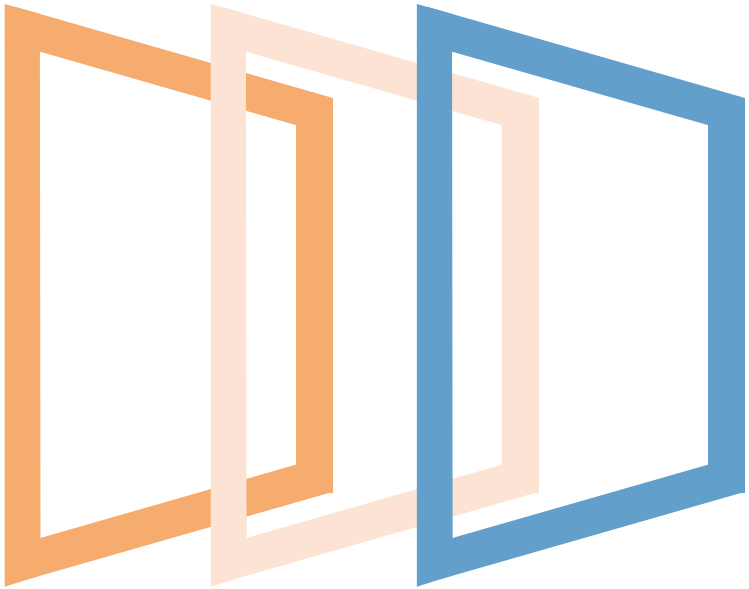
Análisis y hoja de ruta para diseñar la normativa española y europea sobre ciberseguridad en entorno eólico



ENERCLUSTER

minsait

An Indra company

Índice

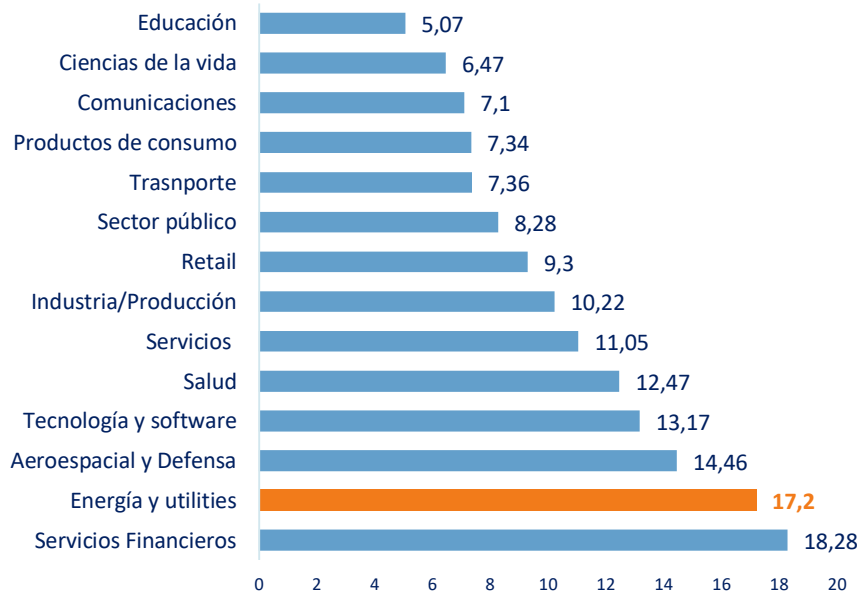
Marco de referencia

01

- Punto de partida: datos y escenarios posibles
- Vulnerabilidades e impacto
- Casos de ciberataques a nivel mundial

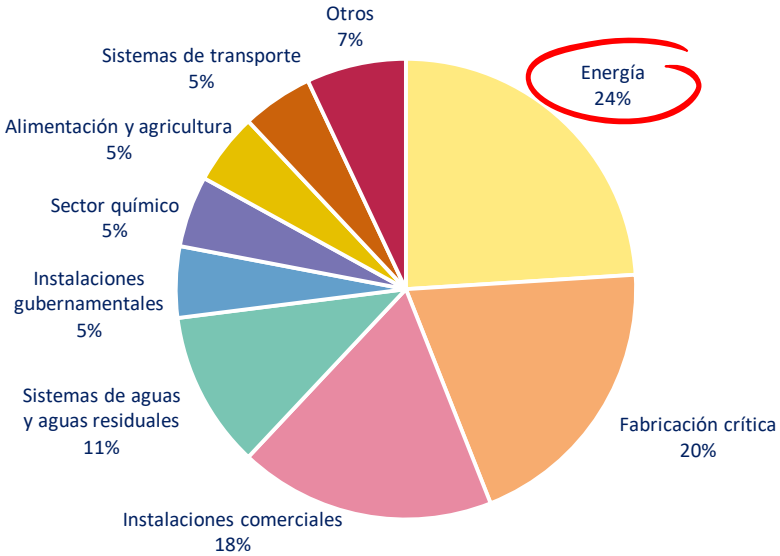
El sector energético es especialmente vulnerable en materia de ciberseguridad: los ciberataques cuestan un promedio de $17,2 M de pérdidas anuales en dicho sector en 2017

