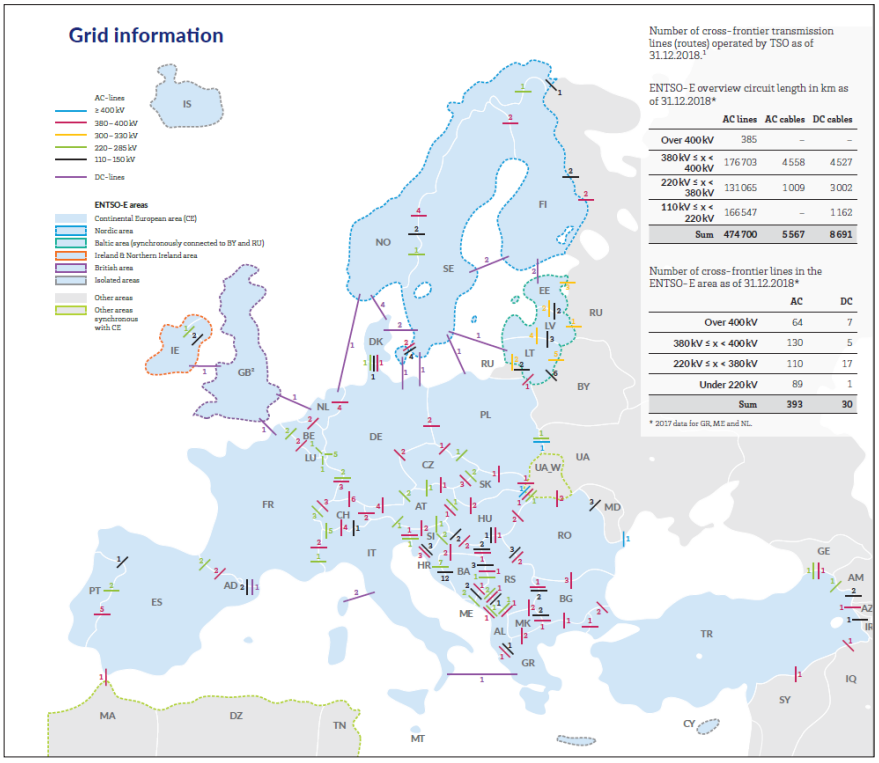


Figura 4. Las interconexiones eléctricas en Europa.

Hay además una tercera ventaja: el aumento de la competencia entre sistemas vecinos. Las importaciones de energía de otros países obligan a los agentes del propio país a tener propuestas más competitivas si quieren que sus ofertas resulten aceptadas, generando una reducción del precio de la electricidad a nivel mayorista.

En resumen, las interconexiones presentan los siguientes beneficios para los sistemas eléctricos:

- Contribuyen a la seguridad del suministro, facilitando funciones de apoyo entre sistemas vecinos. Las interconexiones son el respaldo instantáneo más significativo a la seguridad de suministro.
- Aportan mayor estabilidad y garantía de la frecuencia en los sistemas interconectados.

- Proporcionan un mejor aprovechamiento de las energías renovables.
- Facilitan los intercambios comerciales de energía, aumentando la competencia al aprovechar las diferencias de precios de la energía en los sistemas eléctricos interconectados. Las interconexiones juegan un papel fundamental en el llamado Mercado Interior de la Electricidad en Europa (MIE), que busca integrar el conjunto de los mercados existentes a día de hoy en la Unión Europea en un solo mercado.

Por todo lo anterior, las interconexiones tienen un papel fundamental en la integración de los mercados de energía eléctrica. Este es el objetivo que se persiguió con el Mercado Interior de la Electricidad en Europa (MIE), que buscaba integrar el conjunto de los mercados existentes en la Unión Europea en uno, si bien las capacidades limitadas de las interconexiones suponen una restricción importante en muchas ocasiones a la consecución de ese objetivo.

La capacidad de intercambio se define como el valor máximo de potencia eléctrica instantánea que se puede importar o exportar entre dos sistemas eléctricos manteniendo los criterios de seguridad de cada uno de ellos.

Para calcular esta capacidad, el operador de cada sistema realiza estudios coordinados con los operadores vecinos donde se tienen en cuenta las previsiones de generación y demanda, y los períodos de mantenimiento de las instalaciones, además de realizar simulaciones teniendo en cuenta el fallo de los distintos elementos de red. Todos estos estudios se realizan en diferentes horizontes temporales, desde previsiones anuales hasta diarias, para así poder realizar los máximos intercambios comerciales posibles respetando siempre los criterios de seguridad.

Para que cada país alcance las ventajas enumeradas anteriormente, es fundamental mantener un elevado nivel de capacidad de intercambio. En este sentido, la Unión Europea recomienda que, en el año 2030, represente al menos el 15 % de la capacidad de producción instalada en cada uno de ellos.

Tradicionalmente la planificación del desarrollo de las interconexiones entre dos sistemas nacionales la realizaban de forma bilateral los dos países en cuestión. Sin embargo, esta situación está cambiando en los últimos años debido al objetivo marcado por la Unión Europea de la creación del MIE. La planificación de la red

se está trasladando del ámbito nacional al europeo, ya que todo desarrollo de la red de transporte, y en particular de las interconexiones, tiene influencia en el funcionamiento de otros sistemas y mercados eléctricos. Con esta visión, ENTSO-E (la asociación de los operadores y propietarios de la red de transporte europea) publica cada dos años el *Ten Year Network Development Plan* (TYNDP) que identifica cuáles deben ser los desarrollos de la red de transporte europea en el horizonte de 10 años.

La corriente continua europea es ya una tendencia entre las infraestructuras identificadas en los TYNDP. Inglaterra, por ejemplo, que ya está interconectada con Francia, Holanda e Irlanda con enlaces de este tipo, tiene previsto, además de reforzar estos, conectarse con Bélgica y Noruega. Otros enlaces que ya están funcionando son los que unen en el mar del Norte Noruega con Dinamarca y Holanda, y Suecia con Dinamarca y Alemania; en el mar Báltico Suecia con Polonia, y Finlandia con Suecia y Estonia, y en el Mediterráneo Italia y Grecia. En el ámbito ibérico, están planificados e iniciados los estudios del suelo marino, la construcción de un enlace submarino desde Gatica (cerca de Bilbao) a Coubnezais (cerca de Burdeos) especialmente para reforzar la capacidad de intercambio con Francia, que se verá reforzada, además, por otras interconexiones a través de los Pirineos.

Segunda parte

La digitalización

El mundo se ha vuelto totalmente dependiente de un suministro estable de electricidad. Las redes eléctricas forman parte de las infraestructuras críticas de un país al igual que lo son los principales hospitales, aeropuertos, etc. Es por esto que, las interrupciones de suministro eléctrico sean inaceptables y a menudo conlleven sanciones de los gobiernos a los operadores de la red. La frontera entre lo que se ha llamado OT (*Operational Technology*) e IT (*Informational Technology*) es inexistente. Las subestaciones eléctricas del futuro, digitalizadas, requerirán de una mayor interoperabilidad entre múltiples vendedores, no solo los clásicos vendedores de OT, y vendrán con conceptos nuevos como virtualización de sensores, *machine learning* y otros conceptos anteriormente solo vistos en otras industrias.

La transformación digital puede ser una tarea desalentadora y algo arriesgada en este sector. Las eléctricas han heredado sis-

temas de IT altamente complejos y obsoletos, y deben seguir trabajando con ellos, al tiempo que afrontan los desafíos que les plantea la regulación. Históricamente, estas empresas han adoptado las nuevas tecnologías de manera tardía. Ahora que se cierne sobre ellas una ola de productos y servicios digitales, sienten la urgencia de embarcarse en grandes procesos que llegan tarde, como la mejora de la gestión del trabajo, de los almacenes o la facturación a clientes. A su vez, estos cambios generan riesgos, como la falta de coordinación o la adopción de soluciones tecnológicas a corto plazo que no son tan óptimas. El posicionamiento digital debe ajustarse a cada empresa teniendo en cuenta su tamaño, geografía, arquitectura y beneficios previstos.

Los líderes del sector en Europa y Estados Unidos han desarrollado estrategias de mejora continua, diferenciando los esfuerzos operativos o de *back-office*, de los orientados al cliente.

Es preciso desarrollar una mentalidad multifuncional en toda la empresa. En la mayor parte de las *utilities* se espera que la función de IT impulse la transformación digital de la compañía —lo cual resulta lógico, dada su naturaleza y su relación intrínseca con las tecnologías de la información y las comunicaciones—. No obstante, la llegada de activos inteligentes y conectados implica que la tecnología ya no solo es un facilitador de las transacciones. Más bien, se ha convertido en la esencia del modo en que las compañías operan y hacen llegar su servicio.

Desgraciadamente, muchas unidades de negocio no ven su relación con IT como algo estratégico, sino meramente transaccional y táctico. Y, aunque IT tome las riendas del proceso, son los operadores de las plantas eléctricas, los empleados de a pie, y los directivos, los que deben hacer efectiva la transformación. Son ellos los que deben cambiar la forma de operar de sus plantas y emplear sistemas de control y administración de la red de última generación para impulsar el valor del servicio.

En el desarrollo de su agenda digital, las compañías eléctricas deben considerar todas las palancas de valor a su alcance. Por un lado, las tecnologías como *Blockchain* pueden reducir significativamente los costes *transaccionales.* Además, los costes operativos también pueden recortarse gracias a proyectos de modernización —como el control avanzado de la red, la automatización, el almacenamiento de energía y las microrredes— y mejorar así la rentabilidad de la generación y distribución de energía. Y, por último, a medida que los modelos de negocio se

alejan de la venta de productos básicos hacia recursos energéticos distribuidos, los clientes se integran en la cadena de valor y los sistemas de distribución realizan transacciones de energía en tiempo real, las *utilities* deben invertir en capacidades digitales que habiliten e impulsen los ecosistemas emergentes.

Otra posibilidad que se está abriendo es la Inteligencia Artificial (IA) que ha demostrado ser útil a la hora de predecir desastres naturales, o bien podrá ser utilizada en la predicción climática y por tanto también en las previsiones de funcionamiento de la plantas de energía renovable cuyos recursos, altamente variables y difícilmente predictibles, escapan al control humano. Pero ya se han detectado algunos problemas que manifiesta la IA, y en particular, sus algoritmos, las reglas que rigen a la máquina, que se ven influidos por los sesgos y tendencias del desarrollador o la posibilidad de que las máquinas se descontrolen y supongan una amenaza relevante para el suministro eléctrico. Por ello, el desarrollo de la IA se puede sintetizar en tres preguntas clave *como* podemos enseñar a las máquinas a ser inteligentes, *qué* les enseñamos y *porqué*.

Tanto los humanos como las máquinas necesitamos altas dosis de información para entender lo que pasa a nuestro alrededor. Las máquinas son capaces de representar el mundo exterior a través de paquetes de datos. El contenido de estos datos es vital para la construcción de la «mente artificial» por ello las propias características cognitivas y morales del matemático desarrollador del algoritmo, pues de ellas depende la conciencia de la IA. Esto puede representar un problema pues los sesgos de los desarrolladores pueden acabar trasladándose a la IA.

