La nueva distribución eléctrica:

Ciberseguridad en su transformación digital

Centro de Ciberseguridad Industrial

Fundación Naturgy

La nueva distribución eléctrica:

Ciberseguridad en su transformación digital

Abril 2023

Centro de Ciberseguridad Industrial

Fundación Naturgy

El Centro de Ciberseguridad Industrial (CCI) es una organización independiente, sin ánimo de lucro, cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial, en un contexto en el que las organizaciones de sectores como el de fabricación o el energético juegan un papel crítico en la construcción de la sociedad actual, como puntales del estado del bienestar.

El CCI afronta ese reto mediante el desarrollo de actividades de investigación y análisis, generación de opinión, elaboración y publicación de estudios y herramientas e intercambio de información y conocimiento sobre la influencia, tanto de las tecnologías, incluidos sus procesos y prácticas, como de los individuos, en lo relativo a los riesgos –y su gestión– derivados de la integración de los procesos e infraestructuras industriales en el Ciberespacio.

El CCI es, hoy, el ecosistema y el punto de encuentro de las entidades –privadas y públicas– y de los profesionales afectados, preocupados u ocupados de la Ciberseguridad Industrial; y es, asimismo, la referencia hispanohablante para el intercambio de experiencias y la dinamización de los sectores involucrados en este ámbito.

Paseo de las Delicias, 30, 2ª Planta
28045 MADRID
Tel.: +34 910 910 751
e-mail: info@cci-es.org
www.cci-es.org

Blog: blog.cci-es.org
Twitter: @info_cci
LinkedIn: www.linkedin.com/in/centroCiberseguridadindustrial

Indice

Resumen ejecutivo

La **transformación digital** está modificando los procesos de producción, distribución y consumo de energía. Hoy en día, por ejemplo, es posible obtener en tiempo real datos procedentes de cualquier instalación para detectar riesgos potenciales y anticiparse a un daño, o proporcionar a los consumidores, también en tiempo real, la información que exigen, así como la posibilidad de actuación sobre ciertos sistemas.

Pero este aumento de la conectividad y del despliegue de tecnologías digitales aumenta también la necesidad de proteger los activos críticos frente a amenazas. En el caso específico de la energía, el impacto de un corte de suministro a raíz de un ciberataque podría tener consecuencias muy importantes en todos los sectores, además de afectar a los usuarios finales. Por ello, uno de los pilares sobre los que se asienta la transformación digital es la ciberseguridad. Este documento aborda los retos asociados a la ciberseguridad en uno de los ámbitos de mayor importancia en lo relativo a suministro de energía como es el de la **distribución eléctrica.**

> Uno de los pilares sobre los que se asienta la transformación digital es la ciberseguridad.

Este sector, además, forma parte de un mercado que está cambiando a gran velocidad y las organizaciones llevan tiempo adaptándose, tanto desarrollando los proyectos de digitalización necesarios, como con la incorporación de la ciberseguridad y la compra de nuevas tecnologías o activos. No obstante, sigue enfrentándose a **retos de transformación importantes:**

- La integración de cada vez más generación renovable, típicamente fotovoltaica y eólica.
- La generación distribuida, con la aparición de la figura del ‘prosumer’, donde cambia el paradigma en el que el flujo de energía siempre iba en el mismo sentido.
- La digitalización de las redes, con contadores inteligentes y sistemas de medida avanzada (smart grids) que permiten la gestión de muchos de los nuevos servicios que demandan los consumidores, activos como las nuevas subestaciones digitales que suponen abrir redes tradicionalmente muy cerradas, o la red de puntos de recarga para vehículos eléctricos, que requieren centros de transformación digitalizados para tratar los datos de los consumidores y gestionar el reparto de cargas.

Asociado a la evolución en los ámbitos descritos anteriormente, aparecen nuevos **desafíos en el campo de la ciberseguridad:**

- Las nuevas cadenas de suministro, ya que es necesario abrirse a un mayor número de fabricantes para incorporar las nuevas tecnologías con las que hacer frente a los aspectos anteriores, y en las que es fundamental analizar riesgos a distintos niveles. Se debe contemplar desde el diseño hasta cada una de las fases de la implementación de los nuevos proyectos, así como en las adaptaciones y renovaciones necesarias.

- La asignación de nuevos roles y responsabilidades: la aparición de nuevos actores y la dependencia del hardware y del software, nos den llevar a una adecuada reflexión sobre la asignación de roles y responsabilidades.

- Nuevos sistemas de interdependencias: redes, sistemas de pago, de datos, comunicaciones, etc.

- Niveles de seguridad de dispositivos y aplicaciones.

- Nuevos enfoques para la gestión de vulnerabilidades: obsolescencia de equipos, actualización continua de software, criticidad de equipos, etc.

- El papel de la nube y el diseño de los Centros de Procesamiento de Datos.

> La distribución eléctrica afronta retos importantes en su proceso de digitalización: generación distribuida, nuevos servicios e información a los consumidores, vehículo elétrico...

La creciente actividad de los ciberdelincuentes, unida a su cada vez más evidente profesionalización, hace que sea estrictamente necesario acometer importantes inversiones, a la vez que se intensifican las estrategias de concienciación y de formación del personal, los procedimientos de respuesta a incidentes y, sobre todo, la importancia de involucrar a todos los empleados de la organización en materia de ciberseguridad. Por tanto, las entidades eléctricas deben trabajar tanto en los procedimientos como en las personas, además del ámbito estrictamente tecnológico.

Las organizaciones del sector eléctrico están ya implantando una serie de mecanismos de protección con el objetivo de estar lo menos expuestas posible a la actividad de los ciberdelincuentes. Algunos de ellos son contar con una segmentación y una defensa en profundidad, realizar un seguimiento de cualquier cambio en las configuraciones de los dispositivos, controlar los accesos y privilegios, evaluar y gestionar las vulnerabilidades,

monitorizar todos los aspectos relacionados con la seguridad y garantizar la continuidad del servicio y la seguridad de las personas, el medio ambiente y los equipos.

Dada la relevancia de la ciberseguridad, la propia Unión Europea ha tomado el liderazgo aprobando multitud de **regulación en materia de ciberseguridad,** seguridad y resiliencia, algunas de mucho calado para el sector, entre las que se puede resaltar:

- Directiva NIS2 (Directiva (UE) 2022/2555 del Parlamento Europeo, que exige medidas de seguridad para las entidades críticas, incluye la cadena de suministro y hace responsable a la alta dirección de las organizaciones de su mantenimiento.

- Directiva (UE) 2022/2557 del Parlamento Europeo, sobre un enfoque coordinado en toda la Unión para reforzar la resiliencia de infraestructuras críticas.

- Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales.

> La UE ha tomado el liderazgo desarrollando multitud de regulación en materia de ciberseguridad

Todo ello conlleva unas necesarias **inversiones en ciberseguridad** para reforzar la resiliencia de los operadores y del sistema, incluyendo a los consumidores finales y su nueva manera de relacionarse con el mismo, así como mantener un enfoque coherente y una mayor capacidad de servicios en toda la Unión. Sin duda estas partidas están totalmente justificadas puesto que reforzarán la identificación, protección, detección, respuesta y recuperación de las organizaciones ante una eventual amenaza, conforme a lo indicado en la Directiva NIS2. Es más, el coste relacionado con la gestión y restablecimiento tras un ciberataque será mayor a cualquier carga adicional derivada del cumplimiento normativo. Y, por lo tanto, deben ser adecuadamente reconocidas tanto en lo que respecta a la inversión, como a los costes operativos resultado de una evolución tecnológica continua.

> Es necesario acometer inversiones relevantes en ciberseguridad para reforzar la resiliencia del sistema en su conjunto, las cuales deben ser reconocidas

1. Introducción

El concepto de transformación digital está asociado al cambio, a la evolución que experimentan las compañías para mejorar su operativa y a ofrecer mayor valor a sus clientes aprovechando las ventajas de las tecnologías digitales. Por ello, incumbe a todas las áreas de una empresa y aporta beneficios a las firmas de todos los sectores y a los consumidores finales.

Además, la digitalización está transformando los procesos de producción, distribución y consumo de energía. Hoy es posible obtener en tiempo real datos procedentes de una turbina en una planta de generación, de la compuerta de una presa o del transformador de una subestación y enviarlos a una sala de control donde detectar un riesgo potencial y anticiparse al daño antes de que este se produzca gracias al mantenimiento predictivo.

Asimismo, la Inteligencia Artificial aplicada permite identificar en tiempo real no solamente eventuales anomalías, sino también actividades que pueden mejorar la productividad a medio y corto plazo.

En lo que se refiere a las intervenciones sobre el terreno, el Internet de las Cosas, en su variante IIoT *(Industrial Internet of Things* por sus siglas en inglés; Internet Industrial de las Cosas), pone a disposición herramientas como drones o robots que pueden efectuar inspecciones de infraestructuras eléctricas, aumentando así la precisión y eficacia, además de eliminar el riesgo para las personas y el impacto medioambiental.

Adicionalmente, existe cada vez una mayor exigencia por parte de los consumidores finales a disponer de información en tiempo real como a poder interactuar con los sistemas.

Según un informe de Boston Consulting Group (BCG)[1], las tecnologías digitales que se están utilizando en la industria, incluyendo la energía, están transformando profundamente la producción. Es una nueva manera de articular las relaciones entre proveedores, productores y clientes, así como entre las personas y las máquinas.

En dicho documento se definen los nueve pilares de la digitalización industrial: *Big Data y analytics* (incluyendo Inteligencia Artificial y *Machine Learning*); robots autónomos y colaborativos; gemelos digitales y simulación; convergencia IT/OT; IIoT; computación en la nube; fabricación aditiva (impresión 3D); realidad aumentada; y ciberseguridad.

Cabe destacar que entre estos pilares de la digitalización se incluye la ciberseguridad como uno de los elementos clave que debe tenerse en cuenta. No en vano, con el aumento de la conectividad y el uso de protocolos estándar de comunicación asociados al despliegue de las tecnologías citadas aumenta la necesidad de proteger los activos críticos frente a las amenazas.

Además, la ciberseguridad también juega un papel importante en la competitividad. Si medimos la efectividad sobre los sistemas de producción que pueden considerarse críticos, un ciberincidente sobre tales sistemas

> Las tecnologías digitales que se están utilizando en la industria, incluyendo la energía, están transformando profundamente la producción.

causaría una reducción directa de su efectividad a causa de -como mínimo- pérdidas económicas y productividad (es decir, se incrementan los costes de producción y se reducen las unidades de producción o su calidad).

A todo esto se le añade cómo afectaría al consumidor final un corte de la energía eléctrica a raíz de un ciberataque, en el caso que nos incumbe. ¿Qué consecuencias tendría para la población no disfrutar de calefacción en invierno? ¿O de agua caliente? ¿Cómo influiría en la seguridad que una ciudad no tuviera alumbrado público? ¿Y a un hospital? Un ciberataque, por tanto, no incidiría solamente en la empresa industrial en sí, también en los millones de usuarios y consumidores finales.

En este documento del CCI, cinco profesionales de ciberseguridad del ámbito eléctrico presentan la situación del riesgo en ciberseguridad y sus consecuencias para los sectores críticos de un país, enfocándose en la distribución eléctrica. Los atacantes y el tipo de ciberincidentes es amplio y sofisticado, pero las amenazas potenciales se concentran, en concreto, en cinco tipos que se describen y clasifican en el segundo apartado.

El estudio también muestra cuáles son los retos a futuro de la distribución eléctrica y cómo dichos escenarios deben considerar la ciberseguridad. Para ello se propone un nuevo modelo basado en estándares reconocidos y normas existentes.

El lector encontrará en este documento también las regulaciones y mejores prácticas de ciberseguridad, finalizando con la evolución en la inversión y el gasto del sector eléctrico en esta materia.

2. Situación actual

La actividad de los ciberdelincuentes ha evolucionado con el paso de los años expandiéndose y sofisticándose. Además, a raíz de la evolución vertiginosa que está experimentando la digitalización de toda la sociedad, la superficie de ataque se ha multiplicado. Un contexto que afecta, como no podría ser de otra manera, a la industria.

Este capítulo expone, la situación del sector de la distribución eléctrica en este contexto, así como los incidentes de ciberseguridad de alto impacto, los tipos de incidentes de ciberseguridad más importantes y el papel que está jugando Europa frente a esta situación.

2.1. Sectores críticos

Hablar de incidentes de ciberseguridad ya no es un tema aislado. Es más, aparecen en las primeras planas de los medios de cualquier país, se publican casi de inmediato en redes sociales de miles o millones de usuarios, se comentan y son debatidos en cientos de eventos relacionados con tecnología o incluso muy ajenos a ella.

Históricamente, los sectores más afectados por los ataques fueron la banca y las empresas de telecomunicaciones. La banca porque allí estaba el dinero físico y digital, mucho antes de que llegaran las billeteras digitales a los usuarios; y las empresas de telecomunicaciones porque eran las plataformas de acceso a Internet.

Hoy en día, la situación ha cambiado mucho. Ya no hay sectores que se encuentren "a salvo". Vemos, por ejemplo, que los ciberincidentes que afectan al sector agroalimentario han aumentado un 600% en el último año, y que el FBI ha sacado las primeras notas de advertencia al sector. También hemos sido testigos durante el momento más duro de la pandemia de casos de incidentes relacionados con el sector de la sanidad, donde a pesar de ser un momento tan particular para todos, hubo hospitales que no podían utilizar sus sistemas y vieron afectada la atención de pacientes.

El sector automotriz, las petroleras, las empresas químicas, el sector del *retail,* las manufactureras... Absolutamente todas las empresas, ya sean *startups,* pymes o grandes compañías, están siendo afectadas por diferentes tipos de ataques.

2.2. El sector de la distribución eléctrica

Indudablemente, las compañías del sector eléctrico no son la excepción. Desde hace varios años vienen sufriendo incidentes, más aún en tiempos de guerras como la de Rusia y Ucrania, donde pasan a ser objetivos no solo de ataques físicos y militares, sino también de ciberejércitos tratando de controlarlas.

Además, el sector eléctrico tiene una particularidad extra y bien diferente a la gran mayoría de las otras industrias: si se ve afectado, el resto también lo serán, por lo que se convierten en un claro objetivo.

En el sector eléctrico merece la pena añadir el caso especial de los ataques respaldados por Estados. Es algo que se ha evidenciado desde 2021, especialmente durante el pasado año, tanto por la guerra de Ucrania como por los reiterados avisos de la Agencia de Ciberseguridad norteamericana (CISA) para reforzar las defensas del sector eléctrico. No se puede hablar de ciberejércitos, pero sí de grupos que protegen Estados a nivel técnico y que son dotados de medios para especializar más sus ataques; también a nivel técnico y económico.

Desde 2021 se han experimentado diversos ataques dirigidos sobre los que se ha escrito mucho dadas sus consecuencias, que han servido para detectar una actividad continuada en entornos de nube hasta llegar a constituir casos graves. Entre estos casos cabe resaltar el compromiso de los repositorios de actualizaciones de *software* ubicados en los servidores de proveedores que proporcionan soluciones y servicios de ciberseguridad a entornos militares y energéticos. Este tipo de incidentes fue el inicio del concepto 'ataque a través de la cadena de suministro'.

Respecto a los incidentes, la CISA ha alertado sobre diversos ataques de phishing para lograr credenciales e información de usuarios específicos, aunque también se ha detectado actividad sospechosa en redes de sistemas de energía.

Por otro lado, en Ucrania se están viendo ataques híbridos (físicos y lógicos), con secuencias de artillería y ciberataques simultaneados.

2.3. Atacantes

A partir de lo mencionado, conocer los diferentes atacantes (o mejor conocidos como 'actores' en la terminología específica) que pueden afectar a las organizaciones industriales del sector eléctrico es de suma importancia para entender qué están haciendo las organizaciones para protegerse. Por ello, también es importante conocer su motivación:

- **Grupos *hacktivistas*** que principalmente intentan generar daño reputacional o incluso la disrupción de la operación sin mayores daños a la infraestructura a partir de una causa que los motiva. Por ejemplo, el cuidado medioambiental, razones políticas o religiosas, movimientos sociales reclamando por algún trabajador o por un cliente (o tipo de cliente) afectado, etcétera.

- **Grupos terroristas** cuyo objetivo es sembrar el terror u ocasionar daño. Estos buscan directamente la disrupción de la operación, pero intentando provocar el mayor daño posible a la infraestructura; incluso tratando evitar que vuelva a reactivarse.

- **Grupos criminales** que buscan obtener algún beneficio económico a partir del ataque propiciado.

- ***Insiders*** que suelen ser empleados directos o subcontratados descontentos y que como reclamo intentan generar daños económicos a la organización.

- **Ocasionales** que suelen no tener a la organización como objetivo en el sentido propio de la palabra, sino que están probando técnicas de ataque o hasta incluso *malware* desarrollado y que se encontraron con la organización casi por accidente. No tienen como finalidad ocasionar un daño porque sí, pero principalmente intentan obtener un beneficio tras haberlo ocasionado.

Lo más habitual, en el caso de los tres primeros, donde suelen ser grupos organizados, es perpetrar un ataque a través de un APT *(Advance Persistent Threat)* de tal modo que la organización industrial atacada no es consciente de ello hasta que ya es demasiado tarde. El tiempo promedio en que una entidad suele darse cuenta de que ha sido vulnerada a través de un APT está entre los 6 y los 12 meses de haber comenzado el ataque.

2.4. Incidentes de ciberseguridad de alto impacto

El mapa relacionado con los tipos de ataques potenciales es realmente amplio e incluye, por ejemplo, casos que afectan a la cadena de suministro. Pero si nos centramos en casos más específicos que están afectando

actualmente a las empresas del sector eléctrico, tendríamos que pensar en los siguientes cinco tipos:

Ransomware. Es un *malware* dedicado a cifrar el contenido de los equipos afectados y a solicitar un rescate para recuperarlo. Si clasificáramos la larga lista de empresas afectadas por incidentes de ciberseguridad, esta sería la principal causa.