Costes anuales globales provocados por ciberataques (2017, $M*)



*Coste medio por organización/empresa objetivo

2016 ICS-CERT*: número de incidentes por sector



*US Homeland Industrial Control Systems Cyber Emergency Response Team

Año a año, el sector de la energía es uno de los principales receptores (1° o 2° lugar) de incidentes relacionados con la ciberseguridad de sus instalaciones y equipos según el informe de vulnerabilidad ICS-CERT

Fuente: Accenture & Ponemon Institute 2017
ICS-CERT Annual Vulnerability Coordination Report 2017

La creciente dependencia de la energía eólica hace que los sistemas de control de parques eólicos sean objetivos atractivos para los atacantes

¿Porqué ciberseguridad para las renovables?

- Las energías renovables se están convirtiendo en la nueva fuente dominante de electricidad
- Las penetraciones más altas de DER requieren una mayor administración de la utilidad para mantener la confiabilidad de la red
- Una mayor administración requiere una mejor conectividad del sistema y protocolos de comunicación comunes
- El aumento de la conectividad multiplica la cantidad de plataformas de ataque cibernético
- La red es una infraestructura crítica que requiere una gran seguridad y enfrenta una mayor regulación
- Los propietarios de sistemas renovables enfrentan un mayor riesgo de pérdida de ingresos y más requisitos de cumplimiento

Consecuencias de ciberataques en el sector energético

- Pérdida de producción e ingresos
- Pérdida de datos / IP
- Lesión al personal o espectadores
- Daño del equipo
- Daño reputacional
- Costo de la reparación
- Inestabilidad e interrupciones en la red
- Multas reglamentarias

Existen diferentes normas y organismos reguladores en función de las características de los equipos a los que se pretende proteger

Escenarios de ciberseguridad en energías renovables

Proyectos a gran escala

Conectado a la transmisión de alto voltaje

- **Regulado por:** NERC y Utilidades
- **Grupos de interés:** propietarios de plantas, proveedores de O & M, OEM
- **Vulnerabilidades clave:** SCADA, RTU, turbinas e inversores

Distribuido C & I y Residencial

Conectado al sistema de distribución

- **Regulado por:** State PUCs, utilities
- **Stakeholders:** integradores, servicios públicos, OEM, propietarios
- **Vulnerabilidades clave:** SCADA, Inversores

Productos de supply chain

Múltiples dispositivos integrales a sistemas conectados a la red

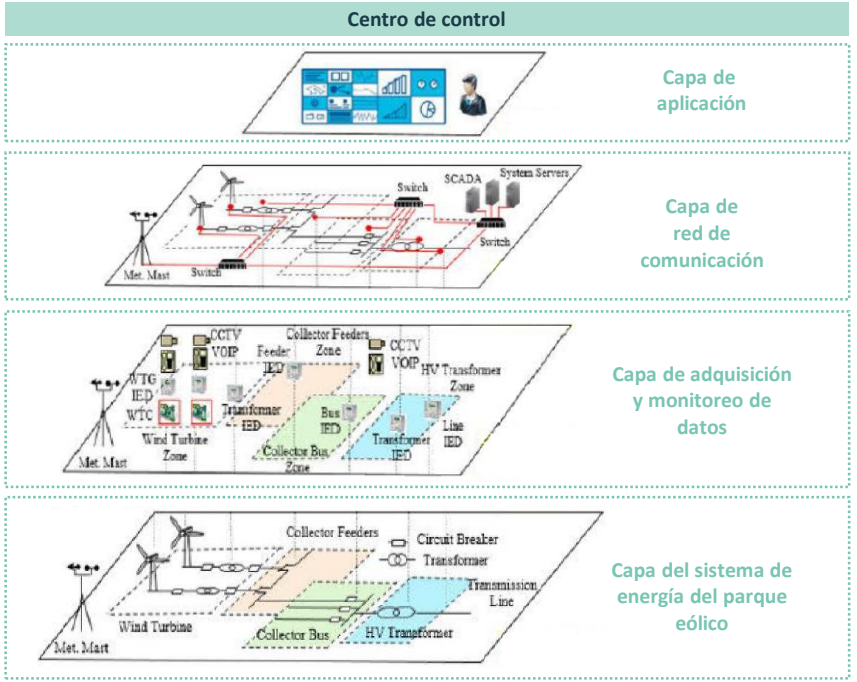
- **Regulado por:** AHJs, servicios públicos, agregación de OEM
- **Stakeholders:** OEMs, Desarrolladores / Instaladores
- **Vulnerabilidades clave:** tecnologías conectadas integradas