Los algoritmos utilizados permiten que la IA identifique, clasifique, categorice y generalice mediante los métodos de *machine learning* (aprendizaje automático) y de *deep learning* (aprendizaje profundo), más sofisticado. El primero trata de alimentar a la máquina con altas dosis de datos predefinidos y categorizados por el humano para que la máquina los reconozca en el futuro y reequilibre su modelo de análisis según la experiencia para reducir el margen de error. El segundo, más preciso, hace pasar la información por múltiples «capas», que se asemejan , a una red neuronal, y permite a la IA fijarse en más detalles y crear sus propios modelos de referencia.

El desarrollador, usando machine learning tiene que predeterminar las características principales del objeto, para que así la máquina

sea capaz de comprender qué es, y así poder identificarlo más tarde. En el proceso de deep learning, a través de las múltiples capas, la máquina es capaz de definir patrones a partir de imágenes y obtener las características que definen el objeto por sí mismo. Este método también hace posible que la IA reconozca diferencias sustanciales entre las fotografías y que sea capaz de, por ejemplo, distinguir entre diferentes objetos aunque estos sean similares.

Según la capacidad de identificación y correlación de datos que tenga, la inteligencia artificial se divide en varias categorías. La IA «estrecha» o «débil» se encarga de una tarea automáticamente, haciendo clasificaciones de acuerdo con unos parámetros predeterminados que va puliendo según la cantidad de datos disponible. Se trata de tareas rutinarias y técnicas. El segundo tipo de IA, todavía más teórico que real, es la llamada IA «general» o «fuerte». Supone capacidad de abstracción, reflexión, afán creativo e improvisación.

Para muchos analistas, China tiene todas las ventajas de la carrera por el dominio de la inteligencia artificial. Es un país con un territorio más grande y más diverso en climas y paisajes que sus competidores. Además, poblacionalmente es mucho mayor y la cultura asiática tiene una concepción de privacidad diferente a la occidental. Mayor población significa más datos con los que alimentar a los algoritmos, mientras que la diversidad geográfica supone variedad de escenarios en los que entrenarlos.

La fragilidad de algunas tecnologías de inteligencia artificial se convertirá en una preocupación creciente en el futuro. De alguna manera, el surgimiento de sistemas críticos de IA como objetivos de ataque cibernéticos comenzará a reflejar la secuencia que se vio hace 20 años en internet, lo que atrajo rápidamente la atención de los delincuentes.

Recíprocamente, los defensores dependerán cada vez más de la IA para contrarrestar los ataques, identificar las vulnerabilidades y fortalecer sus sistemas ante posibles ataques. Con el tiempo, esta inteligencia artificial dirigida a la seguridad también podría ayudar a las personas a comprender mejor las concesiones de entregar información personal a cambio del uso de una aplicación u otro beneficio adicional.

La tecnología 5G y el «Internet de las cosas» está ya listo para su difusión comercial. Si bien tomará tiempo que estas redes, los teléfonos y otros dispositivos se implementen de manera generalizada, el crecimiento se producirá rápidamente.

Aunque los teléfonos inteligentes son el foco de interés para la tecnología 5G, es probable que la cantidad de teléfonos con esta capacidad sea limitada durante el año 2020. Sin embargo, con el tiempo, más dispositivos IoT se conectarán directamente a la red 5G en lugar de a través de un enrutador Wifi. La adopción de 5G ampliará la superficie de ataque y hará que los dispositivos sean más vulnerables al ataque directo. Para los usuarios domésticos, también hará que sea más difícil monitorizar todos los dispositivos IoT. En términos generales, la capacidad de realizar copias de seguridad o transmitir fácilmente volúmenes masivos de datos a almacenamientos basados en la nube dará a los atacantes nuevos objetivos.

Estas tecnologías: el blockchain, la inteligencia artificial y el 5G se basan en el flujo de datos con que se alimentan, por ello la digitalización es la clave que va a permitir su desarrollo.

La digitalización debe marcar el paso hacia un aumento tangible del valor de la empresa a través del mayor flujo de efectivo, la reducción de riesgos y la mejora del servicio. Para ello, los cambios digitales deben integrarse en una arquitectura empresarial basada en una sólida comprensión de los costes, los beneficios y la tecnología. Esta estructura define las actividades a realizar y cómo agruparlas y conectarlas. Cualquiera que sea el objetivo, una arquitectura robusta permitirá evitar costosos errores, ofrecer una mayor flexibilidad y actualizarse conforme avanza la tecnología.

Las industrias más avanzadas en digitalización han aplicado con éxito métodos ágiles que acortan los tiempos y siguen la filosofía de «pensar en grande, pero empezar en pequeño, fallar barato, escalar rápido». Pero el sector eléctrico aún está en una etapa temprana de adopción de estos principios. Para comprender la incertidumbre intrínseca a los nuevos modelos de negocio, las empresas deben atravesar un cambio cultural y educar y asesorar a los equipos sobre los riesgos y ventajas de una implementación ágil.

No es fácil para cualquier organización realizar cambios profundos en su estrategia y en su cultura. Pero, para ser competitivas en el siglo XXI, las empresas del sector eléctrico no deben dejar escapar las capacidades y oportunidades que ofrecen las tecnologías digitales.

En la actualidad, el desarrollo y la implementación de la tecnología digital en el sector energético está resultando esencial para

avanzar hacia un nuevo modelo energético sostenible, eficiente y seguro. El sector energético está experimentando un profundo cambio debido a la necesidad de la *descarbonización*, lograr una mayor *descentralización* de la generación de electricidad y facilitar la *digitalización.*

Estas 3 D caracterizan la transición energética que está comenzando a tener algunos efectos profundos en los sistemas eléctricos de todo el mundo. Los dos primeros aspectos, el mayor uso de recursos renovables limpios pero variables y su característica descentralizada, implican el uso de una mayor y generalmente más compleja infraestructura de redes y por consiguiente una mayor cantidad de datos, ya que estas fuentes se ubican normalmente lejos de los centros de consumo eléctrico y el tamaño típico de la planta es mucho menor que el de las centrales térmicas tradicionales.

La digitalización de la totalidad de la cadena de valor del sector energético implica la operación de redes cada vez más complejas y sofisticadas. Las continuas acciones encaminadas a mitigar el cambio climático, la entrada en juego de nuevas tecnologías en el ámbito de las baterías, las energías renovables o el creciente uso del vehículo eléctrico, necesitan de un despliegue paralelo de las redes inteligentes para su respaldo.

El modelo energético futuro, como ya se ha indicado, se puede beneficiar de los avances tecnológicos tanto en la generación, con el desarrollo masivo de las energías renovables, como en las tecnologías de la información, lo que va a permitir el objetivo buscado de centrar el protagonismo en el consumidor. La dispersión de las fuentes renovables y la ubicación de los consumidores reflejará un modelo energético muy descentralizado. Los avances tecnológicos de las comunicaciones, con equipos que reflejan la digitalización de vanguardia y dispositivos inteligentes, harán una realidad las redes inteligentes con un flujo bidireccional de energía e información que se cruzará entre los generadores y clientes, ambos dispersos, con los operadores de distribución y, a su vez, de stos con el operador del sistema.

El desarrollo de la digitalización ha dado lugar a una civilización hiperconectada, que propicia un acelerado progreso tecnológico al tiempo que abre multitud de posibilidades en todos los ámbitos y sectores de actividad. Sin embargo, el proceso de digitalización del sector energético no está exento de riesgos, pues también puede acarrear nuevas amenazas, entre las cuales la ciberdelin-

cuencia es la más evidente. El sector de la energía no es ajeno a esta problemática, dada las graves afecciones que estas acciones de delincuencia pueden acarrear al sistema eléctrico en su conjunto y a las consecuencias económicas que de ellas se derivan. Uno de los grandes riesgos a los que se enfrenta la digitalización es la ciberseguridad en materia de protección de la información y vulnerabilidad de la infraestructura crítica. Un ejemplo de ataque cibernético fue la paralización de Telefónica causada por la infección por el *ransomware Wannacry* en el 2017.

La ciberseguridad eléctrica

Los Sistemas de Control Industrial (ICS) han sido víctimas frecuentes de ataques no dirigidos, infectando con ransomware estaciones de trabajo de operadores u otros componentes de control. Los vectores de entrada fueron, principalmente, correos de phishing y soportes extraíbles, aunque también se evidenciaron casos en los que la infección se produjo como resultado de la utilización de sistemas de mantenimiento remoto configurados incorrectamente. En todos los casos, el código dañino explotó vulnerabilidades conocidas de software obsoleto y una inadecuada segmentación entre las redes de oficina y las redes de producción. Todo parece apuntar que este tipo de incidentes continuará representando una amenaza significativa para los ICS en los próximos años

En Europa, el número de subestaciones eléctricas excede de los 4 millones (Pavla Mandatova 2013 Eurelectric) y estas, a ojos de un atacante, son 4 millones de entradas posibles a la red eléctrica. En las nuevas redes inteligentes, se conectarán nodos sin ninguna medida de ciberseguridad con subestaciones digitalizadas, sistemas de información geográfica, etc. El nivel de seguridad de la nueva red inteligente estará comprometido por el eslabón más débil de la cadena y por este motivo, los operadores se verán obligados a reemplazar por completo esos nodos obsoletos a nivel de ciberseguridad o bien, realizar un proceso de actualización de los mismos.

En general, y cuando los ataques tienen éxito, el plazo para que se vea comprometido el sistema de información sigue siendo muy corto. El tiempo que media entre la primera acción hostil hasta el compromiso de un activo se mide, frecuentemente, en términos de segundos o minutos. Sin embargo, el plazo para su descubrimiento o detección, que depende en gran medida del

tipo de ataque, suele expresarse en días, semanas o meses. Para la consultora PriceWaterhouse en su área de ciberseguridad «el riesgo tecnológico cada vez tiene más peso y hay un punto clave: además de prepararse para proteger sus activos, ahora la empresa tiene que estar preparada para responder. Es importante que sea resiliente a un ataque, que sepa actuar y remediarlo cuanto antes, porque el tiempo es fundamental».

Si bien parece difícil parar a estos ataques avanzados, es necesario poner todos los medios posibles para detectar intrusiones y parar las acciones que puedan comprometer las infraestructuras críticas de un país o de una organización. Para combatir los ataques a las redes eléctricas, existen estándares de seguridad para el intercambio de información e interoperabilidad en las redes eléctricas y para definir el nivel de seguridad y cómo evaluar los riesgos y amenazas de un sistema de control, y qué requisitos de seguridad debe cumplir para alcanzar un nivel de seguridad avanzado.