El *ransomware* descubierto en los últimos años ha incorporado capacidades considerables. Por ejemplo, exfiltrar información durante un período de tiempo previo a cifrar el contenido de tal manera que si la víctima se niega a pagar para recuperar sus archivos, la extorsión puede variar y exigir un pago a cambio de no hacer pública dicha información.

Phishing. Es, sin dudas, el método más popular en eventos y campañas de concienciación que emplean las empresas intentando que los usuarios estemos más atentos y protegidos; pero, a su vez, el peor enemigo de las áreas de ciberseguridad, ya que el ingenio de los atacantes para enmascarar sus técnicas, suplantando identidades e intentando engañar a las víctimas para que faciliten información o accesos, es impresionante.

Fileless malware. Es un *malware* asociado principalmente a los ataques relacionados con el extendido spam y con la suplantación de identidad que ha puesto de moda, una vez más, la infección de equipos sin la necesidad de contar con un archivo ejecutando una actividad maliciosa en el sistema. Este tipo de *malware* hace uso de herramientas y procesos propios del sistema operativo (por ejemplo Powershell o WMI) sin descargar ejecutables extras en la víctima, dificultando así su detección para las herramientas *antimalware*.

Por lo general, requiere la "complicidad" del usuario del sistema para afectar al equipo, que claramente no lo haría conscientemente. Esta técnica ha sido muy utilizada en los últimos años para afectar estaciones de ingeniería y lograr así comprometer los equipos con los cuales se configuran los controladores del proceso industrial.

Malas configuraciones o configuraciones default. Es importante poner foco especial en las configuraciones, especialmente relacionadas con la explotación de servicios remotos.

La explotación de servicios remotos mal configurados es algo que, al menos desde 2012 con buscadores como ShodanHQ y otras herramientas similares, se intenta prevenir a partir de mostrar lo sencillo que es encontrar los equipos mal configurados en Internet. Sin embargo, y a pesar de tanta información en eventos, redes sociales y medios digitales, continúa siendo un gran problema en el sector eléctrico.

> El sector eléctrico forma parte de un mercado que está cambiando a gran velocidad. Y esta velocidad supone que es necesario reorganizarse internamente y adaptar la cultura.

Explotación de vulnerabilidades. Como cualquier tipo de código escrito, el de los dispositivos de control industrial (como del *software* que utilizan los HMI (Human Machine Interface), los servidores SCADA, las estaciones de ingeniería y el resto de los componentes que requieren un sistema operativo) tiene fallos de seguridad comúnmente conocidos como bugs en un ambiente profesional. Estos fallos de seguridad antes eran poco conocidos por el público en general y representaban una ventaja para los ciberdelincuentes dado que muy pocos tenían información sobre cómo protegerse o qué impacto podrían tener en sus sistemas. Pero ahora se reportan públicamente en diferentes medios con la finalidad de dar a conocer a todos los actores del sector cuándo algo representa una amenaza, el alcance que tiene y las medidas que pueden tomar para mitigar los riesgos.

Hay organizaciones y portales especializados donde se publican estos incidentes, como por ejemplo los CVE de Mitre, los *advisors* de CISA o incluso los propios fabricantes de sistemas industriales (como es el caso de Siemens).

También existen hoy en día muchos sistemas industriales expuestos a Internet, con protocolos de comunicaciones no siempre robustos desde la perspectiva de ciberseguridad, que están expuestos al alcance de expertos y no tan expertos permitiendo que los ataques a partir de estos fallos de seguridad sobre los productos propios del mundo de las tecnologías de operación industrial sean más sencillos, pero a la vez más complejos. Todo ello, más fácil de alcanzar para los atacantes y más complejo de resolver para las organizaciones industriales que son víctimas y que no tienen el conocimiento o las herramientas suficientes para mitigar determinados ataques.

De los cinco tipos de ataques potenciales descritos, los tres primeros afectan a usuarios de manera directa (independientemente del cargo o posición que ocupen). Y los otros dos están relacionados con las áreas de tecnología en sí misma, donde malas prácticas de gestión de la ciberseguridad tanto en el diseño y en el despliegue/ejecución como en el mantenimiento y la operación pueden producir que una amenaza se materialice en la instalación.

La dificultad de combatir estos tipos descritos no es solamente por su sofisticación, sino también en ocasiones por la falta de madurez en cuanto a la cultura y gestión de la ciberseguridad en todo el proceso del ciclo de vida de los proyectos de automatización y digitalización industrial.

El sector eléctrico forma parte de un mercado que está cambiando a gran velocidad. Y esta velocidad supone que es necesario reorganizarse internamente y adaptar la cultura con agilidad, de forma que permita entender que ya no es un operador de servicios, sino un gestor de servicios que debe atender a clientes con una mayor tendencia hacia la digitalización y con exigencias en cuanto a lo que sus consumidores desean: tener información prácticamente en tiempo real y no en la factura final del servicio.

Aunque puede parecer evidente, la regulación en general no suele reconocer los nuevos costes que esto genera en las organizaciones eléctricas, tanto a partir de la necesidad de abordar proyectos de digitalización como de incorporar la ciberseguridad, o incluso en la compra de nuevas tecnologías o activos que también aumentarán los costes de mantenimiento, y no sólo los de inversión inicial.

2.5. Tipos de incidentes de ciberseguridad y lecciones aprendidas

Como ya se ha mencionado, no importa el tipo de empresa ni el sector; todos están en riesgo de ser atacados siempre, y la principal herramienta que existe para defenderse es el propio conocimiento. Cuando un incidente se hace público, visibiliza la problemática y lo pone sobre la mesa de discusión del resto de las empresas. Compartir que determinada tecnología implementada no fue configurada de forma segura o que para determinado proyecto o proceso se debería involucrar de manera más intensa al área de ciberseguridad, tiene beneficios comunes para el sector.

El trabajo de las áreas de ciberseguridad es complejo porque está basado en proporcionar protección a los sistemas internos, a los sistemas comprados de terceros y a los sistemas ejecutados en terceros (como los servicios *cloud*), así como a lo que sucede con las personas, el cambio cultural, las comunicaciones, los papeles, etc.

Si bien es posible citar muchos casos públicos tanto de grandes empresas como de pequeñas, los siguientes ejemplos corresponden a tipos de incidentes sufridos en los últimos cinco años por compañías del sector eléctrico:

- **Acceso no autorizado a los sistemas.** El atacante (o los atacantes) tuvo acceso a información sensible de un grupo acotado de clientes de la empresa que incluye: nombre, DNI, teléfono, correo electrónico, dirección postal o contractual, productos contratados y fechas de vigencia, fecha de factura, tarifa, importe y estado de los pagos e incluso el IBAN.

- **Alteración de los sistemas.** El ciberincidente no solo implicó la disrupción del 90% de los sistemas corporativos (el correo y el servicio de atención telefónica permaneció afectado por semanas), sino que, además, según se publicó, se perdieron 25 años de datos históricos de sus sistemas. Aunque sus servicios relacionados con power grid y la red de fibra no fueran afectados, el gran impacto que tuvieron sus sistemas corporativos a partir de la corrupción de sus documentos afectó a la organización con relación a facturación, atención al cliente, información de consumos históricos, cargas impositivas, etc.

- ***Ransomware.*** Ragnar Locker es un *ransomware* que ha generado graves consecuencias. En las publicaciones existentes se puede comprobar que los sistemas de las empresas afectadas fueron comprometidos y cifrados, y que se exfiltró cerca de 10 terabytes de información de una determinada empresa. También se publicó que la recompensa solicitada por los ciberdelincuentes para descifrar la información de los equipos y no hacer pública la exfiltrada rondaba los 10 millones de euros.

Más allá de los diferentes casos mencionados y de todos los que se pueden citar o encontrar en diferentes informes publicados sobre la situación del sector, se hace muy evidente el crecimiento que han experimentado los ciberincidentes y las amenazas en el sector eléctrico. También es indiscutible la necesidad de aumentar las inversiones, las estrategias de concienciación y de formación del personal, los procedimientos de respuesta a incidentes y, sobre todo, la importancia de involucrar a todos los empleados de la organización. Los ejemplos muestran la importancia de trabajar en los procedimientos, pero también en las personas.

En junio de 2021, la Secretaria de Energía de los Estados Unidos, Jennifer Granholm, advertía en este sentido: “Hay miles de ataques en todos los aspectos del sector energético y del sector privado en general. Está sucediendo todo el tiempo. Por eso, el sector privado y el sector público tienen que trabajar juntos”.

En 2017, Eset anunció el descubrimiento de un *malware* destinado a sistemas de control industrial realmente muy dañino, al que apodó Industroyer, y que según esta empresa estuvo detrás del apagón de casi una hora y media de la capital ucraniana, Kiev. Dicho *malware* tenía como objetivo tomar el control de las subestaciones eléctricas y cortar la distribución de la energía, pero también dañar los equipos.

A diferencia del resto de los casos mencionados, este *ransomware* fue diseñado para afectar a este tipo de industrias. El año pasado, muchos investigadores hacían referencia a él, aunque principalmente para alertar sobre la existencia de una segunda versión que está siendo empleada en tiempos de guerra.

> La regulación en general no suele reconocer los nuevos costes que esto genera en las organizaciones eléctricas.

2.6. Europa frente a esta situación de riesgo

La Unión Europea, ante el aumento de los riesgos y vectores de ataque que se han ido produciendo en los últimos años en las infraestructuras críticas de la propia Unión, ha ido aprobando multitud de regulación en materia de Ciberseguridad, Seguridad y Resiliencia que marca un cambio de enfoque para todos los sectores, especialmente las infraestructuras críticas, tanto a nivel europeo como de los Estados miembro. Cada país va a tener que adaptar sus regulaciones al nuevo marco regulatorio europeo. No obstante, este nuevo marco europeo de Ciberseguridad y Resiliencia se empezó a configurar en 2019.

Para una mejor comprensión del lector, lo podemos clasificar diferenciando la ciberseguridad de servicios, la resiliencia en infraestructuras críticas, la ciberseguridad y seguridad de producto y, por último, la protección de datos. Esto lo veremos de manera esquemática en el apartado 5.3. de este documento.

Concretamente, en lo que respecta a las infraestructuras críticas, habría que resaltar por su trascendencia:

- La **Directiva NIS 2** (Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148).

- La **Directiva (UE) 2022/2557** del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo y la Recomendación 2023/C20/01 del Consejo, de 8 de diciembre de 2022, sobre un enfoque coordinado en toda la Unión para reforzar la resiliencia de infraestructuras críticas.

- La **propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad** para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020 (Ley de Ciberresiliencia), que se aplica a los productos con elementos digitales que se introducen en el mercado.

3. Retos actuales

El sector eléctrico se enfrenta a múltiples retos, aunque son tres los ámbitos principalmente destacados: la generación renovable, la generación distribuida y la virtual *power plant* y, finalmente, la digitalización de las redes.

3.1. La generación renovable (no síncrona)

- La aportación de la producción renovable a los sistemas eléctricos aumenta cada día en muchos países desarrollados, y así seguirá siendo de acuerdo a los objetivos de reducción de emisiones marcados. Este hecho está significando un cambio en el modo clásico de gestionar la aportación de los distintos vectores energéticos, pero también para evaluar el riesgo asociado a cada uno, siendo la ciberseguridad una de las claves a tener en cuenta. De esta manera, la energía solar fotovoltaica y la generación eólica son fuentes que han nacido ya conectadas al exterior.

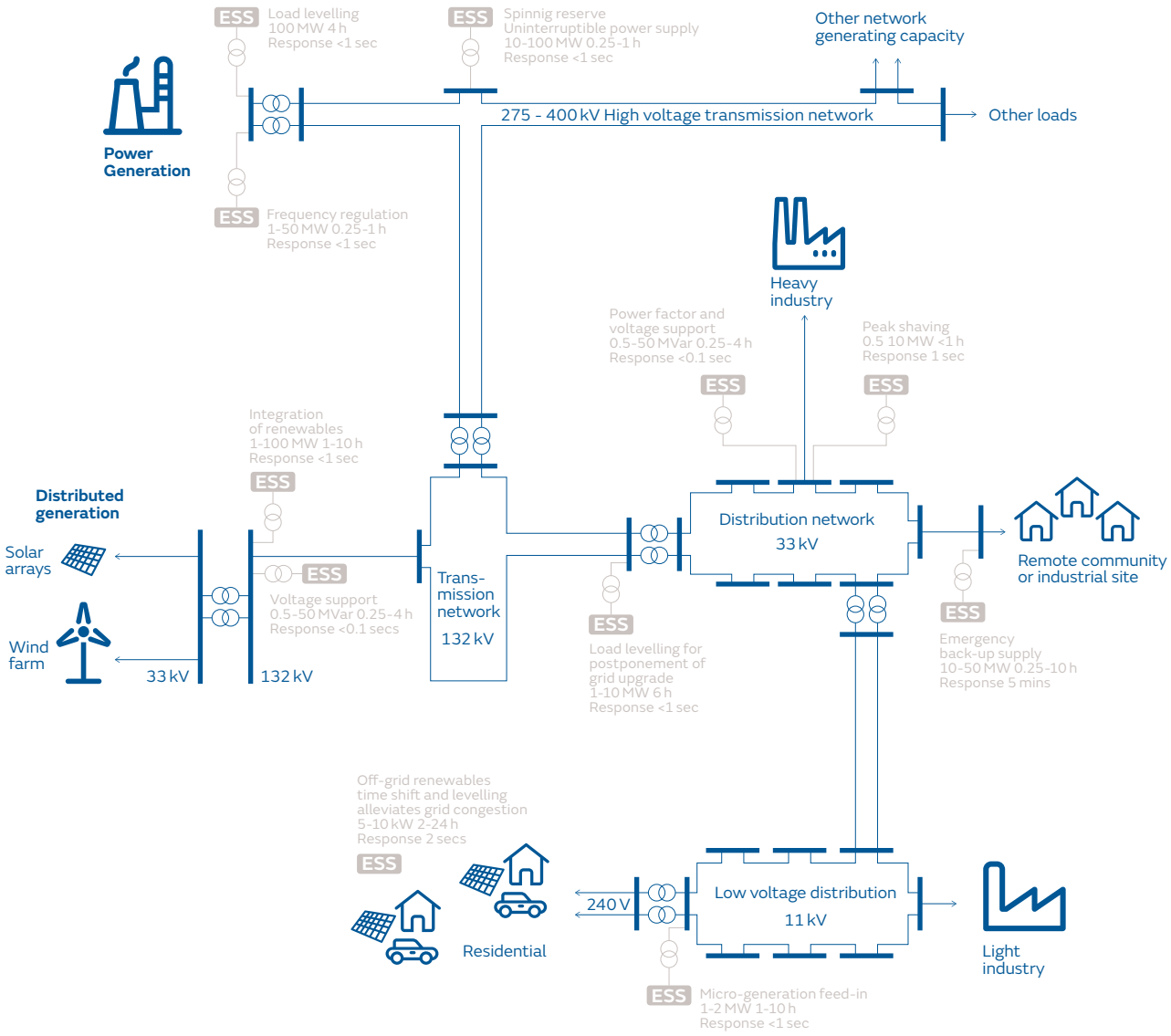
- La generación eólica nació conectada a los proveedores OEM *(Original Equipment Manufacturer)*, principalmente a través de conexiones satélite -hasta 2022 consideradas seguras-, y depende de contratos de servicio, garantías o mantenimiento durante periodos multianuales que requieren envío de datos y acceso remoto a los activos.

- La generación solar ha nacido ya conectada a la nube, considerando además que se trata de un entorno muy distinto donde ya no hay un proveedor tecnológico principal -como ocurre en todas las demás tecnologías-, sino que hay muchas veces hasta cuatro tecnólogos (SCADA, electrónica de potencia, *trackers* y estación meteorológica). Eso sí, el peso principal recae en el integrador o propietario del activo, que en ningún caso gobierna las conexiones exteriores de los tecnólogos citados.