Es importante que las operadoras eléctricas fuercen la implementación de los estándares establecidos tanto en los dispositivos como en el proceso, es decir, que la normativa se implemente en toda la cadena de valor

Las vulnerabilidades en un parque eólico se concentran principalmente en aspectos relacionados con el software de los centros de control y el cifrado de mensajes de control

Principales vulnerabilidades en parques eólicos

- **Redes múltiples:** potencia, controles, datos
- **Puntos clave de acceso**
  - Centro(s) de control
  - SCADA y RTU
  - Turbinas individuales
  - Dispositivos y software integrados
  - Nuevas tecnologías industriales de IoT
  - Acceso de proveedor remoto
- **Seguridad física débil en sitios remotos**
- **Entidades conectadas (remotas)**
  - Centro de control del propietario, proveedor de O&M, OEM, utilities
  - Falta de armonización de seguridad
- **Falta de segmentación de red entre aerogeneradores**
- **Ausencia de autenticación o cifrado de mensajes de control**
- **Controladores de automatización programables (PAC) que ejecutan sistemas operativos heredados**
- **Uso de servicios de administración remota inseguros**
- **Contraseñas predeterminadas fáciles de descifrar y sin firma de código**



Fuente: Ahmed & Kim, 2017, Applied Sciences

"Los controladores no cifran todos sus mensajes, a veces usan contraseñas predeterminadas y no separan las redes, de modo que si un hacker se toma el control de una turbina, podría gobernarlas a todas" - Jason Staggs, investigador de la University of Tulsa

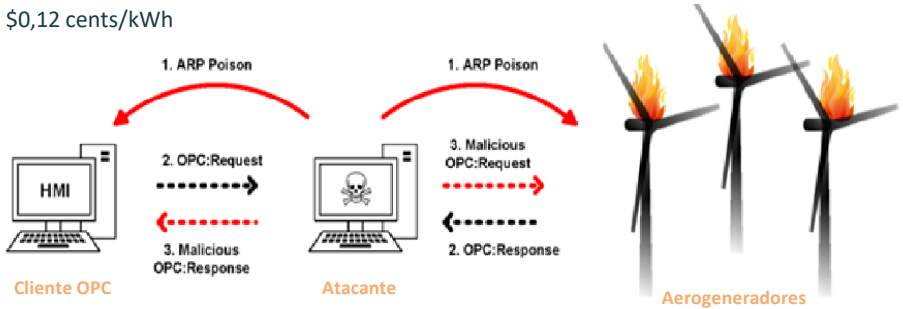
Según las tasas actuales, un parque eólico estándar puede perder desde $10.000 hasta $30.000 por cada hora que no esté en operación

Impacto financiero potencial debido al tiempo de inactividad en un parque eólico

Ejemplo de posibles pérdidas en un parque eólico

Suponemos:

- 167 turbinas x 1,5 MW cada una ≈ parque eólico de 250 MW
- 100% de dependencia de la energía eólica (sin otras fuentes renovables)
- Factor de capacidad del 35% (peor caso)
- **Generación en 1 año**: 250 MW × 365 días × 24 horas × 35% = 766,5 GWh = 766.500 MWh = 766.500.000 kWh
- ≈ $0,12 cents/kWh



Tiempo de inactividad (horas)	Costo acumulado del tiempo de inactividad en un parque eólico estándar
1	~ **$10.500** (35% de capacidad) - **$30.000** (capacidad max.)
8	~ **$84.000 - $240.000**
24 (1 día)	~ **$252.000 - $720.000**
48 (2 días)	~ **$504.000 - $1.440.000**
72 (3 días)	~ **$756.000 - $2.160.000**
168 (1 semana)	~ **$1.764.000 - $5.040.000**
336 (2 semanas)	~ **$3.528.000 - $10.080.000**
672 (1 mes)	~ **$7.056.000 - $20,160,000**
2.016 (3 meses)	~ **$21.168.000 - $60.480.000**