A medida que los sistemas de control son cada vez más esenciales en la cadena de valor del sector eléctrico (generación, transmisión y distribución) y que los sistemas de tecnología de la información están cada vez más conectados a los sistemas de tecnología operativa, aumentan los riesgos para la ciberseguridad. Según el Foro Económico Mundial, los ciberataques plantearon el riesgo tecnológico más importante en 2018 y el tercero más probable. Por estas razones, el Consejo Mundial de la Energía recomienda que las empresas energéticas consideren los riesgos cibernéticos como riesgos empresariales fundamentales. Las empresas deben cooperar para evaluar, comprender y crear una fuerte resistencia a estos riesgos, que amenazan la continuidad del servicio, los datos y los sistemas, y por tanto la reputación. Los factores técnicos y humanos deben mejorarse, y todas las partes interesadas deben elaborar normas y mejores prácticas para hacer frente a estas amenazas actuales.

Pero cuando hablamos del impacto que puede tener un ciberataque en infraestructuras críticas, y en particular en los sistemas eléctricos, hablamos de una posible afectación a los servicios esenciales a la ciudadanía. Dejar sin luz durante unas pocas horas a una región o incluso un país, es algo a lo que no estamos acostumbrados y sin duda tiene grandes repercusiones, no solo a nivel empresarial, sino a nivel social.

Es por esta razón por la que el sector eléctrico, junto con otros servicios esenciales como el agua, el gas, etc., se están convir-

tiendo cada vez más en el objetivo de los cibercriminales, especialmente cuando lo que se busca es notoriedad y provocar daños importantes a nivel estatal. Y de aquí la relevancia de los organismos públicos que proporcionan una coordinación a nivel nacional de la seguridad en los activos críticos.

Según el Informe Tendencias y Amenazas en 2019 del Centro Criptológico Nacional (CCN-CERT) IA-13/19 se entiende por soberanía digital el impulso de un país para recuperar el control sobre sus propios datos y los de sus ciudadanos. Los Estados, y los grupos patrocinados por ellos, y sus acciones contra otros países siguen representando la ciberamenaza más significativa. El objetivo perseguido por este tipo de ataques es siempre el mismo: sustraer información para mejorar su posición estratégica, política, económica o innovadora y aprovecharse de las vulnerabilidades humanas de la víctima, de la que recaban información sensible o confidencial para un ataque posterior.

En los últimos años, los ataques contra los datos personales se han incrementado, y no solo por parte de ciberdelincuentes o grupos hacktivistas, sino también por Estados. El objetivo perseguido suele ser la comisión de ciertos delitos, el robo de identidad (credenciales), la suplantación o el espionaje. Elementos facilitadores de los ataques. La incesante conexión de nuevos dispositivos IoT a Internet, propiciando con ello la distribución de código dañino o participando en ataques (distribuidos de denegación de servicio) DDoS, constituye también un significativo elemento facilitador de esta problemática.

El número de activistas de las amenazas ha aumentado significativamente debido, en parte, al fácil acceso a nuevas herramientas de ataque y a la dificultad permanente para probar la autoría. Se ha evidenciado un incremento en el uso de código dañino por parte de los Estados, dirigido a explotar vulnerabilidades de los sistemas de información de las infraestructuras críticas. Frecuentemente, el objetivo de tales ataques ha sido obtener información sobre el grado de implantación de las medidas de seguridad de las organizaciones, al objeto de poseer datos suficientes que les permita planificar ataques futuros. Esta actividad se ha detectado, especialmente, contra objetivos europeos. El Instituto Nacional de Ciberseguridad (Incibe) gestiona más de 100.000 incidentes al año de empresas y particulares, de los que unos 700 corresponden a operadores estratégicos (desde eléctricas hasta empresas de telecomunicaciones, puertos…). El incremento de ataques a empresas españolas es bastante alto e inversamente

proporcional al gasto que realizan para garantizar la confidencialidad de los datos. Una inversión que a menudo es pobre, dispersa y casi siempre tiene un sentido de urgencia que la hace inútil para construir una verdadera estrategia de negocio. Es el mal de este tiempo: sociedades más digitalizadas y a la vez más desnudas ante el ciberdelito. Quizá por ello las encuestas muestran un derroche de voluntad. Un estudio realizado por Willis Towers Watson y ESI ThoughtLab, cita que organizaciones de todo el mundo quieren aumentar sus inversiones en ciberseguridad un 34% durante el próximo año, y cerca del 12% lo harán en más de un 50%. Pero quien crea que el dinero arregla el problema se equivoca. Sin soluciones integrales en todos los niveles del negocio la respuesta fallará, según los expertos.

La monetización de la información capturada, la propaganda y el reclutamiento son los objetivos principales de este grupo de agentes de las amenazas. No obstante, dada la disponibilidad del *Crime-as-a-Service* y el potencial sabotaje de dispositivos IoT, el atacante podría dejar el dispositivo fuera de servicio o limitar sus funcionalidades.

Los *hacktivistas* siguen activos en la divulgación de información confidencial recabada en los sitios web atacados, en el desarrollo de acciones DDoS y en la desfiguración de páginas web, con el objetivo de llamar la atención de los medios sin perseguir en general, por el momento, la monetización de sus acciones. Los análisis internacionales muestran que el ciberterrorismo aumentará significativamente en los próximos años.

Hay también una fuente de incidentes de carácter interno. La mayor parte del daño parece ser causado por acciones no intencionadas de los empleados que pueden materializarse con ataques a la cadena de suministro de datos.

Así, también, debe considerarse defectuoso desde la perspectiva de seguridad IT un producto que contiene vulnerabilidades conocidas públicamente en el momento de la compra. El mantenimiento del *software* por parte del fabricante, incluida la eliminación de vulnerabilidades, no solo debe ser el procedimiento habitual y el mecanismo para satisfacer la normativa legal aplicable, sino que también debe ser solicitado por el consumidor, como parte del servicio.

La ciberseguridad está en la agenda de todos los gobiernos y de cualquier industria, también en la de los operadores de la red eléctrica. Para un operador de la red eléctrica, perder el servicio

de un nodo de su red puede afectar a los clientes conectados a ese nodo, o si fuese una infraestructura crítica para su operación, podría afectar a millones de clientes ya que el impacto potencial de un incidente de ciberseguridad, en el que se tome control de la red que intercomunica las diferentes subestaciones y el centro de control, puede tener consecuencias devastadoras.

La creciente utilización de numerosos tipos de dispositivos denominados «inteligentes», combinado con la necesidad de dar soporte a las redes de comunicación que hay detrás, pone de manifiesto la necesidad de creación de nuevos mecanismos de seguridad. Por ello, se erigen como fundamentales, a la hora de abordar potenciales problemas, la implementación de medidas y mecanismos tales como:

- una autoridad a cargo de la ciberseguridad en el sector energético;
- la obligatoriedad de remitir informes de incidentes en el sistema;
- la información al consumidor de los riesgos a los que se enfrenta el sistema en este nuevo contexto.

Todas estas medidas, según indica el informe *Cyber Security Strategy for the Energy Sector*, publicado por el Parlamento Europeo, se deben llevar a cabo bajo unos estándares de seguridad comunes y en armonía con los requerimientos ya establecidos por la UE.

Las amenazas y ciberataques

Las amenazas han pasado de tener objetivos particulares: robo de credenciales, sustracción de información, uso ilegítimo de los activos de la organización, etc., a pretender afectar a lo esencial de un país; así lo recoge el último informe de amenazas del Centro Criptológico Nacional (CCN-CERT) «el objetivo perseguido por este tipo de ataques es […] sustraer información para mejorar su posición estratégica, política, económica o innovadora (espionaje). A este objetivo se ha unido el intento de influir en la opinión pública de los países atacados o interrumpir la normal prestación de servicios esenciales (sabotaje)». Y aparecen nuevos conceptos como la «ciberguerra» o «guerra informática» entre países donde los campos de operaciones ya no son tierra, mar o aire, sino el ciberespacio y las tecnologías de la comunicación, y que

tienen como objetivo alterar o causar perjuicio a una nación atacando sus recursos esenciales, como la electricidad.

En el sector eléctrico, un ejemplo de ello fue el incidente ocurrido en Ucrania con el apagón que sufrieron diversas centrales eléctricas del país, en un ataque con virus informáticos. Un gran número de personas se quedaron sin electricidad durante 6 largas horas, abandonadas al frío del 23 de diciembre de 2015. El mismo virus hizo saltar las alarmas unos días más tarde, al ser detectado en la red que controla el tráfico aéreo del aeropuerto de Ucrania.

El virus se llama BlackEnergy y es el primero en la historia involucrado en un apagón eléctrico generalizado. Antes que él, el virus Stuxnet, obra de Israel y Estados Unidos, dañó seriamente diversas centrales nucleares iraníes, pero no dejó a nadie sin luz.

BlackEnergy es solo una de las piezas usadas en el ataque, llevado a cabo por mercenarios informáticos del más alto nivel. Ucrania, después de dos años de guerra con Rusia, no dudó en señalar a este país como culpable, entendiendo que buscaban sembrar el caos y demostrar su fortaleza ante el país vecino, aunque no se pudo afirmar categóricamente porque los atacantes habían borrado muy bien sus huellas. Fue un ataque sofisticado realizado por un equipo de expertos informáticos que usaron armas diversas de carácter cibernético. Parece que los atacantes tenían un plan, estaban coordinados y sabían cómo usar virus y programas de acceso remoto para cegar las defensas del sistema y provocar cambios no deseados en su infraestructura.

El incidente se desarrolló de la siguiente manera: un empleado de una central eléctrica de Ucrania recibió un mensaje de correo electrónico que le animaba a pinchar en un documento adjunto. Al hacerlo, el adjunto instaló un código malicioso en el equipo que abrió una puerta trasera que utilizaron los atacantes para desplegar, de forma silenciosa, el virus «BlackEnergy» en multitud de equipos de la empresa. Este virus se quedó esperando, en silencio, espiando y aprendiendo todos los movimientos de la central. En un momento dado, los atacantes lo activaron e instalaron a distancia un nuevo módulo a BlackEnergy, llamado KillDisk que está programado para destruir archivos vitales de los ordenadores de una central eléctrica. Después manipularon remotamente los ordenadores para provocar los apagones y los operadores veían impotentes cómo se iban apagando subestaciones mientras ellos no podían recuperar el control de los equipos. Acabado el

trabajo, activaron KillDisk, que destruyó los discos duros borrando así las huellas de los hackers en el sistema.

Para provocar más confusión, orquestaron un bombardeo cibernético de los sitios web y centrales telefónicas de la compañía, de forma que los clientes no podían llamar a la misma ni ser informados por web sobre lo que había pasado. A través del ciberataque se consiguió tomar el control de los sistemas de 3 de las principales distribuidoras regionales de electricidad. Este altercado afectó a subestaciones de 100 y 35 kV y provocó cortes de luz que afectaron a un conjunto de 225.000 habitantes.

En el caso de Ucrania, la capacidad de resiliencia fue crítica para recuperar el servicio en aproximadamente 6 horas al existir un sistema paralelo de emergencia que permitió recuperar el control manual.

El módulo KillDisk ha sido adaptado ahora para atacar sistemas industriales, es el icono de un mundo en el que las infraestructuras críticas, medios de comunicación incluidos, se han convertido en principal objetivo.