3.2. La generación distribuida y la *'virtual power plant'*

- La aparición de la figura del "prosumer". El paradigma de la cadena de generación, transporte, distribución y comercialización en que el flujo de la energía siempre iba en una dirección y que había permitido un conocimiento de la red, sus dinámicas, predicción de averías y pronósticos de consumos está cambiando de manera radical en la medida que la generación distribuida se hace asequible y comienza a tener un impacto significativo, no tanto a nivel de casación de energía, pero sí a nivel de estabilidad de la red en entorno local. Ver figura 1:

Figura 1 | **Representación esquemática de ESS (Grid Energy Storage Systems and Applications)**



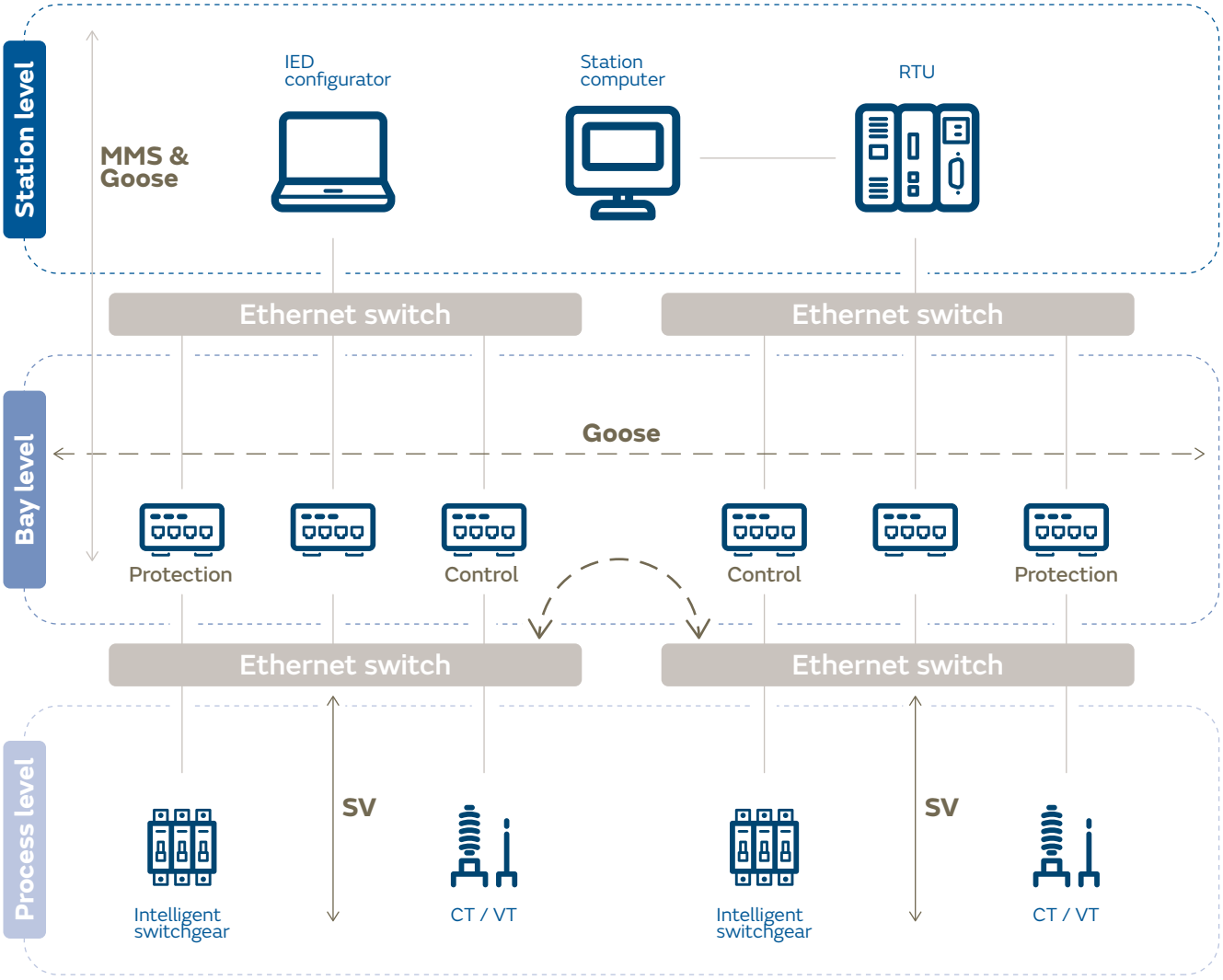
- El concepto de *'virtual power plant'* es pujante, de modo que se plantee como una unidad "negativa a despachar" el conjunto de consumidores domésticos que pudieran ser modificados respecto a su punto de consigna, aun manteniendo una línea base de confort. Por ejemplo, bajar el termostato del aire acondicionado de un millón de consumidores en un grado podría suponer un ahorro de 30 megavatios, con el consiguiente beneficio en estabilidad del sistema, precios marginales y reducción de emisiones. Sin embargo, este planteamiento teórico que se comienza a implantar a nivel técnico vuelve a poner de manifiesto que la necesidad de abordar la seguridad de dispositivos domésticos y la fiabilidad de su medida, junto a su adopción desde entornos en la nube, podría impactar en el sistema eléctrico.

3.3. La digitalización de las redes

Smart grids. Las empresas eléctricas llevan años acometiendo grandes inversiones en los denominados *smart meters* y sistemas de medida avanzada. Estos equipos, que aportan un gran valor para un suministro adecuado y permiten potencialmente la gestión de muchos de los nuevos servicios demandados por los consumidores, conllevan igualmente una necesidad de incrementar la seguridad en la comunicación mediante medidas de encriptación y de seguridad a nivel de capa de aplicación.

- **Redes de distribución.** Nadie duda de los beneficios en cuanto a costes operativos y de mantenimiento de las nuevas subestaciones digitales, de acuerdo al IEC 61850. No obstante, se abren nuevos retos en cuanto a abrir redes tradicionalmente muy cerradas y sobre comunicaciones serie para evolucionar a comunicaciones Ethernet y permitir ese acceso de terceros para el mantenimiento o el envío de datos a entornos de computación en la nube. Esto ha conllevado el desarrollo de normativa de ciberseguridad específica como la IEC 62351, que se está orquestando con el estándar ISA/IEC62443 y que se tratará con más detalle en capítulos posteriores.

Figura 2 | **Arquitectura de subestación según el IEC 61850[2].**



- **Vehículo eléctrico y la red de puntos de recarga.** Se trata de un cambio que trae también retos en varias dimensiones. Por un lado, heredando cuestiones citadas anteriormente, se requieren centros de transformación digitalizados para tratar los datos de los consumidores y gestionar el reparto de cargas. Y es que los puntos de recarga que se van a necesitar son de recarga rápida o superiores, elevando los requisitos de planificación y coeficientes de concurrencia para evitar sobrecargas. Además, se están viendo modelos de gestión muy distintos entre sí: desde modelos en los que la *utility* posee y opera los puntos de recarga, requiriendo de terceros para suministro y mantenimiento pero explotando internamente los datos; hasta los puntos de recarga gestionados por el fabricante tanto a nivel eléctrico como de gestión de datos, haciendo de intermediario entre usuarios y *utilities*.

  Para las distintas posibilidades entre ambos extremos incluidos, el papel del regulador es muy distinto. Hay casos en los que no hay una regulación directa en el sistema, y otros en los que se plantea desde el operador eléctrico del sistema o en los que se propone un esquema sobre los distintos operadores del sistema, *utilities* o no.

  Por otro lado, se debe considerar el futuro impacto, aunque todavía incipiente, del uso reversible de la energía de las baterías de los coches *(vehicle to grid)*. Un devenir que, si bien puede ayudar a aportar estabilidad, plantea también retos en cuando a la apertura de tipos de comunicaciones entre nuevos actores.

> Estas nuevas tecnologías conforman nuevas cadenas de suministro a nivel tecnológico y de ciberseguridad

3.4. Los desafíos de la ciberseguridad en estos ámbitos eléctricos

Para los tres ámbitos presentados se ve claramente que los sistemas tradicionales están obligados a abrirse a modelos en los que nuevas oportunidades vienen asociadas a nuevos retos que se deben tener en cuenta.

Todo ello conlleva un fundamental cambio en la cadena de suministro en el que el mercado se debe abrir a un número mayor de fabricantes para incorporar nuevas tecnologías. Estas nuevas tecnologías, como los dispositivos IoT, vienen acompañadas de conectividad con entornos como la nube; y todo junto conforma nuevas cadenas de suministro a nivel tecnológico y de ciberseguridad que se comentarán a continuación.

- **La nueva cadena de suministro digital.** Ecosistema que abarca desde los fabricantes de dispositivos a los desarrolladores de aplicaciones en nube, pasando por el *firmware* y las aplicaciones embebidas en los dispositivos.

Los aspectos principales de dicha cadena de suministro serán:

- La identificación adecuada de los actores en cada proceso, sus roles y responsabilidades.
- La identificación de las nuevas interdependencias entre los nuevos actores que se deben tener en cuenta.
- Los niveles de seguridad a establecer, tanto a nivel de dispositivo como de aplicación y sistema.
- La necesidad de un enfoque global de la gestión de vulnerabilidades.
- La adopción de la filosofía *zero trust* (confianza cero), tanto para el diseño de arquitecturas como para su operación.

- **Nuevos esquemas de roles y responsabilidades.** Los riesgos en la cadena de suministro, la proliferación de un mayor número de actores y la dependencia del *hardware* y *software* nos debe llevar a hacer ejercicios de reflexión y de transparencia que permitan identificar a los responsables de cada etapa para su diseño, operación, mantenimiento, servicios y ciclo de vida de seguridad.

  Además, los roles no van a ser únicos por vertical, como se indica en la figura 3, sino que se abren distintas dimensiones a nivel de *firmware,* aplicaciones, dispositivos, equipos de usuarios, servidores, comunicaciones, nube, etcétera.

Figura 3 | **Esquema del sector eólico.**

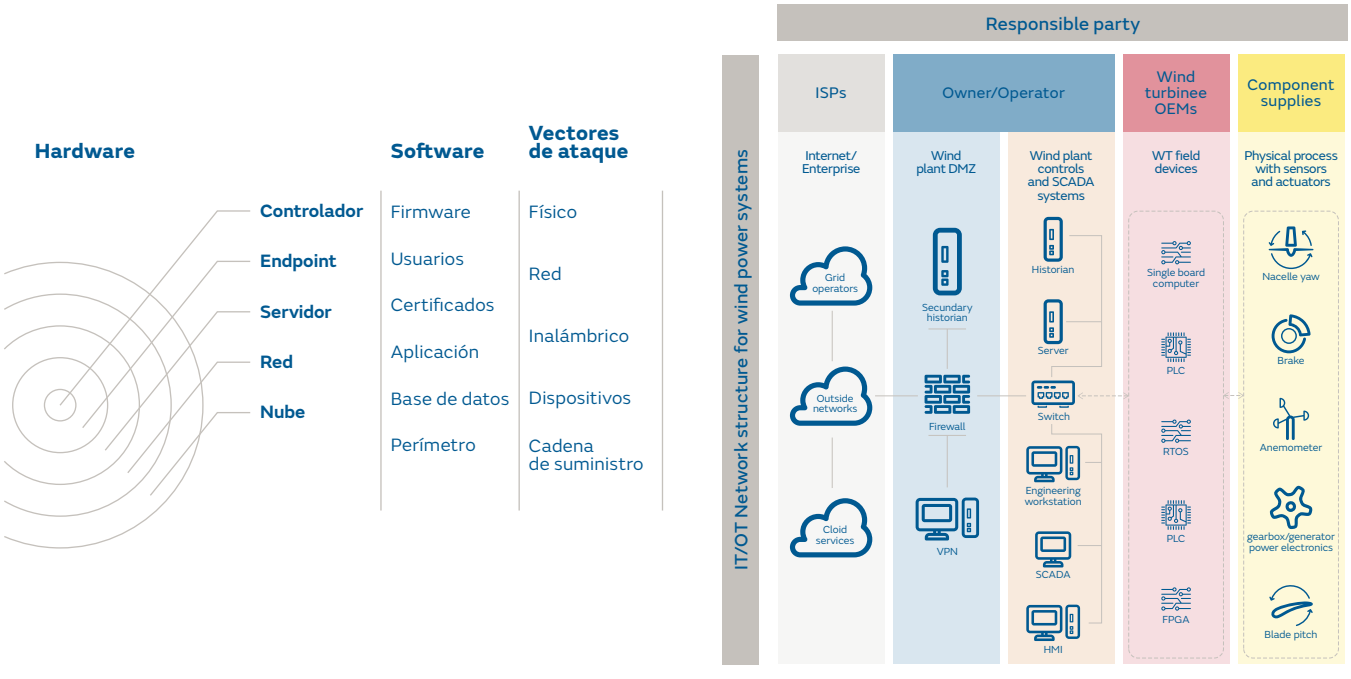
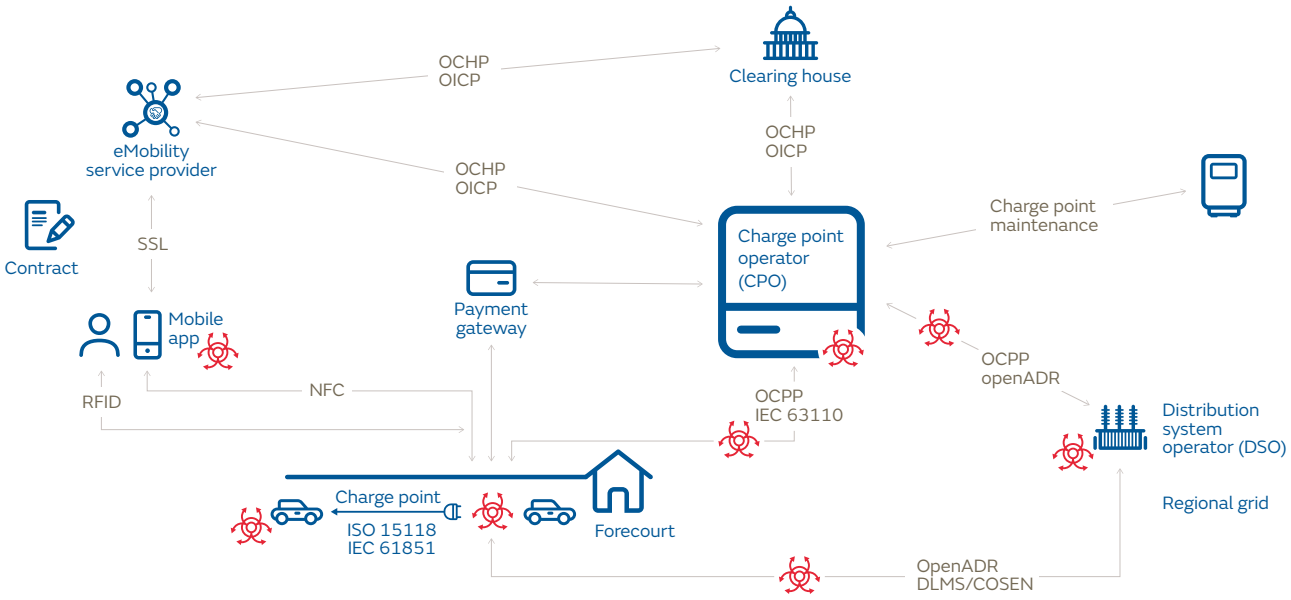


Figura 4 / **Ecosistema simplificado del vehículo eléctrico.**



- **Nuevos niveles de interdependencias.** Sirva de ejemplo la figura 4, un esquema muy simplificado del ecosistema del vehículo eléctrico que muestra las interconexiones entre sistemas como son los puntos de recarga, las *smartgrids,* las redes de distribución, redes de entornos de pago y redes 4G/5G que requieren un nuevo enfoque de riesgos absolutamente nuevo debido a la complejidad en su interconexión.

- **Niveles de seguridad de dispositivos y aplicaciones.** En base a los análisis de riesgos tradicionales, se indican cuántas capacidades de seguridad deben incluir los equipos a desplegar. El auge masivo del Internet de las Cosas y de los sistemas de automatización multipropósito *(commercial off the shelf)* obliga a estandarizar estas metodologías, tanto del análisis de riesgo como del establecimiento de requisitos.

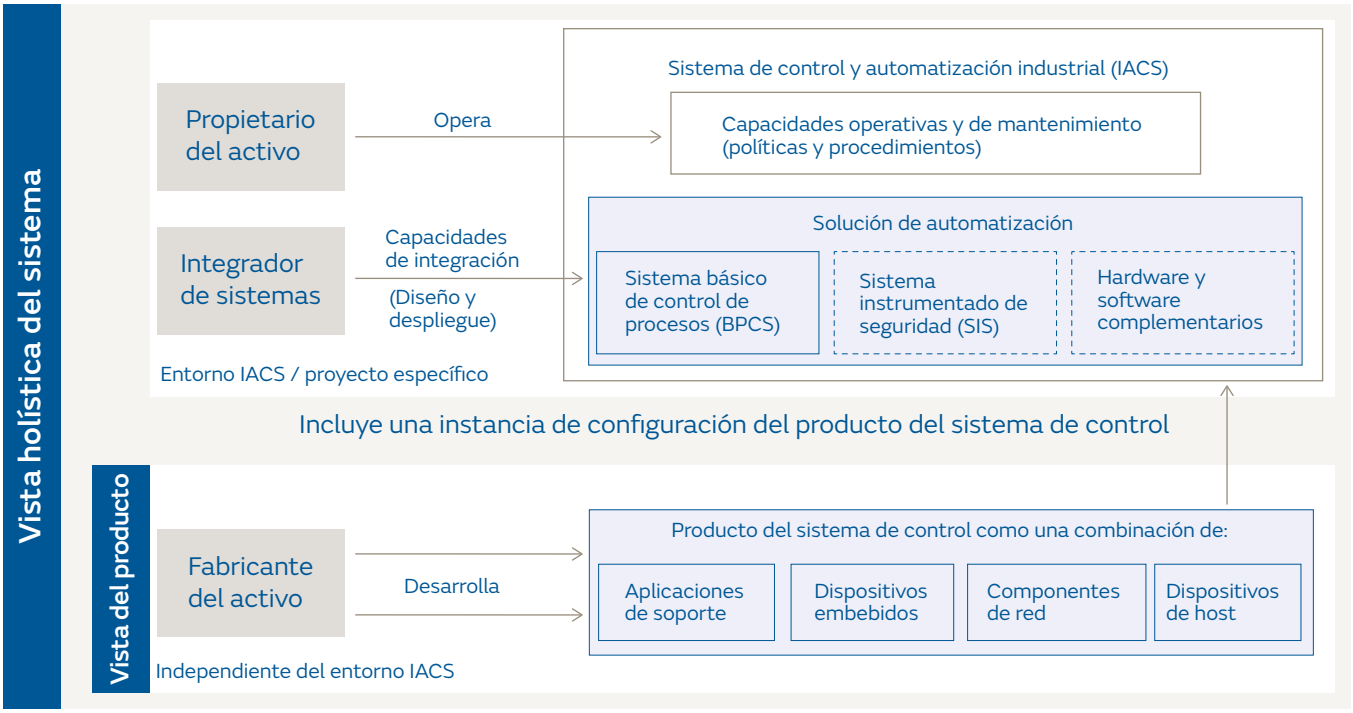
  Además, se está observando que ya no es efectivo hacer un análisis considerando el riesgo de un dispositivo para el proceso, sino que también es necesario el análisis de un conjunto de amenazas -miles o millones- para todo el ecosistema. Esto ha de servir como ejemplo, partiendo de los puntos anteriores, en pequeños paneles solares, equipos de aire acondicionado, aerotermia, cargadores domésticos de vehículo eléctrico, teléfonos móviles y todos aquellos sistemas en los que los ciclos de vida (y de seguridad) de *hardware, software* y *firmware* sean muy distintos. Como ya afirmaba la Agencia de la Unión Europea para la Ciberseguridad en 2019, los ciberriesgos asociados a un evento masivo siempre deben ser considerados.