Fuente: BlackHat USA 2017

Según Jason Staggs, investigador de la University of Tulsa, inhabilitar un parque eólico por un día podría suponer al proveedor de energía hasta $700.000 de pérdidas

En 2013 la empresa eólica Nordex sufrió un fallo en uno de sus productos de control de supervisión y adquisición de datos/interfaz hombre-máquina (SCADA/HMI)…

2013: Vulnerabilidad de scripts de sitios de Nordex en un producto SCADA / HMI

- El **Nordex NC2** es un portal de control para turbinas eólicas fabricadas por la compañía, que permite a un usuario controlar la configuración y las operaciones de los aerogeneradores de forma remota y recibir datos e informes sobre ellos
- El ICS-CERT* advirtió a los usuarios sobre una vulnerabilidad de scripts entre sitios reflejada en una interfaz de control para un portal de control de parques eólicos fabricado
- El error era remotamente explotable y podía permitir a un atacante ejecutar código en uno de los equipos vulnerables

*Industrial Control Systems Cyber Emergency Response Team

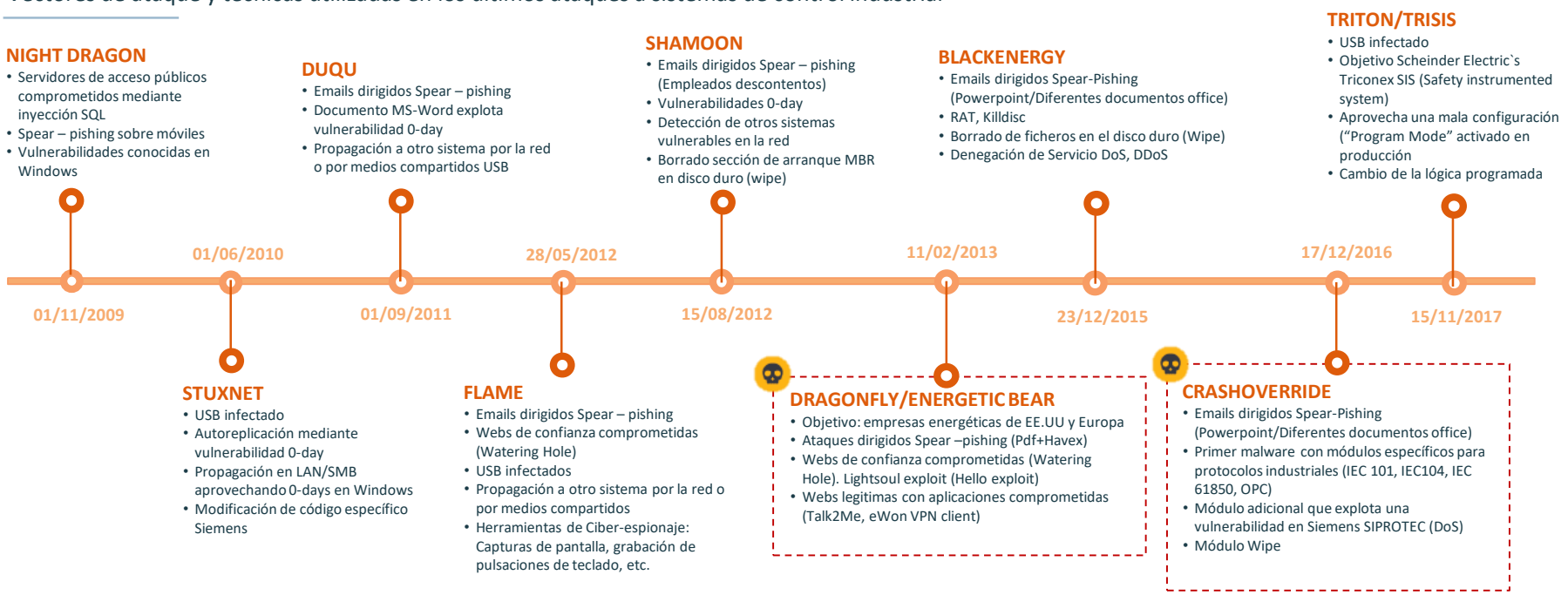
Otros incidentes

- **2018:** El Departamento de Seguridad Nacional de los EE.UU. informa que los actores patrocinados por el estado se dirigen a los sistemas de control industrial relacionados con la energía
- **2017:** El gobierno de EE.UU. emitió una advertencia de ataques de malware (Dragonfly 2.0) contra la industria nuclear y energética; > 12 plantas de energía
- **2017:** Investigador holandés descubrió 17 vulnerabilidades del **inversor solar**
- **2015: Incidente de la red eléctrica de Ucrania**
  - 3 subestaciones perdieron energía por ataque cibernético
  - 225.000 clientes afectados durante horas
  - Primer registro público de corte de energía por ataque cibernético
- **2013:** El grupo de pirateo **DragonFly** infectó a varias compañías de energía renovable en Europa y comprometió los sistemas de control industrial
- **2013:** Vulnerabilidad de scripting entre sitios de Nordex en un producto SCADA / HMI
- **2011-13:** Piratas informáticos iraníes obtuvieron el control de la **presa** en Rye, Nueva York a través de un cable módem
- **2008:** La CIA confirmó un ataque en **Nueva Orleans** que provocó cortes de energía en varias ciudades

…pudiendo ser victima de un ciberataque que no solo encriptase los datos sino que paralizase las operaciones de sus parques eólicos de tal manera que no pudiesen producir electricidad