Posteriormente, el troyano BlackEnergy fue detectado otra vez en Ucrania, en un ordenador del aeropuerto. No pasó nada y el virus fue eliminado, pero elevó las alertas al máximo pues nadie sabía el alcance de la plaga, si había más escondidos en otros ordenadores o si podrían afectar a comunicaciones ferroviarias u otros puntos críticos.

Pasaron los años y BlackEnergy fue modificado para ampliar clientela. Ha sido el responsable en fraudes bancarios o distribución de correo basura, hasta llegar a la más alta meta de un virus troyano: el espionaje electrónico con motivación política. En 2014, BlackEnergy fue detectado en más de 100 organizaciones gubernamentales y empresariales de Polonia y Ucrania. También en ordenadores de la OTAN, la burocracia europea, una universidad norteamericana y un proveedor francés de telecomunicaciones.

La Corporación de Energía Nuclear de la India (NPCIL, por sus siglas en inglés) ha confirmado que recientemente la mayor y más moderna planta nuclear del país fue atacada con un *software* maligno. El virus empleado se ha encontrado anteriormente en ciberataques vinculados a grupos de Corea del Norte.

El ciberataque se conoció públicamente cuando la web VirusTotal publicó un envío de datos que parecía apuntar a una falla en el sistema de la planta, localizada en Tamil Nadu, en el sur del

país. Los datos indicaban la presencia de un *dtrack*, un programa maligno, aunque los responsables de la planta nuclear publicaron un desmentido, pero según expertos podría existir una brecha de seguridad.

El Equipo de Emergencias Cibernéticas tuvo conocimiento del ataque y el problema fue investigado inmediatamente por especialistas del Departamento de Energía Atómica.

El sector nuclear es uno de los más importantes de la India. El NPCIL opera 22 reactores en siete puntos del país.

Según un informe de Naciones Unidas publicado el pasado agosto, los grupos cibernéticos de Corea del Norte (muchos de los cuales operan bajo control directo del Gobierno) se han extendido gracias a su «creciente sofisticación» y han aportado a Pyongyang unos 2.000 millones de dólares (unos 1.800 millones de euros) que ha empleado en su programa de armamento de destrucción masiva.

La política india, es llevar Internet a la vasta población del país en el marco del programa India digital, criticado por la ausencia de leyes de ciberseguridad y marco legal actualizado. Delhi anunció licitaciones para que empresas privadas preparen la mayor red de reconocimiento facial del mundo, que se unirá al sistema biométrico nacional en el que ya están inscritos más de mil millones de ciudadanos, a pesar de las continuas filtraciones de datos privados de sus usuarios.

El *dtrack* fue usado en un ataque de 2016 en el que fue robada información financiera de millones de indios, señalan los expertos. La empresa de ciberseguridad Kaspersky ha asegurado que el virus guarda «similitudes con la campaña DarkSeoul», un programa de espionaje a bancos y medios de comunicación surcoreanos atribuidos al Grupo Lazarus, conectado con grupos ciberterroristas de Corea del Norte.

En septiembre de 2017, la misma empresa Kaspersky reportó lo que se ha denominado Dragonfly 2.0 —una serie de intrusiones en *utilities* de todo el mundo. Durante los últimos seis años, estos atacantes se han infiltrado en el control de las redes eléctricas de varios países, entre ellos EE. UU.

Existen precedentes de otros ataques de grupos organizados sobre importantes infraestructuras críticas. Esta es hoy en día una de las grandes preocupaciones de gobiernos de todo el mundo: las graves inseguridades que presentan muchos sistemas críti-

cos, como plantas nucleares, centrales eléctricas o sistemas de control del tráfico. Las infraestructuras críticas tienen debilidades y en estos momentos hay grupos recolectando información sobre ellas en casi todos los países.

Según una reciente encuesta a las industrias del gas y el petróleo, los ataques informáticos a estas instalaciones se han incrementado de forma generalizada. La mitad de encuestados aseguran que el aumento ha sido de entre el 50 y el 100 %.

Un incidente como el de Ucrania nos demuestra que, con un simple clic en un adjunto de correo electrónico, se puede iniciar un desastre que deje a hospitales e industria seis horas sin energía eléctrica. Debemos buscar la visibilidad total e integrada de lo que está pasando en nuestras infraestructuras y correlacionar todos los eventos de forma integrada.

El enfoque clásico para protegerse las organizaciones contra los ciberataques se basaba en la defensa del perímetro; consistía en segmentar las redes y poner barreras de seguridad para impedir que los atacantes externos pudieran acceder a los sistemas internos de las compañías. En el caso de los sistemas eléctricos, se aislaban totalmente del resto de redes internas y externas, con lo que quedaban menos expuestos a posibles intrusiones.

Esta estrategia está siendo cada vez menos efectiva, dado que con la digitalización y las nuevas tecnologías, las nuevas formas de trabajo en las empresas exigen a las compañías adaptar sus sistemas para ser accesibles desde un mayor número de dispositivos y desde diversas ubicaciones, para poder explotar mejor la información de la compañía. En el caso concreto de los sistemas eléctricos, la proliferación de arquitecturas de tipo *IoT* (Internet de las cosas) para poder recopilar datos de sensores, o el uso de grandes soluciones de *Big Data* están llevando a las compañías a abordar nuevos métodos para proteger adecuadamente los sistemas críticos de acuerdo con los retos que se presentan en estos escenarios.

En este desarrollo de nuevas arquitecturas también aparecen nuevas soluciones de seguridad para mitigar y evitar los nuevos ataques. Estas soluciones se apoyan en los avances de analítica, inteligencia artificial y *Big Data*, y facilitan la detección y la respuesta ante ataques de diversa índole.

La evolución de estos sistemas está despegando aunque, en las soluciones específicas para sistemas eléctricos debido a lo reciente del cambio de paradigma tecnológico, son en algunos casos solo experimentales.

Las tendencias para el futuro

En el informe mencionado del CCN-CERT figuran las tendencias para futuro próximo, donde los agentes estatales continuarán realizando campañas de intrusión como parte de sus estrategias nacionales y es seguro que para ello utilizarán sus cibercapacidades.

Las entidades de los sectores del gobierno, la defensa, los *think tanks* y las ONG continuarán siendo los objetivos prioritarios de sus operaciones. Estas intrusiones, probablemente, serán respaldadas por proveedores de los sectores de telecomunicaciones y tecnología, y pueden incluir compromisos en la cadena de suministro, como se ha observado en los años precedentes. Es de esperar que los futuros ciberataques incrementen su volumen y su sofisticación. Los siguientes párrafos esbozan lo que cabe esperar del inmediato futuro:

- Aumentarán los ciberataques patrocinados por Estados;
- Ataques a la cadena de suministro;
- La nube como objetivo;
- Sofisticación del código dañino;
- Los ciberataques dirigidos a personas;
- Utilización de dispositivos inteligentes en ciberataques;
- Permanencia de los ataques DDoS y su relación con la IoT;
- Incremento del *Criptojacking*;
- El código dañino será más engañoso;
- Aprendizaje automático para bloquear nuevas amenazas;
- IA como herramienta en los ciberataques;
- La adopción de 5G ampliará la superficie de ataque.

Las actuaciones y normativa comunitaria

El estado actual de la ciberseguridad en el sector energético en la UE indica que todavía queda camino por recorrer. Los sistemas inteligentes de energía, englobados actualmente en las *Smart Grids,* requieren de avances en materia de consistencia para la totalidad de la UE, de cara a evitar daños en el sistema. Precisamente, es necesario tener en cuenta que el camino para una transición energética exitosa pasa por solucionar este tipo de in-

cidentes y evitar situaciones tales como la que ocurrió en Ucrania el pasado 23 de diciembre de 2015.

Las autoridades europeas son conscientes de los riesgos inherentes a cuatro grandes sectores «ciberdependientes», como son el transporte, la salud, las finanzas y la energía. La denominada «Internet de las cosas» —interconexión digital de los objetos cotidianos— es ya una realidad, y se prevé que en 2025 haya decenas de miles de millones de dispositivos digitales conectados en la UE. Al tiempo, los sistemas informáticos pueden verse afectados por incidentes de seguridad, desde fallos técnicos a virus, cada vez más frecuentes y difíciles de combatir.

Si nos ceñimos al sector energético europeo, este se encuentra en pleno proceso de transición hacia la «descarbonización», con un fuerte componente de descentralización de la generación. El progreso tecnológico y la digitalización están modificando las redes eléctricas y de gas europeas. Lo que comporta riesgos de exposición a ciberataques e incidentes que pueden poner en peligro la seguridad del suministro. De lo que se trata es de evaluar esos riesgos, y adoptar medidas para mitigarlos.

Por todo ello, ya en julio de 2016 en la Unión Europea, se aprobó la llamada Directiva SRI (sobre seguridad en las redes y sistemas de información), cuyo objetivo era incrementar la ciberseguridad en la UE desarrollando las capacidades nacionales en la materia, incrementando la cooperación a escala europea e introduciendo requisitos en materia de seguridad y de notificación de incidentes para los «operadores de servicios esenciales», que incluye la notificación obligatoria de incidentes en sectores como el de la energía.

Estos operadores de servicios esenciales deben tener en cuenta las directrices de un grupo de cooperación establecido por la Directiva SRI, integrado por representantes de los Estados, de la Agencia de la Unión Europea para la Ciberseguridad (Enisa) y de la Comisión. En junio de 2018, este Grupo creó una línea de trabajo específica sobre la energía. Teniendo en cuenta que cada sector de actividad económica se enfrenta a problemas específicos de ciberseguridad, se hace necesario desarrollar enfoques sectoriales en el marco más amplio de las estrategias generales de ciberseguridad.

El pasado 3 de abril, la Comisión de la Unión Europea publicó la Recomendación 2019/553 sobre ciberseguridad en el sector de la energía. A pesar de tratarse de un acto legislativo de rango me-

nor, el posicionamiento de la Comisión supone un reforzamiento de las numerosas iniciativas que se vienen sucediendo a favor del impulso a la seguridad informática.

La asociación de gestores de redes europeas de transporte de electricidad (ENTSO-E) está debatiendo un documento sobre esta materia. El documento de «ENTSO-E Cyber Security Strategy» está aún en elaboración. Este documento ha sido elaborado en el Digital Committee, que reconoce que con el aumento de los intercambios de información y conectividad entre TSO y DSO (operadores del sistema y de la distribución) de servicios (digitalización, Internet, etc.) respectivamente, se está incrementando el riesgo sobre la ciberseguridad. Por todo ello, es fundamental tener una estrategia común en cuanto a ciberseguridad que permita hacer frente a los riesgos que vengan, y de una forma menos costosa para los TSO (aprovechando sinergias y compartiendo conocimiento).

La estrategia se centra en tres pilares básicos:

- Seguro y resiliente: prevención y cumplimiento (seguro), monitorización, respuesta, recuperación (resiliente).
- Inter-TSO y DSO: se centra en aspectos comunes (la ciberseguridad de cada TSO queda a nivel nacional).
- Información, servicio e infraestructura: estrategia integral que abarca todos los niveles/aspectos.