  En este sentido, recientemente se ha publicado en Europa la Cyber Resilience Act, conocida como CRA, con un enfoque hacia la seguridad de dispositivos y que establece una metodología donde la mayoría de los citados se encuentran dentro del ámbito de la autoevaluación. En estas últimas se tendrán en consideración una serie de supuestos que deban evaluar los fabricantes y mostrar conformidad con su cumplimiento.

Dispositivos y sistemas más específicos se encuentran bajo la calificación de 'críticos' en dos posibles clases: *'class I'* o *'class II'*, que requieren una evaluación de terceros. Tradicionalmente, todos los sistemas asociados a infraestructuras críticas serán contemplados dentro la *class II;* sin embargo, sería muy costoso hacer pasar bajo un esquema de certificación a todos los dispositivos. En este aspecto será clave una toma de postura a nivel sectorial que permita aunar criterios y requisitos a los actores principales de esta nueva cadena de suministro. Por otro lado, es importante destacar el desarrollo del estándar ISA/IEC 62443 (4-1 y 4-2), que proporciona niveles y requisitos de ciberseguridad para todos los dispositivos industriales en los que los aspectos de seguridad intrínseca suelen presentar grandes rangos de variabilidad. Por tanto, se ha convertido en una base ideal a partir de la que establecer dicho modelo sectorial.

Es fundamental tener presente el rol y responsabilidad de cada uno de los actores en la cadena de suministro, donde encontraremos al fabricante del activo que desarrolla el producto tecnológico, aplicaciones y dispositivos, y que deberá contemplar capacidades de ciberseguridad y recomendación de configuración e integración. También está el integrador de sistemas, que diseña la arquitectura y despliega y configura las tecnologías. El tercer rol es el propietario del activo, que opera y mantiene las tecnologías del proceso automatizado.

Figura 5 | **Ciberseguridad holística para IACS (ISA/IEC 62443 2-4:2015).**



- **Nuevos enfoques para la gestión de vulnerabilidades.** Siempre se ha hablado de la obsolescencia como aspecto clave del sistema eléctrico dada la vocación de durabilidad con la que todos los equipos son diseñados. Sin embargo, se están dando numerosos casos en los que equipos nuevos reciben más notificaciones de seguridad. Si bien esto se debe a la mejora en los modelos de madurez de los programas de seguridad de los productos, también se empieza a comprobar la dificultad técnica de mantener unos ciclos de actualización de *software* sin que el servicio crítico sea perjudicado.

Por tanto, el enfoque está cambiando. Por un lado, debe estar basado en métricas que contemplen el elevado número de nuevos dispositivos. Y por otro, en priorizar en base a dos dimensiones: la situación de activos más críticos para el sistema y la situación respecto a las debilidades existentes.
Finalmente, merece la pena comentar el uso de tecnologías como el virtual *patching,* la capa virtual de seguridad delante de los dispositivos industriales con el fin de evitar que un código malicioso los alcance, permitiendo una adecuada mitigación sin tener que renunciar a la disponibilidad del proceso.

- **Entender adecuadamente el papel de la nube.** Es una realidad que la nube está presente en el sector eléctrico en mayor o menor medida. Y que es importante hacer un ejercicio de entendimiento sobre cómo trabajar con ella *(cloud).*

  Los proveedores de servicios en la nube se han dado cuenta de que la ubicación de los CPD (Centros de Procesamiento de Datos) es un aspecto clave, y por ello están ampliando el número de regiones por todo el planeta donde tienen presencia.

  Así, los propios proveedores de servicios en la nube están desplegando sus tecnologías en los propios CPD de las *utilities,* de esta manera algunas dudas relativas a estándares de seguridad o de continuidad de negocio podrían quedar aclaradas.

  Sin embargo, es imprescindible entender que la nube no es un todo o nada: todos los modelos de adopción del *cloud* conllevan un reparto de responsabilidades. Un ejemplo de ello es el esquema de Servicios Web de Amazon que contempla el reparto de responsabilidades respecto a un servicio crítico IT.

> Es fundamental tener presente el rol y responsabilidad de cada uno de los actores en la cadena de suministro.

- **Afrontar adecuadamente el *zero trust*.** Si bien se está hablando mucho de *zero trust* para la protección de datos, clasificación de información, privilegios de acceso y caracterización de usuarios, esta filosofía debe también ser trasladada a los entornos OT de forma adecuada, con la complejidad que ello supone.
  Abordar esta filosofía en esta clase de entornos nos llevará a un mayor nivel de transparencia y visibilidad a todos los niveles ya indicados, de modo que todo esté perfectamente identificado, validado, continuamente verificado y, por supuesto, asociado a una identidad determinada: desde un portátil o el servicio en la nube hasta el equipo industrial.

  Por tanto, asociar control de identidades en los accesos a las redes industriales y al uso de dispositivos de terceros, de los protocolos y aplicaciones conllevará un gran esfuerzo y despliegue de tecnologías de visibilidad e inventario. Pero también permitirá reducir la superficie de exposición a un nivel no alcanzado hasta ahora.

4. Modelo en implantación

Visto todo esto, es importante conocer los componentes necesarios en la nueva distribución eléctrica. Entre ellos la normativa que le afecta y las bases de este modelo desde tres puntos de vista: el humano, el legislativo y el tecnológico.

4.1. Consideraciones, estándares y normas

El sector eléctrico en general es considerado una infraestructura crítica nacional debido a que presta un servicio esencial para el funcionamiento de nuestra sociedad actual, en especial por su mayor utilización en el entorno digital en el que vivimos. Además, el ciberespacio se ha convertido en el quinto dominio de la guerra[3].

Por otro lado, el apoyo a la ciberseguridad nacional es una responsabilidad de todos, no solo del Estado[4]. Por lo tanto, cada organización de este sector debe establecer el diseño de su modelo de ciberseguridad industrial considerando para ello los elementos requeridos en tres dimensiones: personas, procesos y tecnologías. Un modelo que permita proteger los activos con una arquitectura de seguridad que contemple los aspectos regulatorios de

sus ubicaciones geográficas, pero que vaya mucho más allá, empezando por la evaluación de los requerimientos de seguridad de cada instalación y dispositivo de campo de acuerdo con su nivel de riesgo e importancia para el sistema eléctrico del país o región en la que opere; e incluso considerando la coordinación con las entidades públicas y los cuerpos de seguridad, normativos y de control.

A diferencia de lo que sucedía hace algunos años, cuando no se podía contar con elementos que guiaran el desarrollo de un modelo de seguridad digital o de un sistema de gestión de ciberseguridad industrial que respondiera efectivamente a las necesidades del sector eléctrico, hoy en día un modelo de ciberseguridad para la transmisión y distribución de energía eléctrica debe considerar la existencia de múltiples estándares internacionales asociados que pueden emplearse para su desarrollo y que cubren las diferentes necesidades de los procesos industriales enmarcadas en los requerimientos de seguridad de las diferentes partes interesadas de la organización a la que pertenecen.

Por esto, un modelo debe comenzar por considerar los elementos de gestión de riesgo que se pueden encontrar en las normas ISO 31000 y desarrollar los elementos del sistema de gestión de acuerdo con la norma ISO/IEC 27001 y el conjunto de normas ISO 27000[5] para integrarse al sistema de gestión de seguridad digital de la organización con énfasis en el análisis y aplicación de las referencias técnicas de la ISO/IEC TR 27019[6]. Pero esto es solo el comienzo de un entorno que debe ser evolucionado para proteger realmente la infraestructura crítica de la cual se es responsable. Por ello, la aplicación del Marco de ciberseguridad del NIST[7] aporta importantes elementos a la estructuración de un plan de ciberseguridad industrial, ya que nos ayuda a considerar la identificación, protección, detección, respuesta y recuperación en caso de incidentes.

Pero cuando vamos específicamente a la aplicación de protección en el entorno industrial debemos pasar a considerar estándares específicos como el conjunto de normas ISA/IEC 62443. Y cuando nos acercamos al entorno eléctrico, la protección debe considerar elementos que pueden obtenerse de regulaciones internacionales comúnmente aceptadas, de las normas NERC CIP y de estándares específicos como la IEC 62351.

Para el entorno de generación distribuida y el entorno cambiante que genera la nueva realidad de las redes de distribución con usuarios prosumidores, los modelos deben adaptarse a esta realidad y entender que cada parte de la cadena ha de estar protegida, de ser posible desde el diseño, para garantizar la seguridad y resiliencia del sistema.

Todas estas normas antes mencionadas guiarán en el desarrollo de un modelo completo que considere las implicaciones humanas, técnicas y procedimentales necesarias para su creación y funcionamiento en el tiempo.

4.2. Las bases del modelo de gestión

Todo modelo tiene diversos pilares, también el relativo a la nueva distribución eléctrica. En este caso, es importante destacar las dimensiones humana, normativa y tecnológica, las cuales constituyen unos pilares fundamentales que se sustentan entre sí, y que se desarrollarán a continuación.

4.2.1. Dimensión humana

La dimensión humana debe ser la base en un modelo de ciberseguridad industrial para la distribución, ya que todas las partes interesadas han de ser conscientes de las amenazas y riesgos que se están presentando en el entorno; así como de apoyar la disminución de las vulnerabilidades y en las que tenga influencia cada persona con el fin de evitar que éstas puedan ser usadas para lograr ataques efectivos contra el servicio o la misma organización.

Es clave, además, entender que el logro de los objetivos de ciberseguridad es una responsabilidad conjunta que tiene que ser abordada desde la alta dirección en equipo con los responsables de la seguridad, la operación, el mantenimiento, los fabricantes y los integradores. Y para ello, los esfuerzos deben ir más allá de la concienciación y lograr la interiorización del conocimiento y las habilidades requeridas por cada uno de acuerdo con su rol.

La preparación de las personas, igualmente, tiene que incluir escenarios de verificación y simulación que permitan evidenciar que cada uno cuenta con las habilidades y conocimientos necesarios para escalar y responder oportuna y efectivamente ante las situaciones que se puedan presentar.

4.2.2. Dimensión normativa

Esta dimensión está relacionada con el establecimiento de un sistema de gestión de ciberseguridad con un enfoque basado en los riesgos del entorno industrial y que permita reducir el nivel de riesgo inicial a uno aceptable para la organización.

Está enmarcada en las regulaciones aplicables en la zona geográfica donde se encuentran las instalaciones y de acuerdo con normas y estándares comúnmente aceptados en el entorno industrial.

Por ello es necesario que las entidades conozcan y apliquen las principales normas y estándares que facilitan la consecución de un entorno seguro de operaciones para su organización; en especial para la prestación de los servicios esenciales de generación, transmisión y distribución de energía eléctrica.

Este apartado presenta algunas normas y estándares reconocidos que ayudarán al lector a establecer, mantener y monitorizar un sistema de gestión de ciberseguridad con un enfoque internacional y aplicable a entornos industriales.

Para ello se describen las principales normas que permiten identificar, analizar y evaluar los riesgos (ISO 31000), pasando por los estándares que posibilitan establecer un conjunto de controles comúnmente aceptados como los mínimos esperados dentro de una organización (ISO 27000), incorporando más adelante aquellos que deben ser considerados por una organización categorizada como infraestructura crítica (NIST CSF), así como las guías específicas para entornos de redes inteligentes nacionales (NIST) y las asociadas al control de entornos industriales (ISA/IEC 62443).

La dimensión humana debe ser la base en un modelo de ciberseguridad industrial.

La aplicación efectiva e integrada de estas guías, normas y estándares debe realizarse, como se menciona en el apartado correspondiente a la dimensión humana, por personal capacitado, con habilidades y experiencia en ciberseguridad industrial y conocimientos del sector eléctrico y del entorno en el cual se requiere su implementación para lograr una efectiva armonización, una implantación en el entorno y una aceptación dentro de la cultura de la organización.

Las normas son las siguientes:

ISO 31000. Dirigida a gestionar el riesgo al que se enfrentan las organizaciones al integrar éste en todas sus decisiones, actividades y funciones.

Se requiere un análisis de riesgos para el correcto desarrollo de un modelo de ciberseguridad industrial. Por ello, al usar el conjunto de normas ISO 31000 como base es posible seguir su metodología, que es integrable con el resto de sistemas de gestión de la organización y con los análisis de riesgos de otras áreas. A través del análisis del contexto organizacional y de los criterios empresariales se puede identificar, analizar, valorar y definir estrategias de tratamiento de los mismos a la vez que se establecen las estrategias de comunicación y consulta al interior de la organización y los mecanismos de revisión y mejora requeridos para mantenerlos en un nivel aceptable para la institución.

ISO 27000. La norma ISO/IEC 27001, que desarrolla el Sistema de Gestión de Seguridad de la Información, se apoya en la ISO 27002 para establecer sus controles. Pero en el caso de los sistemas de control de procesos del sector energía se puede emplear el documento de referencia técnico ISO/IEC TR 27019, que aplica directamente sobre los sistemas de control de procesos utilizados por la industria de la energía para controlar y monitorizar la producción o generación, transmisión, almacenamiento y distribución de energía y para el control de los procesos de soporte asociados. Además, incluye un requisito para adaptar los procesos de evaluación y tratamiento de riesgos descritos en la ISO 27001:2013 a la orientación específica del sector de servicios de energía de una mejor manera.

Por consiguiente, se debe considerar el desarrollo de un sistema de ciberseguridad industrial que puede integrarse al sistema de gestión de seguridad de la organización y que puede ser guiado por la norma ISO/IEC 27001, que permite establecer el sistema, sopesando el contexto organizacional y los requisitos de las partes interesadas, estableciendo el compromiso de la dirección para su desarrollo de planear de acuerdo con los riesgos e incluyendo los requisitos para manejar las operaciones y el soporte, evaluar el sistema y mejorarlo de acuerdo con lo encontrado.

NIST CSF. El Marco para la mejora de la ciberseguridad en infraestructuras críticas, mejor conocida en inglés como *NIST Cibersecurity Framework* en su núcleo, establece la necesidad de mantener las funciones para identificar, proteger, detectar, responder y recuperar para lograr una gestión efectiva de la ciberseguridad frente a posibles ataques.

Ya que éste fue diseñado especialmente para la protección de infraestructuras críticas, se puede aplicar perfectamente en el diseño del modelo de protección para la nueva distribución eléctrica. Este marco nos hace reflexionar sobre las actividades que debemos tener en cuenta en cada una de las etapas. Los sistemas actuales no pueden considerar únicamente la prevención, sino que han de estar listos para detectar oportunamente los ciberatacantes en el entorno, responder antes de que generen un impacto considerable y recuperarse de una manera que brinde resiliencia a las operaciones manteniendo el servicio esencial.

NIST *Guidelines for Smart Grid Cybersecurity.* Estas guías del NIST[8] ayudan a ver el entorno de la ciberseguridad requerida en las redes inteligentes de energía con sus particularidades. Además, permiten mapear los controles en este tipo de redes de acuerdo con los objetivos de ciberseguridad seleccionando los requerimientos de acuerdo con los riesgos identificados y que permiten responder tanto a las regulaciones y los estándares como al entorno de ciberamenazas existente, todo ello teniendo en cuenta el nivel de impacto en cada punto.

Los requerimientos van desde el control de accesos y el entrenamiento hasta las pruebas y certificación de la ciberseguridad de las redes inteligentes. Eso sí, se contemplan diferentes elementos procedimentales, técnicos y de la gestión del personal y del gobierno.

IEC 62351. La serie de ciberseguridad para redes inteligentes *(smartgrids)* es un conjunto de estándares que incluyen las tecnologías de ciberseguridad para algunos de los protocolos más relevantes en este entorno, incluyendo el DNP3, el ICCP GOOSE y el modelo común de información CIM. Define los requisitos de ciberseguridad para el entorno operativo, entre ellos objetos para la gestión de redes y sistemas, control de acceso basado en roles, gestión de claves criptográficas y registro de eventos de seguridad. Es posible reusar los estándares, lo que facilita la interoperabilidad.

Entre algunos documentos de referencia técnica de estos estándares especialmente importantes para el desarrollo de los nuevos modelos de protección se encuentran el IEC/TR 62351-12, enfocado en la resiliencia de los sistemas de potencia con recursos distribuidos, así como los controles esenciales de la arquitectura definida en la IEC/TR 62351-10.