Detrás de la mayoría de los ciberataques contra infraestructuras críticas suele haber una amenaza persistente avanzada, conocida por sus siglas en inglés APT (Advanced Persistent Threat)

Vectores de ataque y técnicas utilizadas en los últimos ataques a sistemas de control industrial

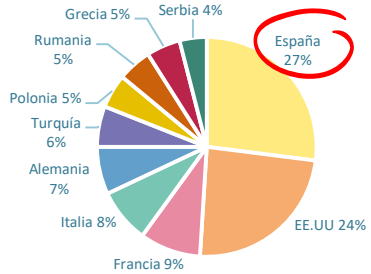


Durante el año 2015, los APT BlackEnergy y CrashOverride tenían como objetivo a la industria eléctrica de Europa del Este y Norteamérica; su principal factor en común era que pretendían conseguir una denegación de servicio en la industria infectada mediante sabotaje

Ciberataques en sistemas eléctricos a nivel mundial: de 2014 a 2017

2014

Ciberataque masivo contra empresas energéticas de Europa y EEUU: España es el país más afectado



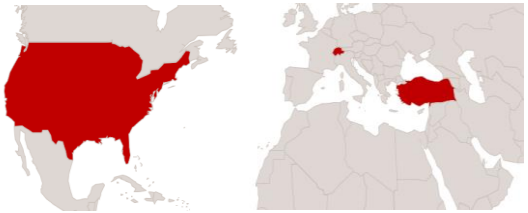
Top 10 países afectados

- Más de un millar de instalaciones energéticas de Europa y Estados Unidos sufrieron un ciberataque masivo
- España fue el país más afectado por la acción, concentrando un 27% del total de equipos infectados por un sofisticado virus informático

- Los sistemas de control de instalaciones (plantas de generación eléctrica, gasoductos, aerogeneradores, los contadores de consumo en tiempo real...) de centenares de compañías europeas y estadounidenses fueron las afectadas
- El ciberataque sólo sirvió para realizar **espionaje industrial**, pero si los atacantes hubieran utilizado la capacidad de sabotaje de la que disponían (gracias al malware empleado) podrían haber causado **daños o interrupciones del suministro de energía** en los países afectados

2017

El resurgimiento en los ataques del sector energético, con potencial de sabotaje en infraestructuras eléctricas de Europa y EE.UU.



Países afectados:

- EE.UU
- Suiza
- Turquía

Motivos:

- Recogida de información
- Sabotaje

- El grupo **DragonFly** llevó a cabo campañas de correo electrónico malintencionadas durante 2016 y en 2017: los correos electrónicos contenían contenido muy específico relacionado con el sector de la energía, así como algunos relacionados con inquietudes comerciales generales
- Cisco escribió en su blog sobre ataques basados en correo electrónico dirigidos al sector energético utilizando un kit de herramientas llamado **Phishery**
- En contraposición a las campañas originales de Dragonfly, los ataques más recientes parecen haber pasado a una fase más exploratoria, ya que las campañas actuales pueden proporcionarles acceso a sistemas operativos, acceso que podría usarse para propósitos más disruptivos en el futuro