En el borrador de documento figuran como temas estratégicos, 4 elementos que se consideran claves en el concepto de la ciberseguridad:

- *Gestión de riesgos*: Se trata de identificar los activos críticos de la red eléctrica europea (sobre todo los afectados por ENTSO-E), y hacer un plan de mitigación de riesgos asociados. Destacan la necesidad de cumplir con los estándares internacionales sobre identificación/gestión de riesgos de ciberseguridad, etc.
- *Arquitectura*: Es fundamental asegurar la ciberseguridad desde el inicio, desde el diseño/planificación, realizar tests de ciberseguridad y auditorías.
- *Apoyo y servicios centrales* (ENTSO-E): Esta organización quiere proporcionar soluciones comunes y plataformas para compartir información y mejores prácticas sobre identificación de amenazas, mecanismos de mitigación, etc. Destacan

además la importancia de impartir programas formativos en materia de ciberseguridad, ya que la clave no es el sistema sino la persona que lo usa.

– *Gobernanza*: El objetivo es que todos los TSO puedan tener madurez suficiente y conocimiento/compromiso sobre ciberseguridad. El Digital Committee de ENTSO-E sería el organismo supervisor del cumplimiento de la estrategia.

La Comisión Europea ha concedido a ENTSO-E (a través de un programa de fondos de la CE: Connecting Europe Facility) una partida para proyectos de innovación en materia de ciberseguridad. Esto permitirá optimizar costes de ENTSO-E y además va en línea y complementa la estrategia planteada.

Por último, es muy probable que la CE haga un código de red sobre ciberseguridad en el futuro. Por tanto, los TSO deben estar preparados para afrontar y cumplir los estándares exigidos por el futuro NC.

La cooperación internacional en ciberseguridad

La cooperación y el intercambio de información son elementos clave en esta materia, y a tal efecto la Comisión ha puesto en marcha iniciativas como la Mesa Redonda (Roma, marzo de 2017) o la Conferencia de Alto Nivel (Bruselas, octubre de 2018) sobre ciberseguridad en el sector de la energía, además de haber impulsado entidades especializadas, como el Centro Europeo de Puesta en Común y Análisis de la Información Energética.

También se ha creado un marco europeo de ciberseguridad para la certificación de productos, procesos y servicios, que será válido en toda la Unión y reviste especial interés para el sector de la energía. Y existe el compromiso de la Comisión de revisar periódicamente sus recomendaciones en esta materia a partir de los progresos realizados «en concertación con los Estados miembros y las partes interesadas».

La iniciativa aprobada por el Ejecutivo europeo aspira, en definitiva, a orientar en materia de ciberseguridad a los Estados miembros y a las partes interesadas, «en particular a los operadores de redes y proveedores de tecnología», teniendo en cuenta tres condiciones específicas: los requisitos específicos de tiempo real del sector energético, los efectos en cascada, y la combinación de tecnologías tradicionales y de vanguardia.

En cuanto a los requisitos de tiempo real de los componentes de la infraestructura energética, se insta a los Estados miembros a velar por que las partes interesadas (operadores de redes de energía y proveedores de tecnología) apliquen medidas de preparación específicas, teniendo en cuenta que algunos elementos del sistema energético, como los relés y protecciones deben reaccionar en milisegundos, lo que dificulta introducir medidas de ciberseguridad.

De ahí que la recomendación europea apele a los operadores de redes de energía para que apliquen las normas de seguridad más recientes para las nuevas instalaciones y estudien medidas complementarias de seguridad física en instalaciones antiguas, además de garantizar una comunicación segura, en tiempo real, cuando haya disponibilidad de productos *ad hoc* en el mercado.

También se sugiere recurrir a redes privadas para programas de teleprotección con el fin de garantizar el nivel de calidad del servicio requerido para las restricciones de tiempo real, así como dividir el sistema general en zonas lógicas y, dentro de cada una, definir restricciones de tiempo y procesos.

Cuando sea posible, los operadores de redes de energía también deberían elegir un protocolo de comunicación segura teniendo en cuenta los requisitos de tiempo real, así como introducir un mecanismo de autenticación adecuado para la comunicación de máquina a máquina, en el que se aborden esos mismos requisitos.

Los denominados «efectos en cascada» hacen referencia al hecho de que las redes eléctricas y los gasoductos están fuertemente interconectados en toda Europa, y un ciberataque que provoque una disrupción o la interrupción de una parte del sistema energético podría desencadenar serias consecuencias en cualquier parte del sistema.

También se recomiende a los Estados miembros velar por que operadores de redes de energía y proveedores de tecnología apliquen medidas de preparación adecuadas, previa evaluación de la interdependencia y la condición más o menos crítica de los sistemas de generación de electricidad y de demanda flexible, las subestaciones y líneas de transmisión y distribución, y las partes que se verán afectadas (también en situaciones transfronterizas) ante la eventualidad de un ciberataque o un ciberincidente.

Asimismo, los Estados miembros también deben velar por que los operadores de redes de energía dispongan de un marco de

comunicación estructurado para compartir señales de alerta temprana y cooperar en la gestión de crisis. Las medidas concretas que la Comisión Europea recomienda a los operadores de redes de energía incluyen velar por que los nuevos dispositivos (como los del «Internet de las cosas») mantengan un nivel de ciberseguridad adecuado. Asimismo, tendrán que considerar los efectos ciberfísicos al establecer y revisar periódicamente los planes de continuidad de las actividades y establecer criterios de diseño y una arquitectura para una red resiliente, que contenga, al menos, los siguientes aspectos:

- Medidas de defensa en profundidad en cada sitio, adaptadas por emplazamiento y adaptadas a su criticidad.
- Identificación de los nodos cruciales, tanto en términos de capacidad de producción de energía como de repercusión para el cliente.
- Colaboración con otros operadores y proveedores de tecnología para evitar efectos en cascada.
- Diseño y creación de redes de comunicación y control que permitan confinar los efectos de los posibles fallos de equipos y sistemas a partes limitadas, y garantizar medidas de mitigación rápidas y adecuadas.

A este respecto, es importante, que siempre que sea posible, incorporar a la normativa, las normas de ciberseguridad internacionalmente aceptadas, y a que tanto las partes interesadas como los clientes, al conectar dispositivos a la red, adopten este enfoque.

Los proveedores de tecnología deberían aportar soluciones ya experimentadas, tanto en tecnologías tradicionales como de vanguardia, de forma gratuita y tan pronto como se tenga conocimiento del problema. Y a los operadores de redes se les insta a adoptar una serie de medidas en sus operaciones, entre las cuales cabe destacar las siguientes:

- Analizar los riesgos de conectar dispositivos tradicionales con otros del «Internet de las cosas».
- Tomar las medidas necesarias contra ataques malintencionados procedentes de dispositivos de consumo controlados de forma maliciosa.
- Establecer una capacidad automatizada de seguimiento y análisis de problemas de seguridad (intentos fallidos de iniciar sesión, alarmas de apertura de puertas…).

- Llevar a cabo periódicamente análisis específicos del riesgo de ciberseguridad en todas las instalaciones tradicionales, especialmente cuando se conectan tecnologías antiguas y nuevas. Mantener actualizado el *software* y el *hardware* de los sistemas tradicionales y del «Internet de las cosas».
- Considerar la ciberseguridad al redactar licitaciones. Colaborar con los proveedores de tecnología para sustituir los sistemas tradicionales cuando sea preciso.

El reciente informe Cybersecurity Report on Europe's Electricity and Gas Sectors, publicado por el Consejo Europeo de Reguladores Energéticos (CEER por sus siglas en inglés) se centra en examinar la ciberseguridad, una de las prioridades más importantes de los distintos Estados Miembros de la Unión Europea, ya que actualmente están trabajando para cumplir con los plazos establecidos por la legislación vigente, especialmente con respecto a la Directiva sobre Seguridad de las Redes y Sistemas de Información. En los últimos años, varias vulnerabilidades de seguridad cibernética se han hecho más que visibles en el sector energético resaltando la necesidad de seguir trabajando activamente en la consolidación de nuevas medidas de resistencia ante este tipo de amenaza. Con el objetivo de superar esta problemática, y tomando en cuenta los esfuerzos en curso para implementar la regulación relacionada con la seguridad cibernética ya existente, los autores del informe ofrecen una serie de recomendaciones que contribuyen a reducir la brecha entre la situación actual y la situación óptima de ciberseguridad en el sector energético.

Las recomendaciones propuestas hacen referencia a la necesidad de aumentar la participación de los reguladores europeos de energía, activar la colaboración entre las partes involucradas y proporcionar una mejor orientación sobre los tipos de medidas y actuaciones a seguir. Para ello, se hace necesario identificar los diferentes actores que juegan, o pueden jugar en el futuro, un papel activo en la compleja resolución de los problemas de ciberseguridad para el sistema energético. Según los autores del informe, aunque no se trata de una lista cerrada, entre los agentes descritos destacarían TSO, DSO, proveedores, generadores y operadores de mercado. Otra tarea prioritaria resaltada en el informe, pasa por dar un papel más relevante a CEER y ACER (Agencia para la cooperación de los reguladores de energía de la Unión Europea), ya que ambos organismos pueden contribuir significativamente al establecimiento de una cultura de ciberseguridad internacional y respaldar y complementar el trabajo de

las Agencias nacionales de regulación. De las evidencias anteriores, los autores concluyen que la cooperación entre los distintos miembros será de vital importancia para contribuir a la creación de un ecosistema homogéneo y seguro, que permita el desarrollo de una cultura adecuada para una mayor innovación y digitalización en el sector energético.

El fortalecimiento de la ciberseguridad y el impulso a nuevas tecnologías como *Blockchain* no conocen fronteras. La cooperación internacional en esta materia es necesaria por los beneficios que pueda reportar el poner en común experiencia y conocimientos. La colaboración se articula mediante las áreas de asuntos internacionales y de vinculación institucional donde se identifican oportunidades de colaboración y se instrumentan programas de trabajo para desarrollar regulaciones más eficaces y operaciones más confiables en el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista.

De acuerdo con el Banco Interamericano de Desarrollo, el cibercrimen le cuesta al mundo hasta 575 mil millones al año, lo que representa 0,5 % del producto interno bruto global. En ese sentido, diseñar, mejorar y fortalecer los sistemas eléctricos, es una tarea estratégica, ya que de ello dependen distintas actividades económicas, y servicios indispensables que garantizan la seguridad y el bienestar de la población. Es por ello que México publicó en 2017 la *Estrategia Nacional de Ciberseguridad* con la visión al año 2030, y desde la parte regulatoria, su comisión reguladora publicó el *Código de Red*.