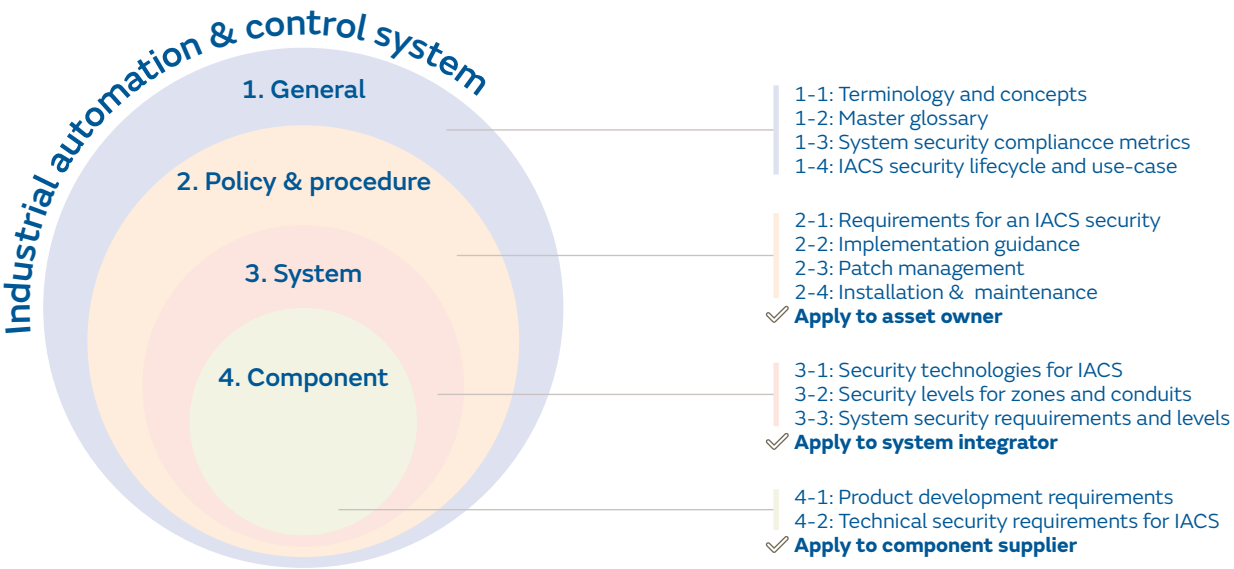
IEC 62443. El ISA/IEC 62443[9] es un estándar internacional de ciberseguridad en sistemas industriales que se centra en la disponibilidad y la integridad de los sistemas. Se basa en el principio de “defensa en profundidad”, el cual consiste en proporcionar múltiples capas de seguridad para evitar que las amenazas que sufre una de ellas puedan propagarse con facilidad al resto y afecten a los activos críticos. Cada capa establece una estrategia de defensa adicional y asume que la precedente pudo haber sido comprometida. Su implementación debe ser realizada con un enfoque basado en el riesgo.

Esta norma identifica tres instancias que influyen en los procesos operativos industriales: los fabricantes de dispositivos y equipos, los integradores de sistemas y los operadores de los sistemas. Además, proporciona un enfoque holístico para una mayor seguridad y, al mismo tiempo, tiene en consideración a los distintos actores.

El estándar se desarrolló para proteger los sistemas de control y automatización industrial (IACS) y las redes de comunicación industrial mediante un enfoque sistemático. Está organizada en varios documentos, incluyendo la IEC 62443-1-1, que define la terminología, conceptos y modelos para la seguridad IACS; la IEC 62443-2-1, que determina los elementos necesarios para establecer un sistema de gestión de seguridad cibernética; la IEC 62443-2-3, que describe los requisitos para los propietarios de activos y los proveedores de IACS y que se encarga de la gestión de parches en el entorno industrial; la IEC 62443-3-3-1, que traza varias categorías de seguridad cibernética, entradas en el sistema de control, los tipos de productos disponibles y las recomendaciones y guías para el uso de estos productos; y la IEC 62443-4-1, que proporciona requisitos para el ciclo de vida de desarrollo de productos seguros; y la IEC 62443-4-2, basada en requerimientos detallados de componentes del sistema de control asociados con los siete requisitos fundamentales: control de identificación y autenticación, control de uso, integridad del sistema, confidencialidad de los datos, flujo de datos restringidos, respuesta oportuna a eventos y disponibilidad de recursos.

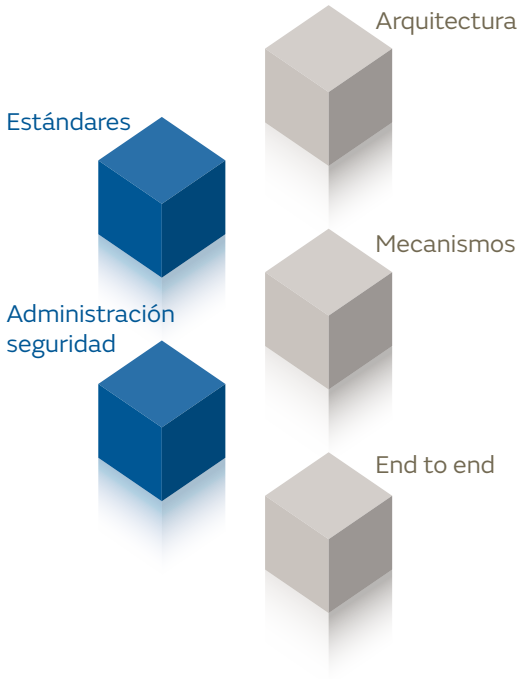
La norma está organizada como puede observarse en la figura 6.

Figura 6 | **The scope of IEC 62443 standard.** Fuente: Alter Technology



Considerando todos los requisitos, elementos y aspectos que incluye la IEC 62443, el sector de la energía va adoptando cada vez más este grupo de normas a fin de reducir y mitigar los riesgos tecnológicos en entornos industriales.

Figura 7 | **Dimensión tecnológica**



4.2.3. Dimensión tecnológica

La dimensión tecnológica (ver figura 7), como otro pilar del modelo, debe considerar la implementación de mecanismos de protección, empezando con la definición de una arquitectura base según las normas y estándares de ciberseguridad industrial y seguridad de la información ya identificados en la dimensión procedimental. A partir de aquí se construirá un modelo de defensa en profundidad estableciendo múltiples capas de protección que permitan autenticar y monitorizar los accesos a los dispositivos de supervisión y control, proporcionar el seguimiento a cualquier cambio en las configuraciones de los dispositivos, implementar mecanismos para garantizar la ausencia de *malware,* aplicar las mejores prácticas de seguridad definidas por los fabricantes y tener un respaldo completo de la plataforma.

El diseño de una arquitectura de seguridad adecuada para estos entornos ha de considerar la implementación de medidas pasivas de control como los firewalls, sistemas *antimalware* y medidas activas como los sistemas de detección y prevención de intrusiones que puedan contener y alertar sobre estas últimas. Eso sí, siempre hay que tener en cuenta que estas tecnologías no deben afectar a los procesos, por lo que deberá primar la alta disponibilidad y continuidad de la operación.

A continuación se presentan ejemplos de algunas buenas prácticas recomendas en la protección técnica:

- **Segmentación y defensa en profundidad.** Para garantizar la seguridad de los sistemas de control industrial es esencial implementar múltiples capas de protección que permitan desarrollar una defensa en profundidad.

> La monitorización sobre los aspectos de seguridad y las redes de comunicaciones debe ser continua: 7 días a la semana, 24 horas al día, 365 días al año.

Estos sistemas deben ser considerados como islas de alta seguridad, separadas de otras redes de la compañía (como las áreas administrativas), así como de las de proveedores y externos mediante mecanismos de control.

Es importante el diseño de esta segmentación teniendo en cuenta las zonas y conductos con base en la norma IEC 62443, donde una zona es una agrupación lógica o física de activos industriales (equipos, aplicaciones o información), los cuales comparten los mismos requisitos de seguridad; y un conducto agrupa las comunicaciones que permiten transmitir información entre diferentes zonas.

Es conveniente crear una DMZ industrial, que será la capa encargada de permitir el intercambio de información seguro entre la red industrial de la red corporativa, aportando protección al tiempo que limita el tráfico de automatización. En esta capa se alojan los servidores y servicios exclusivos para la red industrial.

- **Fortalecimiento.** Deben usarse las mejores prácticas de seguridad definidas por los fabricantes y los centros especializados en ciberseguridad desde la configuración inicial de todos los componentes de la infraestructura y verificarlas durante su ciclo de vida.

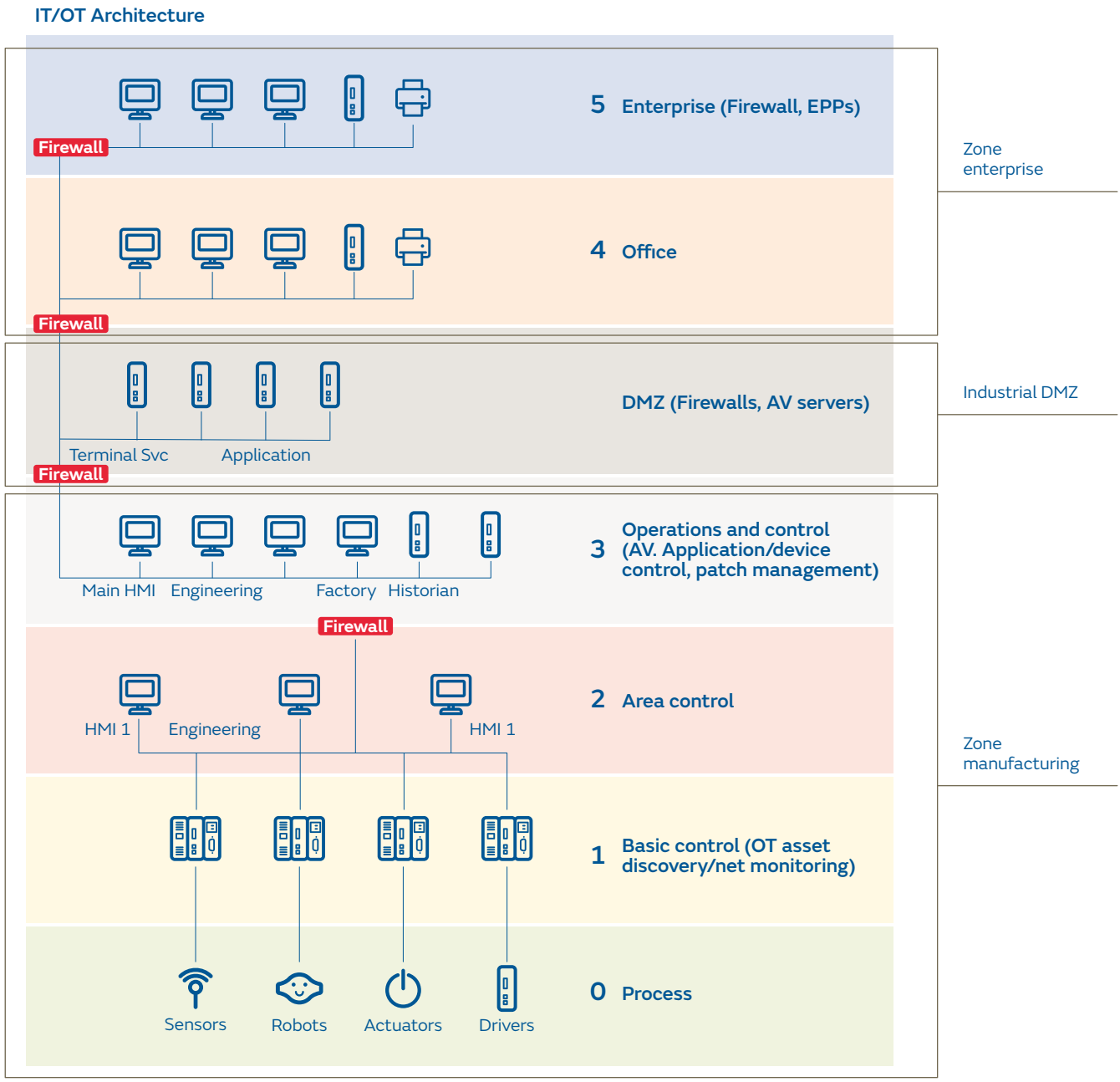
- **Control de configuraciones.** Ha de establecerse un seguimiento de cualquier cambio en las configuraciones de los dispositivos para evidenciar si están autorizados; y en caso de detectar anomalías, investigarlas como posibles incidentes de ciberseguridad.

- **Control de accesos y privilegios.** Los accesos a los dispositivos de supervisión y especialmente los de control y los remotos deben ser autenticados, limitados, monitorizados y registrados para futuras investigaciones de tal manera que permitan identificar tanto los ataques como las acciones indebidas o inadecuadas de los mismos usuarios, administradores, soportes remotos y terceros en las diferentes necesidades de gestión de la plataforma. Solo se debe permitir el acceso a estos sistemas a través de mecanismos seguros y solo deben acceder personas y tecnologías precisas de acuerdo con la necesidad de conocer y del principio del mínimo privilegio.

- **Control de accesos remotos.** Los accesos remotos tienen que hacerse por puntos de control que garanticen que no se involucran personas o dispositivos no autorizados o que no estén limpios en la infraestructura controlados por un “pivote” (máquina de salto), requerido para el acceso remoto a los equipos de la red industrial. Una red industrial que ha de grabar todas las acciones realizadas en la misma.

- **Gestión *antimalware*.** Deben implementarse donde sea posible mecanismos que garanticen la ausencia de *malware* en la red o en los dispositivos, teniendo cuidado con que sus acciones automáticas nunca puedan afectar a la prestación del servicio. Aquí también se tienen que evaluar las listas blancas de aplicación.

Figura 8 | **Modelo Purdue.** Fuente: Gartner.



- **Evaluación y gestión de vulnerabilidades.** La evaluación de las vulnerabilidades de la plataforma tiene que ser constante por métodos pasivos que no afecten la operación. Y también periódica con métodos activos que pueden ser sincronizados con las ventanas de mantenimiento para mantener la infraestructura lo más limpia posible a través de la implementación de los parches requeridos ofrecidos por los fabricantes lo más pronto posible.

- **Monitorización.** La monitorización sobre los aspectos de seguridad y las redes de comunicaciones en zonas seguras debe ser continua (7 días a la semana, 24 horas al día, 365 días al año), especializada y con entendimiento de los protocolos industriales de tal manera que permita el análisis centralizado y la verificación de las anomalías que puedan ocurrir. La monitorización ha de evitar introducir tráfico a las redes de control; además, deberán existir mecanismos y personal de respuesta en tiempo real.

- **Continuidad y resiliencia.** El respaldo completo de la plataforma ha de ser una prioridad. También la verificación de los mecanismos de respaldo, continuidad y resiliencia que se han diseñado para garantizar la continuidad del servicio y la seguridad de las personas, el medio ambiente y los equipos.

4.3. Construcción del modelo

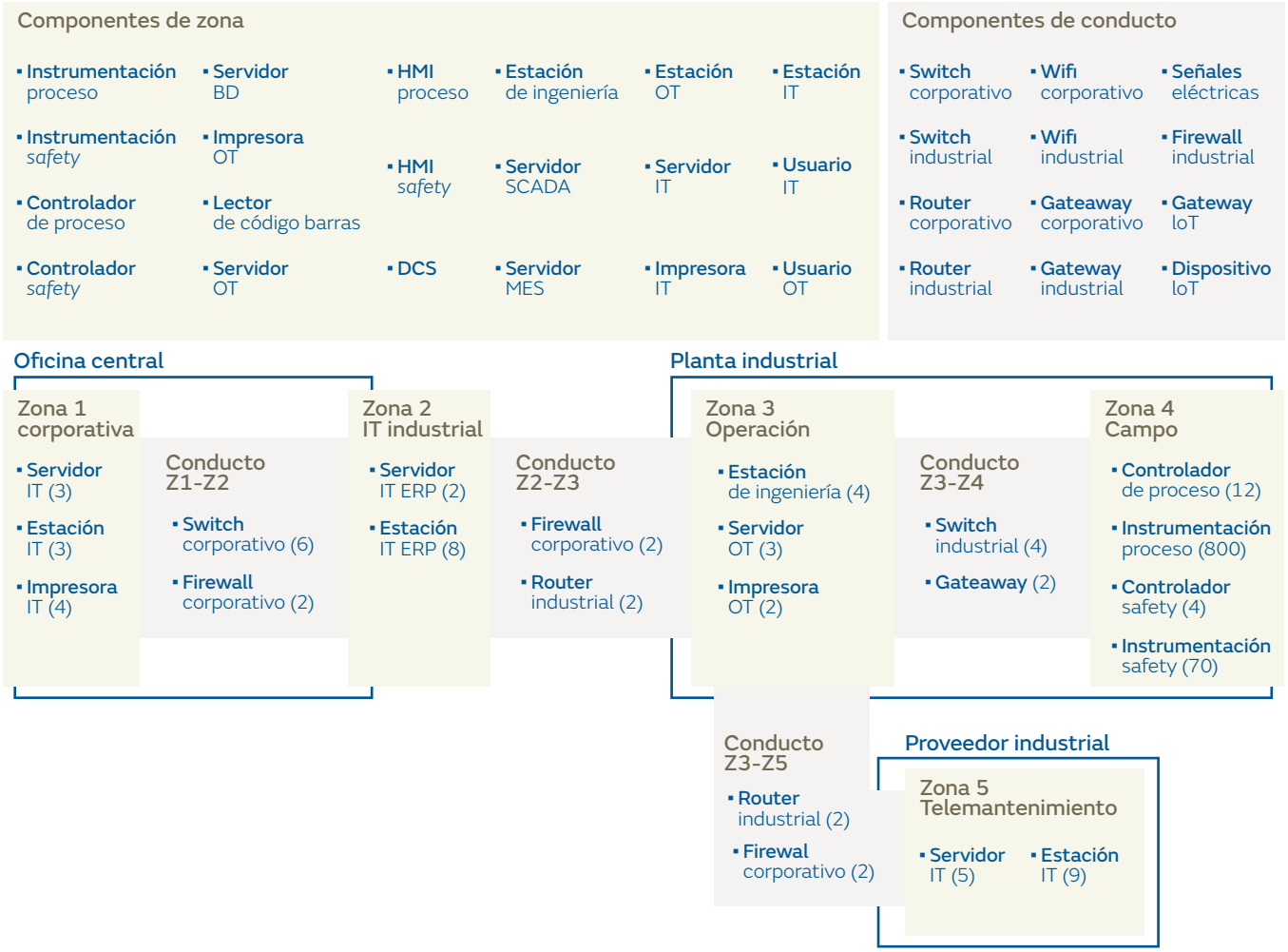
Como ya se ha apuntado, al pensar en un modelo para la nueva distribución eléctrica no podemos solo pensar en el modelo específico de las instalaciones relevantes para la distribución hacia los centros de consumo. Debemos pensar en la protección de toda la cadena que actúa en ocasiones como consumidor y en otras como productor, agregando una complejidad importante pero que puede disminuirse si se trabaja en aplicar seguridad desde el diseño y en cada una de las fases de la implementación de los nuevos proyectos, así como en las adaptaciones y renovaciones necesarias.