Los principales objetivos de este tipo de ataques son operadores de redes energéticas, grandes grupos de generación eléctrica, operadores de oleoductos y proveedores de equipos industriales para el sector de la energía

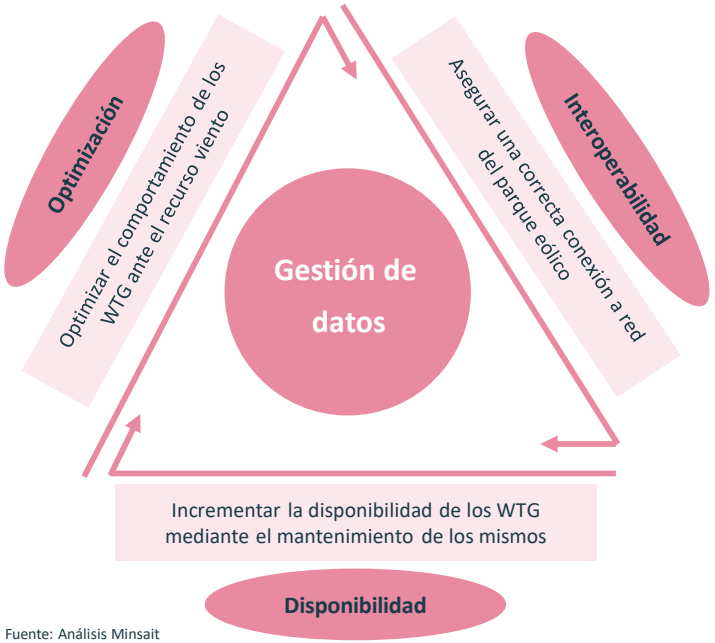
Infraestructura de las redes en parques eólicos

02

- Sistema de control de un parque eólico: funciones y objetivos
- Red de control de operaciones

El objetivo prioritario del sistema de control de un parque eólico radica en contribuir a la rentabilidad del parque, maximizando la captura de la energía eólica…

Sistema de control: objetivos y funciones



Fuente: Análisis Minsait

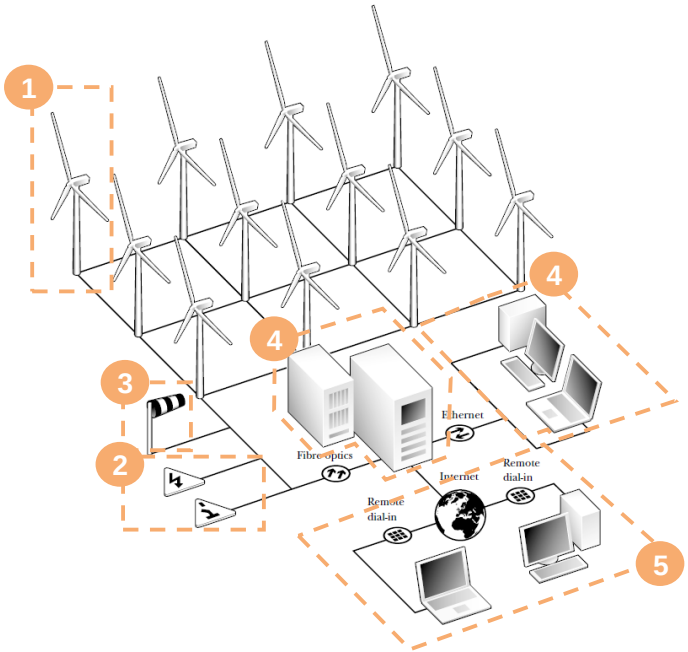
Funciones

- Anticipar con mayor precisión los patrones de viento, aumentando así la disponibilidad de los recursos
- Minimizar los costes de explotación y mantenimiento mediante el diagnóstico predictivo de fallos de comportamiento
- Gestionar de forma remota la producción de las turbinas de manera adecuada para maximizar la producción
- Asegurar la adecuada conexión de los sistemas a la red, equilibrando la producción eléctrica e impidiendo la falta o exceso de producción y capacitando el bloqueo de la red para impedir que un exceso de electricidad pueda sobrecargar el sistema
- Flexibilidad: Permitir el uso de turbinas de diferentes fabricantes
- Manejar de forma eficaz elevados volúmenes de datos:
  - Interacción con sistemas adicionales, por ejemplo, la previsión del tiempo
  - Control en tiempo real de energía activa y reactiva de todo el parque eólico
  - Realizar y presentar cálculos de disponibilidad y productividad