México y Alemania pretenden ser socios estratégicos en la cooperación dirigida al sector energético. Por encargo del Gobierno Federal de Alemania, la Cooperación Alemana para el Desarrollo Sustentable (GIZ) apoya a las instituciones mexicanas para aumentar la sostenibilidad del sistema energético a través del impulso de las fuentes de energía renovable y la eficiencia energética. Para alcanzar dichos objetivos e impulsar sistemas y mercados energéticos más seguros, confiables y ambientalmente sostenibles, la GIZ implementa programas y actividades de fomento y divulgación, de capacitación, de intercambio de mejores prácticas y de sensibilización y asesoría especializada.

En el marco de esta colaboración, se realizaron foros con participación de expertos del sector público, privado y la academia, la conclusión fue que México debe aprovechar la digitalización para mejorar la confiabilidad y la ciberseguridad en el sector eléctrico.

Se celebraron dos eventos para impulsar el diálogo sobre la digitalización en el desarrollo de sistemas eléctricos frente al desafío que representan los potenciales ciberataques a la infraestructura del sector. El primer evento, «Ciberseguridad en el sector eléctrico» fue implementado por la GIZ, en coordinación con la Comisión Reguladora de Energía (CRE) y el Centro Nacional de Control de la Energía (CENACE). En dicho encuentro los asistentes tuvieron la oportunidad de adquirir e intercambiar conocimientos con expertos tanto de las instituciones organizadoras como de la Escuela de Regulación de Florencia, el Instituto de Investigaciones en Energía Eléctrica (EPRI), el Instituto Nacional de Electricidad y Energías Limpias (INEEL) y la Asociación Alemana de Energía e Industria del Agua (BDEW). De la misma manera, se presentaron casos prácticos de países como Alemania, Estonia y México, este último a través de la Comisión Federal de Electricidad (CFE). En las sesiones se discutieron desafíos comunes, las políticas y regulaciones asociadas a la protección de infraestructura crítica que subyacen a la digitalización, y la seguridad cibernética en el sector eléctrico.

En el segundo evento, «Encuentro entre Blockchain y energía», además de la Alianza Energética y la CRE, participaron Blockchain Lab y DKTI Solar, de la GIZ. En este evento, los asistentes conocieron la aplicación Blockchain para redes privadas a través de experiencias internacionales como la de Estonia, país precursor en el uso de esta tecnología para facilitar operaciones de gobierno; y Chile, quien ha iniciado la transformación en Latinoamérica con el uso de plataformas abiertas en el sector regulatorio de energía, así como el uso potencial para detectar ciberataques para darle mayor confiabilidad a la red eléctrica.

Las redes eléctricas, hoy en día, son cada vez más modernas, más inteligentes… y más conectadas. Anteriormente ya se ha mencionado que estamos encarando un nuevo mundo energético. Un mundo de generación energética descentralizada, de fuentes renovables intermitentes, como la solar y la eólica, así como un creciente compromiso por parte de los usuarios.

Pero con todas las ventajas de una red más flexible, dinámica y conectada, también entran en juego nuevos riesgos y amenazas de seguridad, en concreto, de ciberseguridad. Dada la importancia de esta debe existir una regulación y una vigilancia de su cumplimiento.

Las medidas de ciberseguridad deben cumplir con los estándares y con las normativas. Este enfoque beneficia al sector, au-

mentando la conciencia de los riesgos y los retos asociados a un ciberataque.

Las entidades reguladoras han previsto la necesidad de un enfoque estructurado de ciberseguridad. En Estados Unidos, los requerimientos de protección de infraestructuras críticas, de la Corporación de Seguridad Eléctrica Norteamericana (NERC CIP), establecen que cosas son necesarias para asegurar el sistema eléctrico en Norteamérica. El Programa Europeo para la Protección de las Infraestructuras Críticas (EPCIP) hace lo mismo en Europa.

Debido al cambio hacia plataformas de comunicación abiertas, como Ethernet e IP, los sistemas que gestionan las infraestructuras críticas se han vuelto cada vez más vulnerables. El enfoque informático de la ciberseguridad no siempre es apropiado con las limitaciones operacionales a las que se enfrentan las compañías eléctricas.

A medida que las compañías eléctricas experimentan una convergencia entre IT y OT, es cada vez más necesario desarrollar equipos multifuncionales para abordar retos únicos de tecnología segura que abarquen ambos mundos. Proteger contra las ciberamenazas actuales requiere una mayor colaboración entre ingenieros, responsables de las instalaciones críticas y responsables de seguridad, que deben compartir sus conocimientos para identificar los posibles problemas y ataques que afectan a sus sistemas.

Diseño de protecciones de ciberseguridad

Una protección adecuada requiere todo un conjunto de medidas, procesos, medios técnicos y una organización apropiada. Contar con una buena defensa contra ciberataques es un proceso continuo y requiere un esfuerzo constante.

Para establecer y mantener sus sistemas ciberseguros, las compañías eléctricas pueden seguir un enfoque basado en cuatro puntos:

- *Realizar una evaluación de riesgos.* El primer paso consiste en llevar a cabo una evaluación integral del riesgo basada en amenazas internas y externas. Al hacerlo, los especialistas en OT y otras partes interesadas de las compañías eléctricas podrán entender cuáles son sus puntos más vulnerables, y documentar la creación de políticas de seguridad y mitigación de riesgos.

- *Diseñar una política y procesos de seguridad*. La política de ciberseguridad de una compañía eléctrica proporciona un conjunto de reglas a seguir. Estas deben ir encabezadas por el conjunto de estándares de la Organización Internacional de Estandarización (ISO) y de la Comisión Electrotécnica Internacional, que proporcionan recomendaciones y buenas prácticas sobre gestión de la seguridad de la información. En ellas se describe la lista de activos que deben protegerse, identifica las amenazas a dichos activos, las acciones no autorizadas y la consiguiente responsabilidad en caso de violación de la política de seguridad. También es importantes contar con procesos de seguridad bien diseñados. Los procesos del sistema de ciberseguridad deben ser revisados y actualizados regularmente, para seguir esta evolución. Una de las claves es realizar una revisión una o dos veces al año.
- *Ejecutar proyectos que implementen el plan de mitigación de riesgos.* Es importante seleccionar una tecnología de ciberseguridad que se base en estándares internacionales, para asegurar que se puede seguir una política de seguridad apropiada y las acciones de mitigación de riesgo propuestas. Un enfoque de «seguridad desde el diseño» basado en estándares internacionales puede ayudar a reducir aún más el riesgo, al asegurar los componentes del sistema.
- *Gestionar el programa de seguridad.* Una gestión eficaz de los programas de ciberseguridad implica también la gestión de los ciclos de vida de los activos de información y comunicación. Para ello, es importante mantener una documentación rigurosa y «viva» sobre el *firmware* de los activos, los sistemas operativos y las configuraciones.

También requiere conocer de forma exhaustiva la previsión de las actualizaciones y de la obsolescencia tecnológica, además de ser consciente de las vulnerabilidades conocidas y los parches existentes. La gestión de la ciberseguridad también requiere que ciertos eventos provoquen una evaluación, como determinados puntos en los ciclos de vida de los activos o como las amenazas detectadas.

Una de las pautas que cobra más importancia, dadas las características de este tipo de incidentes, es la elaboración de un análisis exhaustivo de los *logs* de acceso. Este análisis debería ayudar a esclarecer los hechos y a sacar conclusiones con un fundamento más concreto, acerca de la intencionalidad, o no, del fallo en el servicio eléctrico.

Como conclusión más importante ante este tipo de situaciones se resalta la importancia que tiene el intercambio de información de ciberataques y el tratamiento que se da a los mismos. De esta manera, otras empresas podrán extraer lecciones aprendidas, como implementar procedimientos en el caso de sufrir un fallo, o detectar algún problema en la infraestructura de red, basándose en las acciones ejecutadas por otros.

En las compañías eléctricas, la seguridad es asunto de todos y no basta con instalar tecnología. También deben implementar procesos organizativos para hacer frente a los retos de una red descentralizada. Esto significa evaluar de forma regular y mejorar continuamente su proceso de ciberseguridad y seguridad física, para salvaguardar nuestro nuevo mundo energético.

Sin embargo, el análisis de riesgos de ciberseguridad o simplemente un análisis de las vulnerabilidades conocidas de un sistema de control todavía es una actividad poco demandada por las *utilities* en el sector eléctrico.

La evaluación de riesgos de ciberseguridad incorpora metodología del análisis de riesgos de seguridad tradicional, que se complementan y proveen seguridad (*safety*) y ciberseguridad desde las fases tempranas de un sistema.

Para la gestión de ciberseguridad es mejor definir los requisitos/medidas de ciberseguridad que un sistema debe cumplir en la fase de diseño y mantener el nivel de seguridad del sistema durante el ciclo de vida del proyecto. Esto aplica tanto a sistemas como a componentes del sistema.

Una vez que se ha realizado la estimación de los riesgos de ciberseguridad, hay que determinar las medidas necesarias y suficientes para alcanzar el nivel de seguridad deseado para el producto o sistema analizado. El objetivo es realizar un análisis de riesgos durante la fase de diseño. Se evalúa la seguridad desde el diseño en 4 aspectos:

- Plataformas seguras. Considerar la ciberseguridad desde la fase de diseño de un sistema o producto permite seleccionar el *hardware* y *software* más adecuado sobre el que se construirá la solución.

  Medidas de seguridad como arranque seguro de un sistema, certificados de autenticación, etc., se basan en plataformas seguras y en algoritmos avanzados de criptografía. Definir los requisitos de seguridad desde la fase de diseño permitirá

identificar los componentes necesarios para alcanzar el nivel de seguridad deseado y evaluar la plataforma para evitar problemas de capacidad de cómputo o memoria.

- Aplicaciones seguras. Al realizar un análisis de riesgos e identificar las posibles amenazas en una fase anterior al diseño y codificación de una aplicación, se desarrollará pensando en contramedidas posibles para esas amenazas, mejorará los eventos, *logs* y evidencias que faciliten la investigación de un ataque y en definitiva será más robusta.
- Productos seguros. Un producto seguro se basa en plataformas y aplicaciones seguras. Se debe realizar un proceso de asegurar el sistema mediante la reducción de las vulnerabilidades del mismo, minimizando los permisos con los que corren las aplicaciones, configurando los servicios siguiendo las buenas prácticas de los fabricantes, minimizando los servicios instalados y los puertos accesibles desde interfaces seguras y no seguras.
- Arquitecturas seguras. Por último, también se debe considerar la definición de arquitecturas seguras durante la fase de diseño con la creación de diferentes zonas de seguridad, las cuales serán analizadas independientemente para ver el nivel de seguridad que deben alcanzar dependiendo de su criticidad, el número de amenazas presentes y la probabilidad de que ocurran.

Una vez hecha esta segregación por zonas, se debe identificar el tráfico entre zonas e implementar medidas de seguridad acordes, tal como, se refleja en la figura 5.