En diversos países se han establecido regulaciones y normas técnicas que incluyen la definición de ciberseguridad de los medidores de energía, de las redes inteligentes y de los dispositivos que facilitan el intercambio de datos con los centros de gestión y control de medida, elemento que también debe considerarse en el modelo para lograr una protección completa del entorno de distribución eléctrica hasta los centros de consumo.

La protección de los centros de control del entorno de distribución eléctrica y de los diversos dispositivos de campo en las subestaciones se pueden beneficiar ampliamente de la metodología propuesta por la norma IEC 62443. Esta normativa facilita identificar las zonas de estos componentes con sus niveles de seguridad adecuados según las amenazas a las que están expuestas ellas y los conductos que permiten el intercambio de datos, aplicando el principio de “defensa en profundidad” para la protección mediante capas.

De igual forma, con el crecimiento de la Industria 4.0 es indispensable la convergencia IT y OT, con el propósito de extraer los datos de los sistemas de control y supervisión industrial y gestionarlo desde IT para la toma de decisiones y/o gestión. Por lo tanto, el modelo de ciberseguridad debe incluir los aspectos necesarios para proteger las redes y sistemas industriales de los vectores de ataque que pueden presentarse en la red IT.

Figura 9 | **Zonas y conductos IEC62443.** Fuente: Centro de Ciberseguridad Industrial.



Para ello, el Modelo Purdue y la separación en zonas y conductos de la norma IEC 62443 son una base fundamental que facilita la definición de capas de protección de los sistemas industriales mediante la definición de varios niveles sobre los que se aplicarán medidas de ciberseguridad, tanto en los sistemas de los niveles OT (0, 1, 2 y 3) como de los niveles IT (4 y 5), a fin de proporcionar protección en la convergencia IT y OT.

En cada uno de los niveles de este modelo y de las zonas y conductos se tienen que definir las medidas de ciberseguridad apropiadas, basadas en la evaluación de riesgos y en la definición del nivel objetivo al que se desee llegar.

Para definir las medidas necesarias se deberán seguir los siguientes pasos:

1. Evaluar las capacidades de ciberseguridad de cada componente o subsistema, considerando los siete requisitos fundamentales y contrastando cada uno con los requisitos de ciberseguridad que presenta la norma.

2. Determinar el nivel de ciberseguridad objetivo al que se desea llegar (ver figura 10).

3. Determinar el nivel de ciberseguridad alcanzado por cada componente o subsistema y validar si supera o si es menor al nivel de seguridad objetivo.

4. Para los componentes que no alcancen el nivel de ciberseguridad objetivo, se debe considerar las medidas compensatorias para reducir las brechas.

5. Realizar el análisis de riesgos a los componente o sistemas que tienen brechas a fin de determinar la prioridad de implementación de contramedidas.

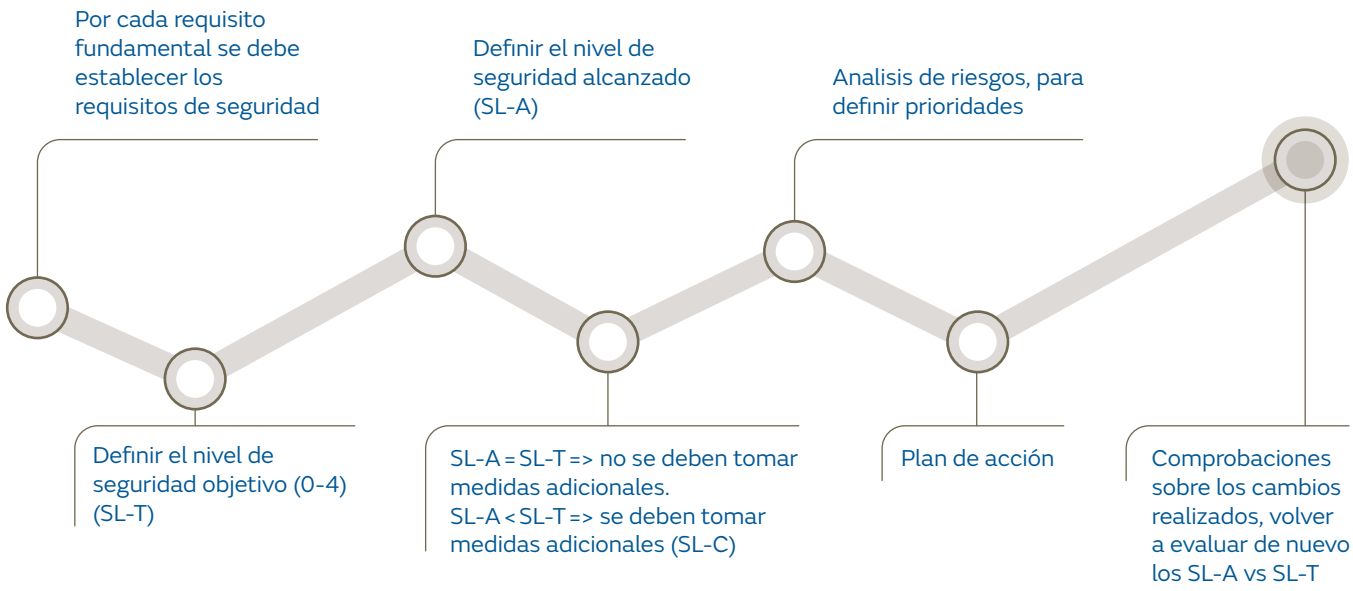
6. Definir el plan de acción y cronograma de implementación.

7. Realizar la reevaluación de los componentes y sistemas.

Figura 10 | **Niveles de ciberseguridad.**

Cada vez que se realice una modificación en los sistemas industriales, su nivel de seguridad debe ser evaluado. De esta manera se obtendrá el nivel de seguridad alcanzado (SL-A) y se podrá comparar este con el nivel objetivo (SL-T) (ver figura 11).

Figura 11 | **Evaluación niveles de seguridad.**



> Se requiere un modelo integral que permita responder a las diferentes regulaciones y las nuevas realidades en los diferentes puntos de la cadena.

Por otro lado, uno de los aspectos que acelera una digitalización segura de los entornos industriales, especialmente de un sistema de distribución eléctrica con dispositivos de campo que pueden localizarse incluso en las residencias de los consumidores , es considerar el principio de “confianza cero”. Esto permitirá resistir mejor los ataques que puedan presentarse.

Todo ello abarca tres principios básicos:

1. **Comprobar de forma explícita.** Entre los mecanismos de contención a implementar se deberán incluir aquellos que garanticen la autenticación y autorización, considerando que se niega de manera predeterminada, siempre en función de todos los datos disponibles. Esto incluye la identidad del usuario, la ubicación, el estado del dispositivo, el servicio, la clasificación de datos y las anomalías.

   En cuanto a los dispositivos que contempla esta red, deberían contar con mecanismos de autenticación de doble factor y basarse en tecnologías de cifrado avanzada que garanticen que solo éstos pueden pertenecer a la misma.

2. **Uso de acceso con menores privilegios.** Limitar el acceso de los usuarios con los permisos suficientes y en el tiempo preciso, implementar directivas basadas en riesgos y protección de datos, impulsar la detección de amenazas y mejorar las defensas.

3. **Asumir la vulneración.** Aplicando el principio de “defensa en profundidad” se minimiza el radio del alcance y se segmenta el acceso, se comprueba el cifrado de extremo a extremo y se utilizan los análisis para obtener visibilidad, impulsar la detección de amenazas y mejorar las defensas.

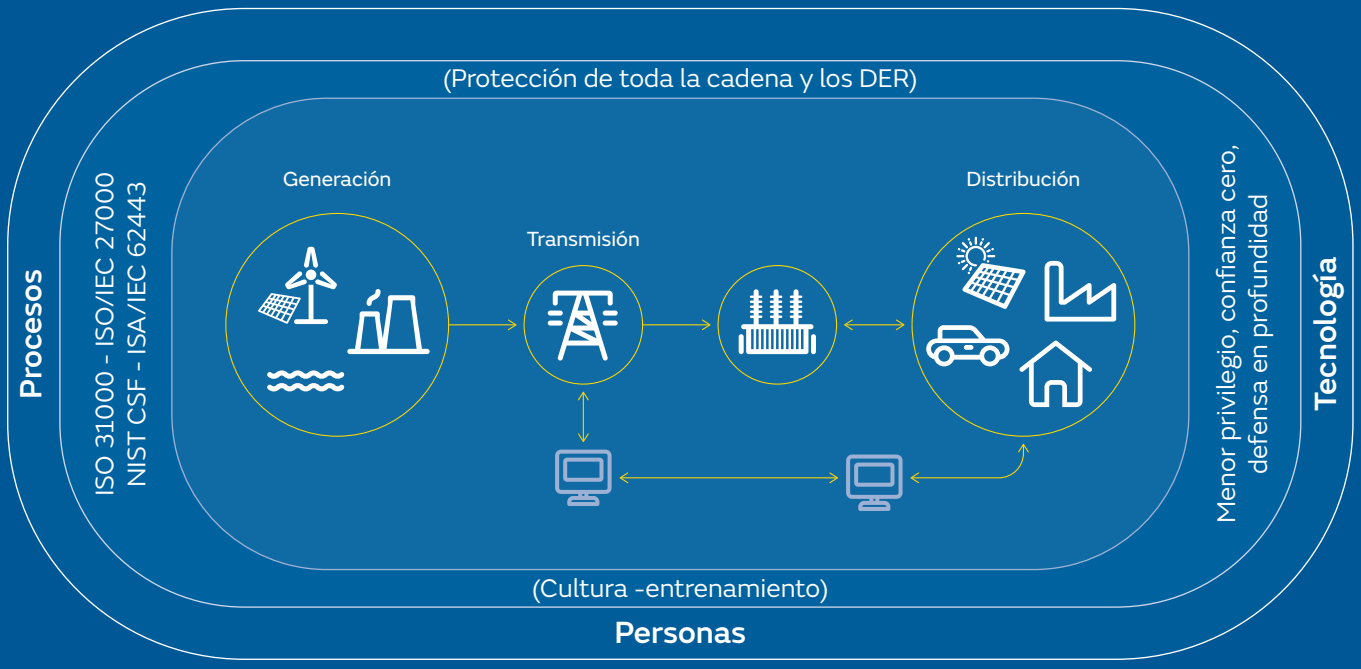
Como plantea el Departamento de Energía de los Estados Unidos[10], los recursos de energía distribuida se están enfrentando a una serie de vectores de ataques. Entre ellos *ransomware,* compromisos en la cadena de suministro, *botnets* o gusanos. Todos podrían afectar a una escala importante a toda la cadena de suministro del sector eléctrico. Es por ello que la seguridad debe estar en el ADN de cada uno de los componentes de las redes inteligentes y de la distribución eléctrica.

Asimismo, la Comisión Europea, que busca medidas unificadas de ciberseguridad a través de la Directiva NIS 2, exige medidas de seguridad para las entidades críticas. De hecho, hace responsable a la alta dirección de las organizaciones de su mantenimiento e incluye la gestión de la cadena de suministro. Además, ya ha presentado propuestas para una Ley de Resiliencia Cibernética que permita una protección ante productos con características de seguridad inadecuadas. Unos productos que deberán incluir la ciberseguridad desde el diseño, la gestión de vulnerabilidades y la seguridad durante todo el ciclo de vida de los productos.

Se requiere entonces un modelo integral que permita responder a las diferentes regulaciones y las nuevas realidades en los diferentes puntos de la cadena, considerando los elementos clave y facilitando la respuesta oportuna frente a los eventos e incidentes que se puedan presentar.

Por todo ello se han de considerar a las personas, los procesos y la tecnología requerida para lograr el mantenimiento de la confidencialidad, integridad y disponibilidad de los sistemas ciberfísicos involucrados y de la información que permitan mantener la operación continua y resiliente del sistema eléctrico como un todo en los nuevos escenarios de comunicaciones bidireccionales y de gestión, interconexión e interacción continua en toda la cadena (ver figura 12).

Figura 12 | **Modelo de ciberseguridad en distribución eléctrica.**



5. Regulaciones

La Unión Europea ha tomado un papel de liderazgo en materia de Ciberseguridad. Un ejemplo de ello son las diversas normativas que ha puesto en marcha recientemente, todas ellas de gran calado: servicios esenciales, ciberresiliencia o Seguridad desde el diseño son algunos de los elementos que ha querido potenciar a nivel comunitario.

5.1. Marco normativo actual de la ciberseguridad

Este capítulo aborda el marco regulatorio de la ciberseguridad y la resiliencia a nivel europeo, el cual marcará las regulaciones de los Estados de la Unión.

En el último trimestre de 2022 se han aprobado multitud de regulaciones europeas en materia de ciberseguridad, seguridad y resiliencia que marcan un cambio de enfoque para todos los sectores, especialmente para las infraestructuras críticas, tanto a nivel europeo como a nivel de cada Estado miembro; cada uno de ellos va a tener que adaptar sus regulaciones al nuevo marco regulatorio europeo.

Adicionalmente, se contemplan normas y buenas prácticas de ciberseguridad promovidas y adoptadas en otros países.

5.2. Regulación de ciberseguridad y resiliencia europea

La resiliencia es uno de los pilares de la ciberseguridad que ha querido potenciar la Unión Europea: es vital que las organizaciones se recuperen ante un potencial ciberataque. A continuación se destacan diversas normativas relacionadas con este elemento, algunas de ellas publicadas de forma reciente.

Ciberseguridad de servicios. En este apartado podemos destacar dos normativas. La primera es el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la ciberseguridad) y a la Certificación de la Ciberseguridad de las tecnologías de la Información y la Comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 (Reglamento sobre la ciberseguridad).

La segunda es la conocida como Directiva NIS 2 (Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de

ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148).

Esta última normativa entró en vigor a los 20 días de su publicación en el Diario Oficial de la Unión Europea, el 16 de enero de 2023.

Además, a más tardar el 28 de octubre de 2024, los Estados miembros adoptarán y publicarán las medidas necesarias para dar cumplimiento a lo establecido en ella, y comunicarán inmediatamente a la Comisión el texto de dichas disposiciones, de aplicación a partir del 29 de octubre de 2024.

Resiliencia en infraestructuras críticas. Aquí cabe destacar la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo y Recomendación 2023/C20/01 del Consejo, de 8 de diciembre de 2022, sobre un enfoque coordinado en toda la Unión para reforzar la resiliencia de las infraestructuras críticas.

Los Estados miembros adoptarán y publicarán, a más tardar el 28 de julio de 2024, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en esta normativa, y comunicarán inmediatamente a la Comisión el texto de dichas disposiciones, las cuales deberán aplicar a partir del 29 de enero de 2025.

Ciberseguridad y seguridad de producto. En este apartado diferenciamos, de nuevo, dos regulaciones. La primera, la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020, conocido como Cyber Resilience Act.

Y la segunda, la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a las máquinas y sus partes y accesorios.

Protección de datos. Destaca el RGPD; es decir, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

5.3. Principales implicaciones de la ciberseguridad

Como se ha mencionado con anterioridad, la Unión Europea tiene un papel de liderazgo en materia de ciberseguridad. De ahí que recientemente haya publicado varias normativas de gran calado para el sector, como son el caso de la conocida como Directiva NIS 2, la Directiva de Resiliencia de las entidades críticas y la Propuesta de Reglamento relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020, de las que destacamos los puntos más importantes.

5.3.1. Directiva NIS 2

Los sistemas de información y redes se han convertido en una característica central de la vida cotidiana con la rápida transformación digital y la interconexión de la sociedad, incluso a nivel transfronterizo.

Ese desarrollo ha llevado a una expansión del panorama de las ciberamenazas, generando nuevos desafíos que requieren respuestas adaptadas, coordinadas e innovadoras en todos los Estados miembros.

Las autoridades han establecido una serie de normas mínimas relativas al funcionamiento de un marco reglamentario coordinado, instaurando mecanismos para una cooperación eficaz entre las autoridades responsables de cada Estado miembro, actualizando la lista de sectores y actividades sujetas a obligaciones en materia de ciberseguridad y proporcionando remedios efectivos y medidas de cumplimiento que son clave para el cumplimiento efectivo de dichas obligaciones.

5.3.1.1. Prevención de vulnerabilidades y gestión y respuesta de incidentes

Las políticas de higiene cibernética proporcionan las bases para proteger la red y las infraestructuras de sistemas de información, *hardware, software* y seguridad de aplicaciones en línea, así como los datos comerciales o de usuarios finales en los que se basan las entidades.

Las políticas de ciberhigiene que comprenden un conjunto básico común de prácticas, incluidas las actualizaciones de *software* y *hardware,* los cambios de contraseña, la gestión de nuevas instalaciones, la limitación de las cuentas de acceso a nivel de administrador y la copia de seguridad de los datos, permiten un marco proactivo de preparación y seguridad y protección general en caso de incidentes o ciberamenazas. Es ENISA, en este sentido, quien debe supervisar y analizar las políticas de ciberhigiene de los Estados miembros.

La conciencia y la ciberhigiene son esenciales para mejorar el nivel de la ciberseguridad dentro de la Unión; en particular a la luz del creciente número de dispositivos conectados, y que son víctimas de un volumen de ciberataques cada vez mayor. Por tanto, deben realizarse esfuerzos para mejorar la conciencia general de los riesgos relacionados con dichos dispositivos, mientras que las evaluaciones a nivel de la Unión podrían ayudar a garantizar una comprensión común de tales riesgos en el mercado interior.

Los Estados miembros han de desarrollar una política que aborde el aumento de los ataques de ransomware como parte de su estrategia nacional de ciberseguridad, y tratar las necesidades específicas de ciberseguridad de las pequeñas y medianas empresas.