… y supervisando el comportamiento de las diferentes WTG que componen el parque en su conjunto

El sistema de control actúa como el sistema central que integra los diferentes sistemas de telemando empleados…

Sistema de control: objetivos y funciones



Fuente: Análisis Minsait

Sistema de control del aerogenerador

1	Controlador principal	• Controlador central encargado de la operación de toda la turbina (curva de potencia, sistema pitch …)
	Turbine Condition Monitoring	• Sistema independiente respecto del controlador central responsable del control de fallos en la turbina
	Convertidor de potencia	• **Controlador del convertidor de potencia cuyo objetivo es la regulación de todos los parámetros de conexión a la red del parque**

Sistema de control del parque eólico

2	Estación meteorológica	• **Sistema de recopilación y predicción de datos meteorológicos de interés para la operación del parque**
3	Sistema SCADA	• **Sistema de gestión del parque que aglutina todos los sistemas y componentes del mismo permitiendo las actividades de O&M**
4	Subestación eléctrica	• **Sistema de control en tiempo real de los sistemas de conexión del parque a red eléctrica (potencia activa y reactiva, picos de tensión…)**
5	Control integral de parques	• **Sistema encargado del control y conexión a red de varios parques eólicos de un mismo operador**

Áreas de interés para medidas de ciberseguridad

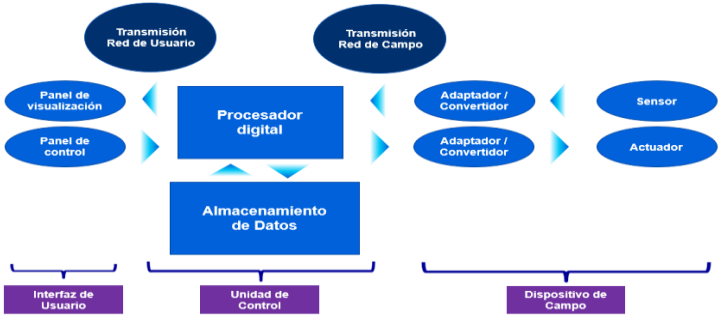
… conectando los controladores de las WTG, la subestación eléctrica y la estación meteorológica con el control central y optimizando su funcionamiento

3 En la actualidad, el control y gestión de los parques eólicos se realiza mediante un sistema de control y monitorización SCADA…

Definición y descripción

- SCADA (Supervisory Control And Data Acquisition): registro de datos y control de supervisión
- Es un sistema de control industrial (aplicación software) que sirve para supervisar y medir el proceso, monitorizando los resultados para los operarios, con la finalidad de controlar y corregir el funcionamiento del parque

Esquema SCADA



Funciones

	Características
Herramientas de operación y supervisión del parque eólico	• Visualización y control operativo de datos en tiempo real • Visualización de datos y diseño de pantalla personalizados • Resúmenes y alarmas de funcionamiento • Herramientas de diagnóstico y reparación para una rápida resolución de averías
Histórico de bases de datos y presentación de informes	• Base de datos histórica SQL, estándar de la industria y exportación de datos del informe a otros • Altamente flexible y preconfigurado • Sistema de información basado en la Web
Otros	• Soporte UPS • Interfaces estándar (OPC, ODBC) • Interfaz de predicción de viento

Fuente: Análisis Minsait

… el cual permite a los operarios supervisar y corregir el funcionamiento del parque en tiempo real, aumentando la utilización del mismo

3 Los sistemas SCADA están formados por unidades MTU y RTU que se comunican a través de buses de comunicación …

			Componentes / Subsistemas	Descripción
HARDWARE	MTU (Master Terminal Unit)	CPU	Módulo CPU Principal	Microprocesador principal con HMI y entradas I/O
			Unidad Asíncrona de serie	Enlaces asíncronos de serie V.24 / V.28
			Unidad Convertidora de Energía	Diferentes voltajes: 48 Vdc, 24, 110, 125, 220, 250, etc.
			Simulador I/O	Simula y monitoriza inputs y outputs
	RTU (Remote Terminal Unit)	Entradas y salidas I/O	Unidad Digital de Entrada	Inputs digitales a 24 Vdc, 48, 110, 125, 220, etc.
			Unidad Digital de Salida	Outputs digitales
			Unidad de Conversión de Analógico a Digital	Mediante aproximación sucesiva de al menos 120 por segundo
			Unidad Analógica de Entrada	Inputs analógicos
			Unidad Analógica de Salida	Outputs analógicos
			Rack con entradas de conexión I/O	Rack de al menos 21 ranuras y conector DIN
		Comunicaciones	Redes Industriales	Sistema de red que transfiere datos (bus de campo, LAN, LAN/WAN)
SOFTWARE			Gestor de Comunicaciones	Adquisición de los datos de los sensores
			Módulo de bases de datos e históricos	Gestiona la base de datos
			Módulo de sinópticos de pantalla	Permite visualizar esquemas y datos representados
			Módulo de gestión de alarmas	Permite visualizar alarmas y mensajes
			Módulo de edición de históricos	Consulta el registro de cada sensor (permite editarlo)