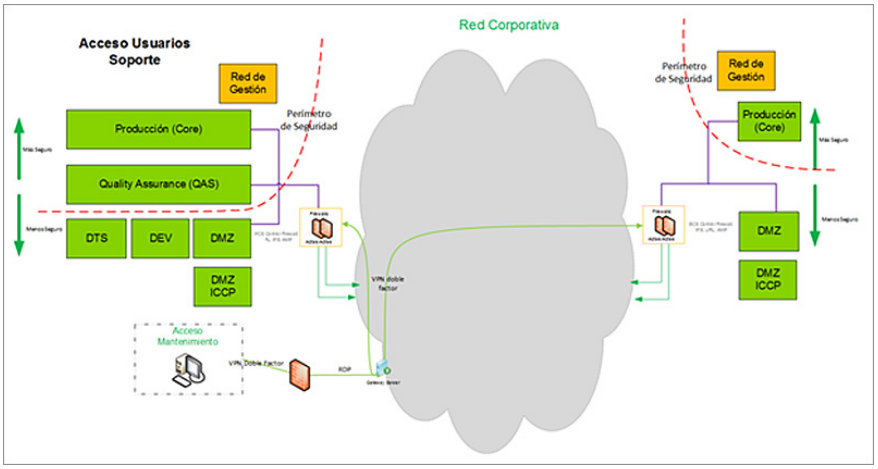


Figura 5. Segmentación y medidas de seguridad perimetral para un DMS avanzado.

La seguridad de un sistema se debe basar en procesos maduros para asegurar que las medidas definidas se consideran en cada etapa de la vida de un sistema. El estándar IEC-62443, que se expone en la figura 6, define 4 niveles de seguridad y describe qué requisitos funcionales debe cumplir un producto o un sistema para alcanzar el nivel deseado.

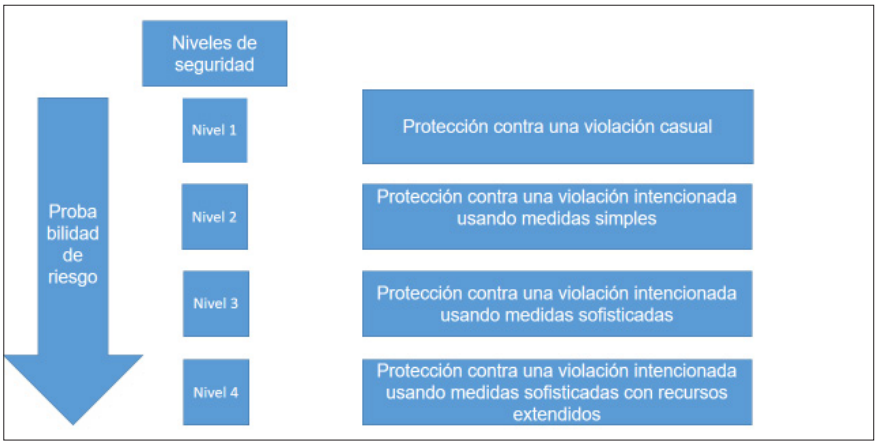


Figura 6. Niveles de seguridad definidos por IEC-62443.

Medidas de ciberseguridad a un sistema de control existente

A continuación, se expone el proceso para incrementar el nivel de seguridad de un SCADA, un DMS o una subestación eléctrica. Para ello se va a seguir el estándar IEC-62443.

Para asegurar que se está listo para empezar la actualización del sistema y limitar el tiempo en el que el mismo estaría sin operar debido a estas actividades de actualización, se han marcado en azul los trabajos que se deben realizar *in situ* y en color naranja aquellos trabajos que se pueden llevar en oficina o sin influenciar en la operación del sistema.

El primer paso, ver figura 7, para defender un sistema es conocer qué se va a defender, algo básico, pero a veces olvidado. Tanto el dueño del activo como el responsable del proyecto de actualización del sistema debe realizar este ejercicio de colección de información *in situ*. Durante este proceso, un experto de ciberseguridad realizará tareas no intrusivas sobre el sistema para obtener información de todos los componentes del sistema, como tipo de dispositivo. Además, se llevarán a cabo entrevistas con el personal responsable para:

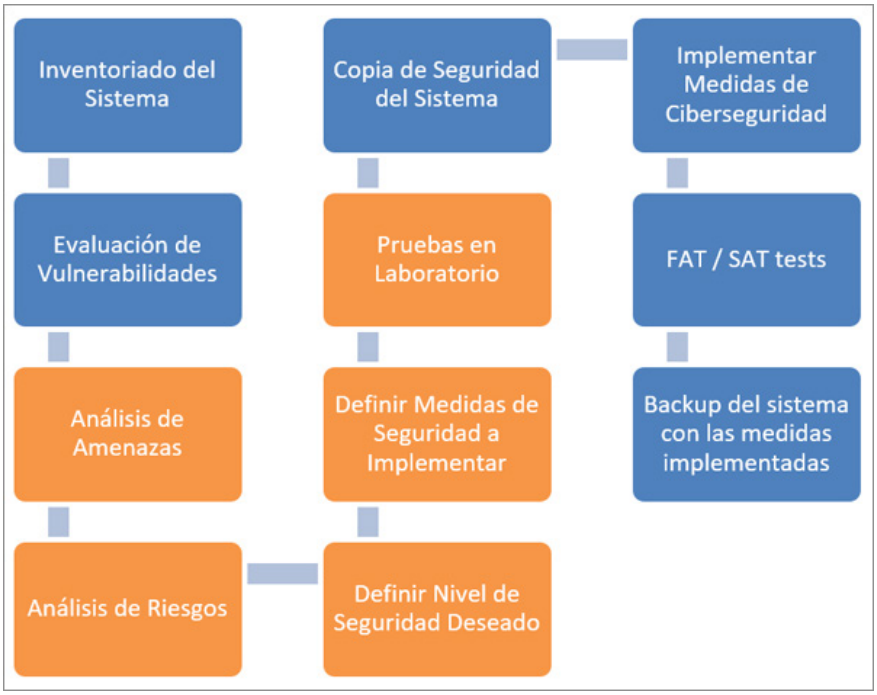


Figura 7. Flujo de trabajo de implementación de medidas de seguridad en un proyecto existente.

- Recolectar arquitectura de red del sistema y otros posibles subsistemas existentes.
- Inventarios existentes (activos, configuraciones).
- Políticas de seguridad o normativas aplicables.
- Evaluación de vulnerabilidades del sistema.

Este proceso se podrá hacer *in situ* o en *back-office* usando la información recogida. Dependiendo de la criticidad del sistema se optará por una manera o la otra.

El sistema se puede clasificar según su criticidad para la operadora eléctrica, el gobierno, etc., y definir el nivel de seguridad requerido o deseado para este sistema. Para este proceso la operadora eléctrica se puede apoyar en la definición de los niveles de seguridad hecha por IEC-62443 o por otras organizaciones como la americana NIST.

A continuación se pasa a listar y clasificar todas las amenazas existentes para el sistema, la probabilidad de que cada amenaza

ocurra en las diferentes zonas, o activos del sistema en estudio y el impacto de las mismas. Impacto no sólo económico sino también en el entorno y en las personas. Imaginemos por ejemplo el impacto de un apagón generalizado en un hospital o en una planta de tratamiento de aguas.

Con esto se pueden identificar los riesgos, ordenar por criticidad y analizar aquellos que se está dispuesto a asumir.

Una vez realizado el análisis de riesgos y definido el nivel de seguridad que se quiere alcanzar, el estándar IEC-62443 en su parte 3-3 define los requisitos funcionales que un sistema de control industrial o eléctrico debe implementar para alcanzar nivel de seguridad 1, 2 o 3.

Se identificarán los requisitos funcionales que son posibles implementar por criticidad o por facilidad de implementación en el sistema existente y mejora de la postura de seguridad general del sistema.

Una buena medida para minimizar el tiempo de interrupción del servicio y asegurar la buena aplicación de medidas a implementar es crear una plataforma espejo.

En esta fase, una vez se ha hecho una copia del sistema para asegurarnos que podemos volver a un estado anterior en caso de que sea necesario, se proceden a implementar las medidas diseñadas.

Antes de poner en ejecución el sistema, se deben probar:

- Las nuevas funcionalidades.
- La desaparición de vulnerabilidades/riesgos identificados en las fases iniciales.
- La correcta operación del sistema.

Por último, se procedería a realizar una copia del sistema ya actualizado, se creará una nueva línea base con el inventariado actualizado y se procederá a comenzar una nueva iteración para atacar nuevos riesgos que hayan podido aparecer o los ya identificados.

El Blockchain

La tecnología Blockchain consiste en una plataforma virtual abierta y distribuida donde se realizan las transacciones económicas

de distinta índole entre los usuarios. Con esta tecnología se prescinde de los intermediarios representados por las entidades bancarias y se evoluciona hacia un sistema descentralizado donde los usuarios realizan los movimientos directamente. Las transacciones dejan de ser procesos opacos y pasan a ser información disponible por todos los usuarios, sin perder la confidencialidad. Por lo que Blockchain puede definirse como un gran libro de cuentas que contiene el historial de todas las operaciones realizadas desde su creación, organizadas en bloques y encriptadas por códigos de seguridad para que no se modifiquen de manera maliciosa (figura 8).

La utilidad de Blockchain no se reduce únicamente a las transacciones económicas, también se pueden llevar a cabo transacciones de otro tipo, como las energéticas. Otro concepto relacionado con esta tecnología son los contratos inteligentes, que son documentos disponibles en la plataforma que contienen las condiciones de un determinado contrato. La ventaja de estos contratos es que cuando se cumplan los requisitos especificados en el documento, Blockchain ejecuta automáticamente los términos del contrato entre los participantes, por ejemplo el intercambio de energía, aligerando el proceso y eliminando la existencia de impagos.

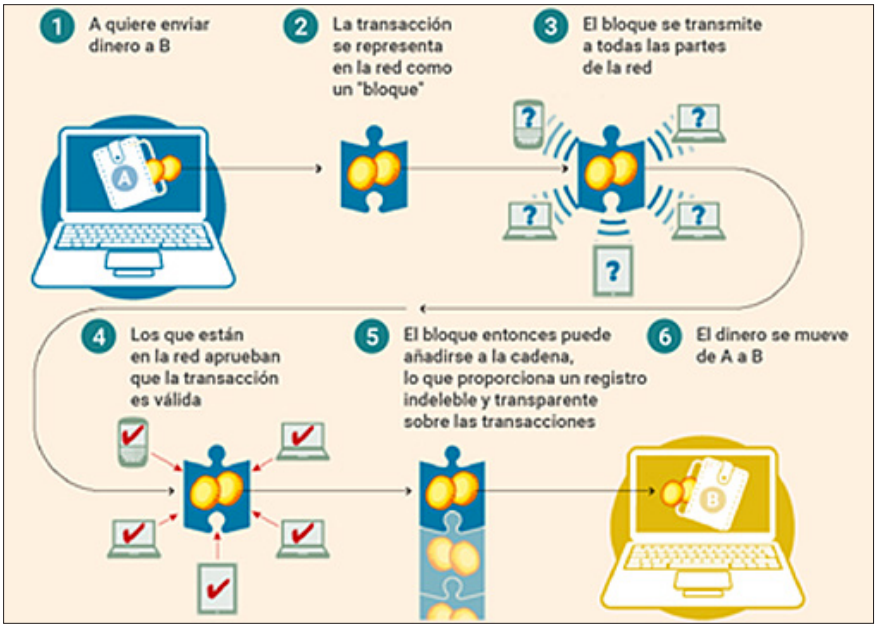


Figura 8. Ejemplo de funcionamiento de Blockchain. Fuente: Financial Times.