Como parte de sus estrategias nacionales de ciberseguridad, estos países también tienen que adoptar políticas sobre la promoción de la ciberprotección activa como parte de una estrategia defensiva más amplia. En lugar de responder de manera reactiva, la protección cibernética activa es la prevención, detección, monitoreo, análisis y mitigación de violaciones de seguridad de la red de manera activa, combinada con el uso de capacidades desplegadas dentro y fuera de la red de la víctima.

Dado que la explotación de vulnerabilidades en las redes y los sistemas de información puede causar una interrupción y un daño significativos, identificar y remediar rápidamente dichas vulnerabilidades es un factor importante para reducir el riesgo. Por lo tanto, las entidades que desarrollan o administran redes y sistemas de información deben establecer procedimientos apropiados para manejar las vulnerabilidades cuando se descubren. Dado que estas suelen ser localizadas y reveladas por terceros, el fabricante o proveedor de productos o servicios de TIC (tecnologías de la información y la comunicación) también tiene que establecer los procedimientos necesarios para recibir información sobre vulnerabilidades de terceros.

Por otro lado, ha de promoverse y desarrollarse una cultura de gestión de riesgos que implique evaluaciones y la implementación de medidas de gestión adecuadas a las amenazas.

Las medidas de gestión de riesgos de ciberseguridad deben tener en cuenta el grado de dependencia de la entidad esencial o importante en la red y los sistemas de información. Así como incluir medidas para identificar cualquier riesgo de incidentes, prevenir, detectar, responder, recuperarse de ellos y mitigar su impacto. La seguridad de las redes y los sistemas de información tiene que incluir la seguridad de los datos almacenados, transmitidos y procesados. Las medidas de gestión de riesgos de ciberseguridad deben prever un análisis sistémico, teniendo en cuenta el factor humano, para disponer de una imagen completa de la seguridad de la red y el sistema de información.

Por lo tanto, las medidas de gestión de riesgos de ciberseguridad también deben abordar la seguridad física y ambiental de las redes y los sistemas de información al incluir medidas para proteger dichos sistemas de fallas, errores humanos, actos maliciosos o fenómenos naturales. Todo ello en línea con los estándares europeos e internacionales.

Con el fin de demostrar el cumplimiento de la gestión de riesgos de ciberseguridad y en ausencia de esquemas europeos de certificación de ciberseguridad apropiados adoptados de conformidad con el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, los Estados miembros, en consulta con el Grupo de Cooperación y el Grupo Europeo de Certificación de la ciberseguridad, deben promover el uso de las normas europeas e internacionales pertinentes por parte de entidades esenciales e importantes. O pueden exigir a las entidades que utilicen productos, servicios, servicios TIC y procesos TIC certificados.

Para evitar imponer una carga financiera y administrativa desproporcionada a entidades esenciales e importantes, las medidas de gestión de riesgos de ciberseguridad deben ser proporcionales a los riesgos planteados para la red y el sistema de información en cuestión. Eso sí, teniendo en cuenta el estado de la técnica de tales medidas y, cuando corresponda, las normas europeas e internacionales pertinentes, los estándares y el costo de su implementación.

Las medidas de gestión de riesgos de ciberseguridad deben ser proporcionales al grado de la exposición de la entidad esencial o importante a los riesgos y al impacto social y económico que tendría un incidente.

> Los productos críticos con elementos digitales estarán sujetos a procedimientos específicos de evaluación de la conformidad dependiendo de su nivel de riesgo de ciberseguridad.

5.3.1.2. Cadena de suministro

Las organizaciones están obligadas a abordar los riesgos derivados de la cadena de suministro de una entidad y su relación con sus proveedores. Las entidades esenciales e importantes deben evaluar y tener en cuenta, en este sentido, la calidad general y la resiliencia de los productos y servicios, las medidas de gestión de riesgos de ciberseguridad integradas en ellos y las prácticas de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro.

En particular, se ha de alentar a las entidades esenciales e importantes a incorporar medidas de gestión de riesgos de ciberseguridad en los acuerdos contractuales con sus proveedores directos y proveedores de servicios. Esas entidades podrían considerar riesgos derivados de otros niveles de proveedores y prestadores de servicios. Por lo tanto, las entidades esenciales e importantes tienen que ejercer una mayor diligencia al seleccionar un proveedor de servicios de seguridad gestionados.

Para seguir abordando los riesgos clave de la cadena de suministro y ayudar a las entidades esenciales a gestionarlos adecuadamente, el Grupo de Cooperación, junto con la Comisión Europea y ENISA, y cuando proceda tras consultar a las partes interesadas pertinentes (incluidas las de la industria), debe llevar a cabo evaluaciones coordinadas de riesgos de seguridad de las cadenas de suministro críticas con el objetivo de identificar por sector los servicios críticos TIC, los sistemas TIC, los productos TIC, las amenazas y las vulnerabilidades relevantes.

Para localizar las cadenas de suministro que deben estar sujetas a una evaluación coordinada de riesgos de seguridad se tratan de tener en cuenta los siguientes criterios: la medida en que las entidades esenciales e importantes usan y confían en servicios TIC críticos específicos, sistemas TIC o productos TIC; la relevancia de servicios TIC críticos específicos, sistemas TIC o productos TIC para realizar funciones críticas o sensibles, incluido el procesamiento de datos personales; la disponibilidad de servicios alternativos TIC, sistemas TIC o productos TIC; la resiliencia de la cadena de suministro general de servicios TIC, sistemas TIC o productos TIC a lo largo de su ciclo de vida frente a eventos disruptivos; y para servicios TIC emergentes, sistemas TIC o productos TIC, su importancia futura potencial para las actividades de las entidades.

Además, debe hacerse hincapié en los servicios TIC, los sistemas TIC o los productos TIC que estén sujetos a requisitos específicos derivados de terceros países.

5.3.1.3. Notificación de incidentes

Cuando las entidades esenciales o importantes tomen conocimiento de un incidente significativo, se les debe exigir que envíen una alerta temprana sin demora indebida y, en cualquier caso, dentro de las 24 horas. Esa alerta temprana tiene que ir seguida de una notificación de incidente. Las entidades afectadas tendrán la obligación de presentar una notificación de incidente sin demoras indebidas y, en todo caso, dentro de las 72 horas siguientes a la toma de conocimiento del incidente significativo. El objetivo es, en particular, actualizar la información enviada a través de la alerta temprana e indicar una evaluación inicial del incidente significativo, incluido su gravedad e impacto, así como indicadores de compromiso cuando estén disponibles. Además, tendrán que presentar un informe final a más tardar un mes después de la notificación del incidente.

Cuando corresponda, las entidades esenciales e importantes deberán comunicar a los destinatarios de sus servicios, sin demoras indebidas, cualquier medida o remedio que puedan tomar para mitigar los riesgos resultantes de una amenaza cibernética significativa. La provisión de dicha información debe ser gratuita y estar redactada en un lenguaje fácilmente comprensible.

5.3.1.4. Responsabilidad

Los órganos de dirección de las entidades esenciales e importantes tienen que aprobar las medidas de gestión de riesgos de ciberseguridad y supervisar su implementación, existiendo responsabilidad por ello.

5.3.2. Directiva de Resiliencia de Infraestructuras Críticas

El Diario Oficial de la Unión Europea publicó, el 27 de diciembre, la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas: una nueva legislación que obliga a los Estados miembros a adoptar medidas específicas para garantizar la prestación de los servicios esenciales, pero que, sobre todo, establece la identificación de las entidades críticas y que aborda el cumplimiento de las obligaciones impuestas a estas últimas. Este documento destaca los elementos más importantes de ella.

5.3.2.1. Identificación

Esta normativa establece un procedimiento para que los Estados miembros identifiquen las entidades críticas utilizando criterios comunes sobre la base de una evaluación nacional de riesgos. En este sentido, al identificar las entidades críticas, los Estados miembros tendrán en cuenta los resultados de la evaluación de riesgos y aplicarán los siguientes criterios:

a) La entidad presta uno o más servicios esenciales.

b) La prestación de dicho servicio depende de la infraestructura situada en el Estado miembro.

c) Un incidente tendría efectos perturbadores significativos en la prestación de ese servicio o de otros servicios esenciales en los sectores mencionados en el anexo que dependen del servicio.

Las autoridades competentes designadas nacionales elaborarán una lista de los servicios esenciales en sectores específicos. Estas llevarán a cabo, a más tardar el 29 de octubre de 2025, y posteriormente cuando sea necesario, al menos cada cuatro años, una evaluación de todos los riesgos pertinentes que puedan afectar a la prestación de tales servicios esenciales, con vistas a identificar las entidades críticas y a ayudar a dichas entidades a adoptar medidas necesarias.

La Directiva de Resiliencia de Infraestructuras Críticas se alinea con la NIS 2, garantizando que las autoridades competentes designadas en virtud de esta normativa y las designadas en virtud de la Directiva NIS 2 adopten medidas complementarias e intercambien información cuando sea necesario en relación con la ciberresiliencia y la resiliencia no cibernética; y que las entidades especialmente críticas de los sectores considerados esenciales, en la NIS 2, también estén sujetas a obligaciones generales de mejora de la resiliencia para hacer frente a los riesgos no cibernéticos.

5.3.2.2. Análisis y gestión de riesgos de resiliencia

El objetivo de esta directiva no es proteger un conjunto limitado de infraestructuras físicas cuya perturbación o destrucción tendría un impacto transversal significativo, sino aumentar la resiliencia de las entidades críticas para la prestación de servicios esenciales de los Estados miembros para mantener las funciones sociales o económicas vitales en el mercado interior en una serie de sectores que sustentan el funcionamiento de muchos otros en la Unión.

Las entidades críticas evaluarán periódicamente todos los riesgos pertinentes sobre la base de las evaluaciones nacionales de riesgos y otras fuentes de información pertinentes. Además, adoptarán medidas técnicas y organizativas adecuadas y proporcionadas para garantizar su resiliencia y velarán por que estas medidas se describan en un plan de resiliencia o en un documento equivalente.

5.3.2.3. Medidas de resiliencia de las entidades críticas

Las entidades críticas tienen que definir y aplicar un plan de resiliencia o documentos equivalentes que describan detalladamente estas medidas. Cuando las hayan adoptado en virtud de las obligaciones contenidas en otros actos del Derecho de la Unión que también sean pertinentes para estas medidas, las describirán, asimismo, en dichos documentos.

Por otro lado, las entidades críticas han de notificar sin demora indebida a la autoridad competente los incidentes que perturben o puedan perturbar de forma significativa sus operaciones. Estas notificaciones incluirán toda la información disponible necesaria para que la autoridad competente pueda comprender la naturaleza, las causas y las posibles consecuencias del incidente, incluida la determinación de cualquier impacto transfronterizo. No obstante, dicha notificación no implicará un aumento de la responsabilidad de las entidades críticas.

5.3.3. Propuesta de Reglamento relativo a los requisitos horizontales de ciberseguridad para los productos

Esta Propuesta por el que se modifica el Reglamento (UE) 2019/1020 relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales establece lo siguiente: normas para la introducción en el mercado de productos con elementos digitales destinadas a garantizar la ciberseguridad de dichos productos; requisitos esenciales para el diseño, el desarrollo y la fabricación de productos con elementos digitales y las obligaciones de los operadores económicos en relación con dichos productos respecto de la ciberseguridad; requisitos esenciales para los procesos de gestión de las vulnerabilidades establecidos por los fabricantes para garantizar la ciberseguridad de los productos con elementos digitales a lo largo de todo el ciclo de vida y las obligaciones de los operadores económicos en relación con dichos procesos; y las normas relativas a la vigilancia del mercado y a la aplicación de los requisitos y las normas antes mencionados.

Se aplicará a todos los productos con elementos digitales cuyo uso previsto y razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red.

Los productos críticos con elementos digitales estarán sujetos a procedimientos específicos de evaluación de la conformidad y se dividirán en las clases I y II según lo establecido en el anexo III de la propuesta, dependiendo de su nivel de riesgo de ciberseguridad, conforme al que la clase II presenta un riesgo más elevado. Un producto con elementos digitales se considera crítico y, por tanto, se incluye en el ya mencionado anexo III considerando las repercusiones de las posibles vulnerabilidades de ciberseguridad presentes en el producto con elementos digitales. A la hora de determinar el riesgo de ciberseguridad se tienen en cuenta la funcionalidad del producto con elementos digitales relacionada con la ciberseguridad y el uso previsto del producto en entornos sensibles, como el industrial, entre otros.

La Comisión también estará facultada para adoptar actos delegados que completen este Reglamento mediante el establecimiento de categorías de productos altamente críticos con elementos digitales, a cuyos fabricantes se

les debe exigir la obtención de un Certificado Europeo de Ciberseguridad expedido en el marco de un esquema europeo de certificación de la ciberseguridad, a fin de demostrar la conformidad con los requisitos esenciales establecidos en el anexo I de la Propuesta de Reglamento o parte de ellos.

Para determinar estas categorías de productos altamente críticos con elementos digitales, la Comisión tendrá en cuenta el nivel de riesgo de ciberseguridad vinculado a cada categoría de productos con elementos digitales, a la luz de uno o varios de los criterios tomados en consideración para la inclusión de productos críticos con elementos digitales en el anexo III, así como de la evaluación que determine si dicha categoría de productos es utilizada por las entidades esenciales del tipo contemplado en el anexo I de la Directiva NIS 2, si sirve a estas entidades de referencia o si, en el futuro, podría desempeñar un papel importante para sus actividades; o bien, si resulta pertinente para la resiliencia de la cadena de suministro global de productos con elementos digitales frente a las perturbaciones.

5.3.3.1. Obligaciones de los operadores económicos

Los requisitos y obligaciones esenciales de ciberseguridad exigen que los productos con elementos digitales solo se comercialicen si, habiendo sido suministrados debidamente, instalados de manera adecuada y mantenidos y utilizados para los fines previstos o en condiciones de uso que se puedan prever razonablemente, cumplen los requisitos esenciales de ciberseguridad establecidos en este Reglamento.

Los requisitos y obligaciones esenciales impondrían a los fabricantes a tener en cuenta la ciberseguridad en el diseño, el desarrollo y la producción de los productos con elementos digitales a actuar con la diligencia debida en lo que respecta a la seguridad al diseñar y desarrollar sus productos. Pero también a ser transparentes respecto a los aspectos relativos a la ciberseguridad que deban ponerse en conocimiento de los clientes, a garantizar el apoyo en materia de seguridad (actualizaciones) de manera proporcionada y a cumplir los requisitos relacionados con la gestión de las vulnerabilidades.

Se establecerían también obligaciones para los operadores económicos, desde los fabricantes hasta los distribuidores y los importadores, relativas a la introducción en el mercado de productos con elementos digitales, proporcionalmente a su papel y a sus responsabilidades en la cadena de suministro.

5.3.3.2. Conformidad del producto con elementos digitales

Se presupondrá que los productos con elementos digitales que sean conformes a normas armonizadas o partes de estas cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea son acordes con los requisitos esenciales del Reglamento propuesto. Cuando no existan normas armonizadas o éstas sean insuficientes, cuando se produzcan retrasos indebidos en el procedimiento de normalización o cuando la solicitud de la Comisión no haya sido aceptada por los organismos europeos de normalización, la propia Comisión podrá adoptar especificaciones comunes mediante actos de ejecución.

Además, se presumirá que los productos con elementos digitales que hayan sido certificados o para los que se haya expedido una declaración de conformidad de la Unión Europea o un certificado en el marco de un esquema europeo de certificación de la ciberseguridad establecido en virtud del Reglamento (UE) 2019/881 y para los cuales la Comisión haya especificado, mediante acto de ejecución, que puede otorgar la presunción de conformidad con el Reglamento propuesto, son conformes con los requisitos esenciales del presente Reglamento o con parte de éstos en la medida en que la declaración de conformidad de la Unión Europea o el certificado de ciberseguridad, o partes de éstos, contemplen dichos requisitos.

El fabricante llevará a cabo una evaluación de la conformidad del producto con elementos digitales y los procesos de gestión de las vulnerabilidades que haya establecido para demostrar la conformidad con los requisitos esenciales establecidos en el anexo I por medio de uno de los procedimientos establecidos en el anexo VI: los fabricantes de productos críticos de las clases I y II utilizarán los módulos respectivos necesarios para su cumplimiento; los fabricantes de productos críticos de la clase II deberán recurrir a un tercero para su evaluación de la conformidad.

5.4. Mejores prácticas de otros países

Durante la última década, distintos organismos y entidades, principalmente en Estados Unidos y Europa, han desarrollado estándares y buenas prácticas de aplicación a un entorno de automatización y digitalización industrial como el que encontramos en la distribución eléctrica. En la figura 13 se pueden apreciar las prácticas más

reconocidas y aceptadas actualmente. Para facilitar la identificación de los puntos fuertes de cada una de estas buenas prácticas, se han situado en un eje cuatro áreas: “diseño”, que contempla la incorporación de requisitos de ciberseguridad en los nuevos proyectos; “operación”, que incluye medidas para gestionar el riesgo en la operación y mantenimiento de la ciberseguridad en una infraestructura o instalación existente; “tecnología”, que aplicaría a adoptar medidas de ciberseguridad de implementación y configuración técnica; y “global”, que incluye estrategia, buen gobierno y compliance en ciberseguridad.

Estas buenas prácticas son las siguientes:

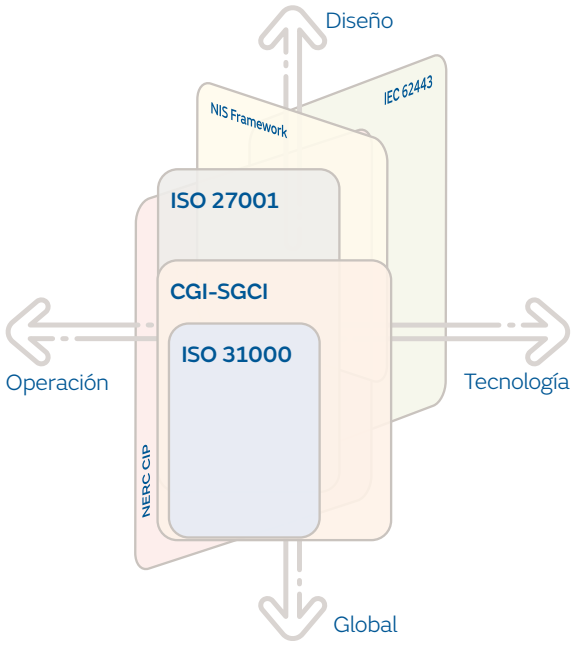
- Mejores Prácticas Operativas para NERC CIP BCSI. Estándares de protección de infraestructura crítica de la *North American Electric Reliability Corporation* (NERC CIP) para *BES Cyber System. Information (BCSI),* CIP-004-7 y CIP-011-3.

- Mejores Prácticas Operativas para NIST 800 171. Protección de información no clasificada controlada en sistemas y organizaciones no federales.

- Mejores Prácticas Operativas para NIST 172. Requisitos de seguridad mejorados para proteger información no clasificada controlada: un suplemento de la publicación especial NIST 800-171.

- Mejores Prácticas Operativas para NIST 800 181. *Workforce Framework for Cybersecurity* (Marco NICE).

Figura 13 | **Mejores prácticas**



- Mejores Prácticas Operativas para NIST 800-53 Rev 4. Controles de seguridad y privacidad para organizaciones y sistemas de información federales.
- Mejores Prácticas Operativas para NIST 800-53 Rev 5. Controles de seguridad y privacidad para sistemas de información y organizaciones.
- Mejores Prácticas Operativas para NIST 1800 25. Integridad de datos: identificación y protección de activos contra ransomware y otros eventos destructivos.
- Mejores Prácticas Operativas para NIST CSF. Marco de seguridad cibernética NIST.
- Sistema de Gestión de la Ciberseguridad Industrial del Centro de Ciberseguridad Industrial. Este documento incluye también los requisitos de los estándares ISO 27001 (controles ISO 27002) e IEC 62443, así como el modelo de madurez del CCI.
- IEC 62351. Gestión de sistemas de energía e intercambio de información asociada -Seguridad de datos y comunicaciones-. Todas las partes.
- IEC 62443-1-1 *"Models and Concepts"*.
- IEC TR 62443-1-2 *"Master Glossary of Terms and Abbreviations"*.
- IEC 62443-1-3 *"System Security Compliance Metrics"*. Define las métricas de cumplimiento para la seguridad en los sistemas de control y automatización industrial.
- IEC TR 62443-1-4 *"Security Life Cycle and Use Cases"*. Se centra en el ciclo de vida y en dar ejemplos de uso para aplicaciones típicas dentro de los sistemas de control.

- IEC 62443-2-1 *"Requirements for an IACS Security Management System"*.
- IEC TR62443-2-2 *"Operating a Control Systems Security Program"*.
- IEC TR 62443-2-3 *"Patch Management in the IACS Environment"*. Guía práctica para llevar a cabo un programa de gestión de actualizaciones desde el punto de vista tanto del propietario como del proveedor de soluciones.
- IEC 62443-2-4 *"Certification of IACS supplier security policies and practices"*. Se centra en la certificación de proveedores de productos de seguridad para los sistemas de control y automatización industrial.
- IEC TR62443-3-1 *"Security Technologies for IACS"*. Ofrece una descripción de tecnologías existentes para la protección de redes y sistemas industriales, exponiendo sus ventajas y limitaciones. Se encuentra en fase de revisión.
- IEC 62443-3-2 *"Security Risk Assessment and System Design"*.
- IEC 62443-3-3 *"System Security Requirements and Security Levels"*. Describe los requisitos técnicos del sistema para definir el nivel de seguridad del activo analizado.
- IEC 62443-4-1 *"Product Development Requirements"*. Define el proceso de desarrollo que tienen que llevar a cabo los nuevos dispositivos que se creen para los sistemas de control, aunque también puede ser aplicado a los dispositivos ya existentes.
- IEC 62443-4-2 *"Technical Security Requirements for IACS Components"*. Agrupa los requisitos técnicos para mejorar la seguridad de los componentes, de forma individual, dentro de la red industrial. También aborda la segmentación de la red para restringir los flujos de datos dentro de ella y entre redes.
- ISO/IEC 27001. Sistema de Gestión de la Seguridad de la Información.
- ISO 31000. Gestión del riesgo-directrices.
- CEN/CLC/JTC 13/WG 3. Estándar de evaluación de seguridad tecnológica GlobalPlatform para IoT Plataformas (SESIP) v1.0.
- Mejores Prácticas Operativas para el Marco de Evaluación Cibernética del NCSC. Controles del marco de evaluación cibernética del Centro Nacional de Seguridad Cibernética del Reino Unido.
- Mejores Prácticas Operativas para los principios de seguridad en la nube del Centro Nacional de Seguridad Cibernética del Reino Unido. Principios de Seguridad en la nube del Centro Nacional de Seguridad Cibernética.

6. La inversión en ciberseguridad del sector eléctrico

Combatir el aumento y sofisticación de los ataques que están sufriendo las infraestructuras críticas en general, y la distribución eléctrica en particular, requiere elevar el nivel de madurez en la cultura y gestión de la ciberseguridad en los entornos actuales y futuros de automatización y digitalización industrial.

Además, las regulaciones en materia de ciberseguridad, aunque procuran minimizar la carga financiera y administrativa, implican inversiones y gastos para gestionar este riesgo cada vez más importante. Estas inversiones están justificadas en la medida en que contribuirán a reforzar la resiliencia de los operadores y del sistema, incluyendo a los consumidores finales y su nueva manera de relacionarse con el mismo, así como a proporcionar un enfoque más coherente y a una mayor capacidad para prestar servicios fiables en toda la Unión. Asimismo, se espera que cualquier carga adicional derivada del cumplimiento normativo se vea ampliamente superado por los costes asociados de tener que gestionar y recuperarse de perturbaciones graves que pongan en peligro la prestación ininterrumpida de servicios relacionados con funciones sociales vitales.

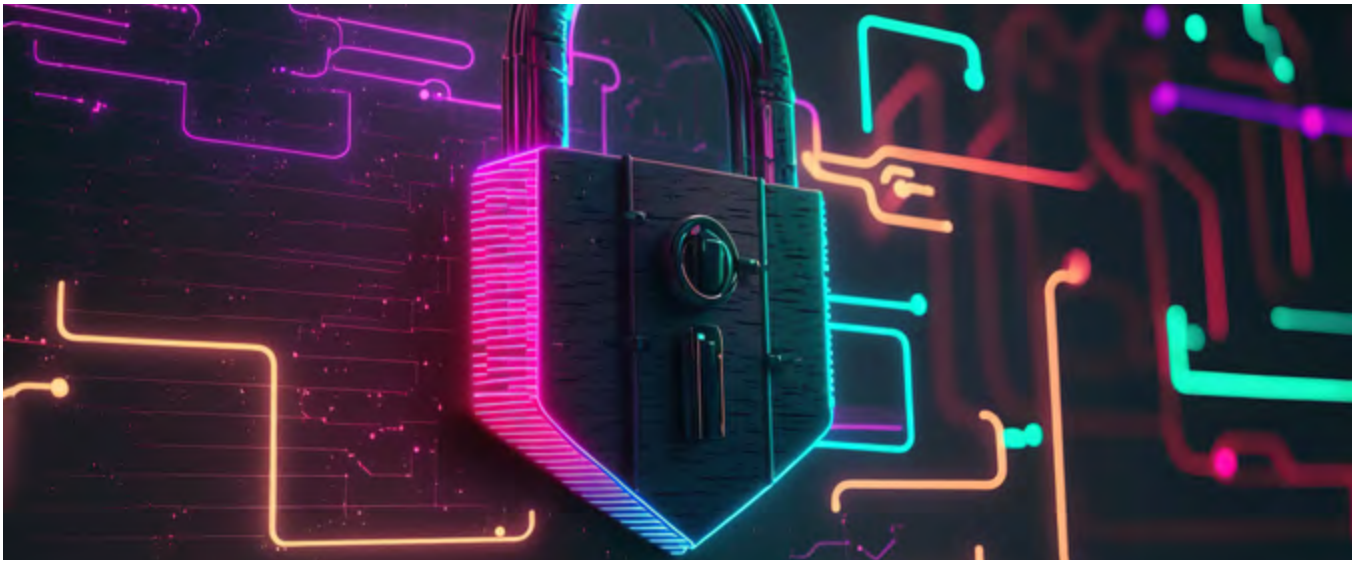
Ante este escenario de riesgo, se ha realizado una consulta a varios operadores del sector eléctrico europeo sobre la evolución que han tenido en la inversión y gasto en ciberseguridad. Algunos resultados interesantes son los que se muestran a continuación:

- El personal interno dedicado a la ciberseguridad se duplicó en los dos últimos años, mientras que los recursos externos aumentan, pero solo ligeramente.

- Hace dos años, los recursos de ciberseguridad se dedicaban al entorno corporativo en un 80%, respecto al 20% en el entorno de operación. Pero actualmente ha cambiado: ahora estaríamos en un 60% en corporativo y un 40% en operación. Esto se debe a los requisitos normativos y a los incidentes sufridos en estos últimos años.

- También se aprecia una evolución en la proporción de inversión (CAPEX) del 30% respecto al 70% de gasto (OPEX) hace dos años a un equilibrio del 50% entre CAPEX y OPEX.

Estos resultados evidencian el importante esfuerzo que se está realizando desde los operadores eléctricos para proteger la infraestructura de servicios esenciales cumpliendo con la regulación existente y futura. Pero este esfuerzo no será puntual: la digitalización del sector, y por tanto la mayor dependencia de la tecnología, como ya se ha indicado a lo largo del documento supondrá el incremento de recursos humanos y económicos para hacer frente a este riesgo.



Este aumento de la inversión en los recursos para proteger los servicios esenciales deberá también incluir la responsabilidad e inversión de la cadena de suministro.

La reorganización de las cadenas de suministro utilizando tecnologías avanzadas han sustituido el modelo lineal que va desde el proveedor al productor y del distribuidor al consumidor, y viceversa, a un modelo más integrado, no solo del modelo comercial de una empresa, sino también de su propio ecosistema tecnológico. Los proveedores tienen conexiones directas con las redes o sistemas de una empresa (incluidos los sistemas ERP (Enterprise Resource Planning o Planificación de Recursos Empresariales), sobre las aplicaciones de pedidos y facturación) y en algunos casos tienen acceso a datos corporativos o de operación propios. Asimismo, existen interconexiones similares entre los proveedores a lo largo de las cadenas de suministro.

Este escenario aumenta de forma significativa el perímetro a considerar por una distribuidora eléctrica, es decir, amplía las oportunidades para que un atacante pueda acceder a sus datos o al control de su operación, por ello es necesario además realizar evaluaciones de su relación contractual continuamente con los proveedores dentro de sus cadenas de suministro y comprobar que se realizan las inversiones necesarias también por ellos para aplicar las medidas de ciberseguridad.

> Estos resultados evidencian el importante esfuerzo que se está realizando desde los operadores eléctricos para proteger la infraestructura de servicios esenciales cumpliendo con la regulación existente y futura.

7. Conclusiones

La situación actual de riesgo de ciberseguridad, así como la evolución en los servicios demandados por los consumidores de electricidad, plantea múltiples desafíos en la distribución eléctrica que están impulsando acciones, normas y regulaciones sobre el sector a todos los niveles:

- El eléctrico es un sector en el que un ciberataque puede conllevar importantes implicaciones. No solamente por una potencial interrupción del suministro que afecte directamente a los consumidores, sino por las consecuencias que afectarían al resto de sectores. El sector eléctrico se enfrenta, por tanto, a ciberataques y amenazas de muy alto impacto potencial. Para combatirlo es necesario desarrollar una elevada madurez en todo lo relacionado con la cultura y la gestión de la ciberseguridad en el proceso del ciclo de vida de los proyectos de automatización y digitalización industrial con el objetivo final de minimizar los riesgos que generan dichas amenazas y garantizar los servicios esenciales a la sociedad.

- La evolución del consumidor final de electricidad hacia una categoría de prosumidor afecta, sin duda, a la gestión de la ciberseguridad de este sector. Los clientes, que también están en plena transformación digital, demandan información en tiempo real sobre sus consumos. Y esto supone una necesaria reorganización interna y una readaptación para que las empresas eléctricas pasen de ser un operador de servicios a un gestor de servicios.

- La creciente actividad de los ciberdelincuentes, unida a su cada vez más evidente profesionalización, hace que sea estrictamente necesario acometer importantes inversiones, a la vez que se intensifican las estrategias de concienciación y de formación del personal, los procedimientos de respuesta a incidentes y, sobre todo, la importancia de involucrar a todos los empleados de la organización en materia de ciberseguridad. Por tanto, las entidades eléctricas deben trabajar tanto en la tecnología como en los procedimientos como en las personas.

- La transformación en la distribución eléctrica conlleva necesariamente la implementación de una nueva cadena de suministro digital, la definición de nuevos roles, considerar las cada vez más evidentes interdependencias, la estandarización de las metodologías relacionadas con esta materia, la consolidación del cloud y la adopción del zero trust.

- Por tanto, a la hora de establecer un modelo para la nueva distribución eléctrica es por tanto necesario pensar, en materia de ciberseguridad, en la protección de toda la cadena de suministro desde el diseño y en cada una de las fases de la implementación de los nuevos proyectos, así como en las adaptaciones y renovaciones necesarias.

- Las organizaciones del sector eléctrico ya llevan tiempo implantando una serie de mecanismos de protección con el objetivo de estar lo menos expuestas posible a la actividad de los ciberdelincuentes. Algunos de ellos son contar con una segmentación y una defensa en profundidad, realizar un seguimiento de cualquier cambio en las configuraciones de los dispositivos, controlar los accesos y privilegios, evaluar y gestionar las vulnerabilidades, monitorizar todos los aspectos relacionados con la seguridad y garantizar la continuidad del servicio y la seguridad de las personas, el medio ambiente y los equipos.

- Todo lo anterior conlleva que el sector eléctrico, como consecuencia de su categorización como servicio esencial, se enfrenta a una vorágine de normativa de ciberseguridad. Sobre todo, con la publicación por parte del Boletín Oficial de la Unión Europea, a finales del año pasado, de la conocida como la Directiva NIS 2 y de la Directiva sobre resiliencia de las entidades críticas.

- Estas nuevas regulaciones a nivel europeo implican una mayor inversión a la hora de gestionar los riesgos de ciberseguridad. Sin duda estas partidas están totalmente justificadas puesto que reforzarán la protección, detección, respuesta y recuperación de las organizaciones ante una eventual amenaza. Es más, el coste relacionado con la gestión y restablecimiento tras un ciberataque será mayor a cualquier carga adicional derivada del cumplimiento normativo. Y, por lo tanto, deben ser adecuadamente reconocidas tanto en lo que respecta a la inversión, como a los costes operativos resultado de una evolución tecnológica continua.

> Se plantean múltiples desafíos en la distribución eléctrica que están impulsando acciones, normas y regulaciones sobre el sector a todos los niveles.

8. Referencias

1. Boston Consulting Group. *Embracing Industry 4.0 and Rediscovering Growth.* Disponible en: https://www.bcg.com/capabilities/operations/embracing-industry-4.0-rediscovering-growth

2. J. Julian Claveria y A. Kalam. *GOOSE Protocol: IED's Smart Solution for Victoria University Zone Substation (VUZS) Simulator Based on IEC61850 Standard.* Disponible en: (PDF) *GOOSE Protocol: IED's Smart Solution for Victoria University Zone Substation (VUZS) Simulator Based on IEC61850 Standard* (researchgate.net)

3. J. Andress and S. Winterfeld. *Cyber Warfare, Second Edition: Techniques, Tactics and Tools for Security Practitioners. Syngress; 2nd edition, 2011.*

4. A. D. Campen. *Uncommon Means for the Common Defens, in Cyberwar: Strategy and Conflict in the Information Age (A. D. Campen, D. H. Dearth, and R. T. Goodden, eds.). Páginas 71-75. Fairfax, Virginia: AFCEA International Press, 1996.*

5. G. Disterer. ISO/IEC 27000, 27001 and 27002 *for Information Security Management. Journal of Information Security,* nº 4. Páginas 92-100, 2013

6. Tecnología de la información. Técnicas de Seguridad. Controles de Seguridad de la información para la industria de servicios de energía (ISO/IEC 27019:2017, versión corregida 2019-08) (Ratificada por la Asociación Española de Normalización en mayo de 2020).

7. National Institute of Standards and Technology. Marco para la mejora de la seguridad cibernética en infraestructuras críticas, tech. rep., NIST, 2018.

8. Pillitteri, V. and Brewer, T. (2014). *Guidelines for Smart Grid Cybersecurity, NIST Interagency/Internal Report (NISTIR). National Institute of Standards and Technology, Gaithersburg, MD.* Disponible en: https://doi.org/10.6028/NIST.IR.7628r1 (fecha de consulta: 9 de diciembre de 2022).

9. Centro de Ciberseguridad Industrial. Estableciendo Zonas y Conductos, 2018

10. *U.S. Department of Energy's, Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid,* octubre de 2022.

11. *World Economic Forum - Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards. 2019.*

12. *DOE. Roadmap for Wind Cybersecurity. 2020.*

13. Centro de Ciberseguridad Industrial. Guía de Ciberseguridad en el Ciclo de Vida de un proyecto de digitalización industrial. 2021.

Centro de
Ciberseguridad Industrial

Fundación
Naturgy