Actualmente, Blockchain todavía presenta algunas limitaciones. En primer lugar, la legislación de los países debe ajustarse al desarrollo de la tecnología y uniformizarse para todo el mundo. La descentralización del sistema conlleva que muchos usuarios estén intercambiando información y ejecutando algoritmos complejos al mismo tiempo, con lo cual se limita el número de transacciones y la velocidad de ejecución. En cuanto a la parcela de seguridad, los nombres privados de los usuarios pueden ser vulnerables ante los ciberataques. Además, la plataforma Blockchain no es del todo anónima, si bien es cierto que el nombre público no revela tu identidad, las transacciones son públicas y llegan a desvelar información confidencial. En resumen, las características principales de la tecnología Blockchain expuestas anteriormente, se pueden agrupar en los siguientes puntos:

- Red distribuida: cada usuario conforma un nodo y todos tienen los mismos privilegios.
- Transmisión directa entre usuarios: no existen intermediarios, las transacciones se hacen directamente entre los usuarios.
- Transparencia y pseudoanonimato: las transacciones se publican en el libro de cuentas con los nombres públicos de los usuarios.
- Registros inalterables: una vez se añade un bloque a la cadena, es prácticamente imposible modificar la información de las transacciones que contiene.
- Contratos inteligentes: contratos digitales que se ejecutan directamente cuando se cumplen las condiciones especificadas.

Aplicación de Blockchain en el sector energético

La irrupción de la tecnología Blockchain es una potente herramienta para facilitar la transición hacia las redes inteligentes. Una red inteligente se caracteriza por estar descentralizada, donde los usuarios pueden consumir y producir energía al mismo tiempo (prosumidores). Esto hace que el sistema tenga muchas dificultades para gestionarse desde un organismo central, como se hace actualmente. Además, en una red inteligente el flujo de información pasa a ser bidireccional a través de los contadores inteligentes y el vehículo eléctrico puede adoptar un papel clave en el aplanamiento de la curva de demanda (*Vehicle to Grid*).

Así pues, las oportunidades que ofrece la tecnología Blockchain se adaptan perfectamente a las necesidades del sistema energético del futuro, —descentralizado, flexible, transparente y abierto—. En un mercado energético funcionando bajo la tecnología Blockchain, la energía tendría un valor en *tokens*, los consumidores podrían intercambiar *tokens* por energía mediante transacciones.

Conclusiones

El sistema eléctrico europeo es un sistema robusto y muy interconectado, ambas características facilitan los pasos para avanzar en la transformación energética hacia un sistema más respetuoso con el medio ambiente al utilizar masivamente energías renovables. Sin embargo, las características de este tipo de energías, su aleatoriedad y difícil predictibilidad, hacen compleja la integración de las mismas en condiciones de seguridad. Por ello los operadores de los sistemas eléctricos se han ido dotando de determinadas herramientas para garantizar la continuidad del suministro incluso con una presencia elevada de estas energías.

Por otra parte las redes eléctricas que discurren por el territorio, son en su gran mayoría infraestructuras de superficie sometidas a las agresiones de los fenómenos atmosféricos o accidentes naturales para lo cual deben estar dotadas de protecciones eléctricas coordinadas entre sí para despejar las posibles faltas o cortocircuitos que se produzcan.

Esta transformación del sector eléctrico consistente en una descarbonización, se hará realidad a través de las energía renovables que están distribuidas para lo que se necesitarán los avances que se están produciendo en digitalización aplicada al volumen inmenso de los datos que se produzcan al adquirir los consumidores un papel más activo en el suministro.

Pero a la vez que nos interconectamos a través de las redes inteligentes, incrementamos el riesgo de las actuaciones maliciosas de agentes que pretenden para atacar las infraestructuras eléctricas buscando afectar a la continuidad del suministro.

Los sistemas de control han dejado de ser sistemas aislados, poco conocidos por atacantes. Han pasado a ser infraestructuras críticas para el buen funcionamiento de cualquier sociedad, gobierno o industria.

Implementar medidas de seguridad siempre será más eficiente en términos de tiempo y coste si se tiene en cuenta desde una

fase de diseño del sistema o producto. Los fabricantes están haciendo un esfuerzo para mejorar la seguridad de sus sensores y de los sistemas que integran, pero los operadores deben exigir la implementación de elementos de seguridad en los sistemas que operan basándose en marcos y estándares específicos para sistemas de control industrial y eléctrico.

Los sistemas existentes carecen de medidas de seguridad suficientes, si estos sistemas necesitan ser integrados con otros elementos de las nuevas redes eléctricas, deben pasar por un proceso de actualización y alcanzar un nivel de seguridad suficiente para evitar ser controlados por un atacante y/o ser usados para realizar un ataque a toda la infraestructura de red.

Por último, no podemos dejar de tener en cuenta que la mayoría de estos ataques tienen en común utilizar el eslabón más débil de la seguridad, las personas, y sistemas TI al alcance de todos, como son el correo electrónico o un dispositivo USB (o *Pendrive*) manipulado. El atacante logra ganarse la confianza de la víctima que hace que ejecute el *malware* o código dañino dentro de su ordenador.

Una línea de actuación que siguen muchas empresas para incrementar la seguridad es la formación, concienciación y sensibilización de todo el colectivo asociado con los procesos empresariales, ya que las personas pueden marcar la diferencia entre el rechazo de un ataque o su éxito. Dentro del colectivo afectado está tomando fuerza incluir a todos los actores de la cadena de suministro, desde colaboradores, proveedores, fabricantes de dispositivos, etc.

Con todo esto y con la rápida evolución de la tecnología y el ritmo de aparición de nuevas amenazas, sería un error pensar que los sistemas son inexpugnables y que existen medidas de seguridad que te mantienen protegido completamente contra cualquier ataque. Lo cierto es que los atacantes cada vez son más en número y tienen más recursos, muchos de ellos incluso estarán financiados por gobiernos, y por esta razón las compañías ya no solo invierten en protección, sino también en formación y sensibilización hacia sus colectivos y también en tener actualizados sus mecanismos de resiliencia para poder reaccionar ante un ataque exitoso.

En conclusión, ante una situación de incremento en los ataques que tienen como objetivo sistemas críticos, es vital la inversión económica y humana de forma continuada en seguridad; la im-

plantación de medidas técnicas, un adecuado gobierno y procesos de seguridad, la concienciación de las personas y los mecanismos de contingencia serán claves para mantener la estabilidad de los sistemas eléctricos.

Referencias bibliográficas

ARTEAGA, Félix. «Ciberseguridad y seguridad integral en el sector energético». Real Instituto Elcano. 9/7/2019.

AYERBE, Ana I. «Ciberseguridad: construyendo cadenas de suministro seguras y de confianza». Real Instituto Elcano. 10/9/2019.

BARRERO, Óscar. Cinco pasos para la digitalización de las eléctricas. *Price Waterhouse*. 23 de noviembre de 2018.

CIBERTIME CIBERSEGURIDAD Y TECNOLOGÍA. «Ciberseguridad: las tareas del sector eléctrico». 5/9/2018.

CIER y BANCO INTERAMERICANO DE DESARROLLO (BID). «Taller de ciberseguridad en el sector eléctrico en América Latina y el Caribe». Montevideo: 25/10/2018.

CIGRE CHILE. «Los desafíos de la ciberseguridad en el mercado eléctrico». Kennet Pugh.

COUNCIL OF EUROPEAN ENERGY REGULATORS (CEER). «CEER Cybersecurity Report on Europe electricity and gas sector». 26/10/2018.

ENERGÉTICA XXI. «Ciberseguridad en infraestructuras de telegestión de medidas de consumo en redes de distribución de energía eléctrica». N.º 152. Octubre 2015.

ENERGÍA A DEBATE. «Dialogan sobre ciberseguridad en el sector eléctrico». 15/11/2018.

ENERGIA Y SOCIEDAD. «El rol de la ciberseguridad en la digitalización de la red eléctrica».

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2019. Orden PCI/487/2019, de 26 de abril, por la que se publica dicha estrategia aprobada por el Consejo de Seguridad Nacional.

EUROPEAN PARLIAMENT. «Directorate general for internal policies. Cibersecurity strategy for the energy sector». 2016.

FUNDACIÓN PARA LA SOSTENIBILIDAD ENERGÉTICA Y MEDIOAMBIENTAL (FUNSEAM). «Ciberseguridad en el sector energético».

INFORMES SITUACIÓN DE CIBERSEGURIDAD CERT.

INSTITUTO DE INVESTIGACIÓN TECNOLÓGICA (IIT). «El sector eléctrico español del futuro. Retos y políticas». Diciembre 2018.

INTERNET WIKIPEDIA. «European of Transmission System Operators for Electricity».

JIMÉNEZ, Juan Carlos. «Ciberseguridad en el sector energético: el valor de la prevención». *Gas actual.* Abril 2019.

KASPERSKY. «Ciberseguridad para infraestructuras eléctricas».

MORALES CABELLO, Eduardo. «La ciberseguridad aplicada al monitoreo y control de los sistemas eléctricos de potencia». *Revista Electroindustria*. 11/9/2019.

OBSERVATORIO DE LA CIBERSEGURIDAD DE AMÉRICA LATINA Y EL CARIBE.« ¿Estamos preparados en América Latina y el Caribe?». Informe de ciberseguridad 2016.

OJEA, Laura. «Los ciberataques al sector energético de todo el mundo aumentan alrededor de un 41 % en solo los seis primeros meses de 2019». *El periódico de la energía.* 4/10/2019.

RED ELÉCTRICA DE ESPAÑA. «Criterios de ajuste y coordinación de protecciones». Año 2016.

RED ELÉCTRICA DE ESPAÑA. «Interconexiones eléctricas. Un paso para el mercado único de la energía». Septiembre de 2012.

REVISTA DE ENERGÍA. «La ciberseguridad en los sistemas eléctricos de potencia». Junio 2019.

SCHEINER ELECTRIC. «Ciberseguridad: cómo pueden las empresas eléctricas reducir sus amenazas». Año 2016.

SINC. La ciencia es noticia «La red eléctrica europea seguirá funcionando aunque el mundo se desmorone». 7/3/2019.

SMARTCITY INFO. «China lanza una red nacional de servicios basados en Blockchain para el desarrollo de ciudades inteligentes». 12/11/2019.

SMARTGRIDS INFO. «Análisis y evolución de ciberseguridad en el IoT de infraestructuras críticas eléctricas». Comunicación presentada en el IV Congreso SmartGrids.

VINYES, Enric. «Ciberseguridad para la red eléctrica actual». Schneider Electric. 5/12/2017.