Fuente: Análisis Minsait

… registrando las RTUs las señales del proceso, que son enviadas a la MTU para su posterior análisis y generación de señales de control

3 La MTU incorpora los convertidores de energía y los simuladores, junto con el módulo de CPU principal…

Descripción

- La CPU interpreta las instrucciones y procesa los datos contenidos en los programas del sistema. En el caso de los parques eólicos off-shore, es el encargado de enviar los algoritmos de control preconfigurados

Componentes

1	**Módulo CPU Principal**	• Microprocesador principal con batería de litio • Interfaz bus con bus de direcciones (24 bits) y bus de datos (16 bits) • Con temporizador y posibilidad de autoarranque
2	**Unidad Asíncrona de Serie**	• Enlaces asíncronos de serie V.24 / V.28 • Señales: TD, RD, RTS, CTS, DCD, DSR y DTR • Normas y certificados: IEC 950
3	**Unidad Convertidora de Energía**	• Voltajes de entrada: 48 Vdc, 24 Vdc, 110 Vdc, 125 Vdc, 220 Vdc, 250 Vdc, etc. • Voltaje de salida para el bus: 5V y 12V • Una por cada rack o RTU
4	**Simulador I/O**	• Panel de control para simular entradas y salidas • Visualiza y simula entradas y salidas tanto analógicas como digitales • Potenciado mediante fuente externa: 24 Vdc, 48 Vdc, 125 Vdc, etc.

Algoritmos de control

- Permiten mitigar las fluctuaciones de potencia mediante la inercia de la turbina de viento del rotor, como un componente de almacenamiento de energía
- Ajustan la velocidad del rotor para que, cuando la energía eólica sea superior a la media, el rotor pueda acelerar almacenando el exceso de energía de modo cinético

Certificaciones

- Normativa IEC 61131 - 3
- Protocolo IEC 61850 y IEC 61400 – 25
- Normativa EN 600068–2–6 / EN 60068-2-27/29
- Normativa EN 61000-6-2 / EN 61000-6-4 / EN 61000-1-9

1


2


3


4


Fuente: Análisis Minsait

… y los módulos de entradas y salidas que se conectan en un rack destinado a alojar equipamiento electrónico y de comunicaciones

3 En el caso de las RTUs, la mayoría de los fabricantes optan por la utilización de sistemas basados en PLCs…

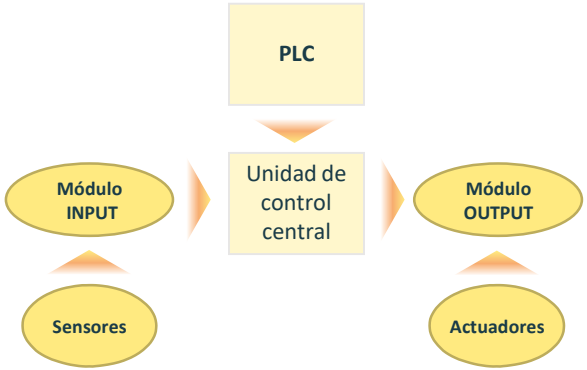
Descripción PLC



Descripción

- Es un ordenador digital que sirve para la automatización de procesos electromecánicos
- Se adjuntan a las RTU´s (Remote Terminal Unit) dispuestas en los puntos de control de los diferentes sistemas para enviar la información a la MTU (Master Remote Unit) Así, los operarios pueden supervisar el sistema y enviar algoritmos de control
- Vienen diseñados para entradas y salidas múltiples, con un intervalo amplio para los cambios de temperatura, inmunes al ruido eléctrico y resistentes al impacto y a la vibración

Proceso



Principales suministradores

- ABB
- GE Fanuc
- Mitsubishi Electric
- Moeller
- OMROM
- Schneider Electric
- Siemens

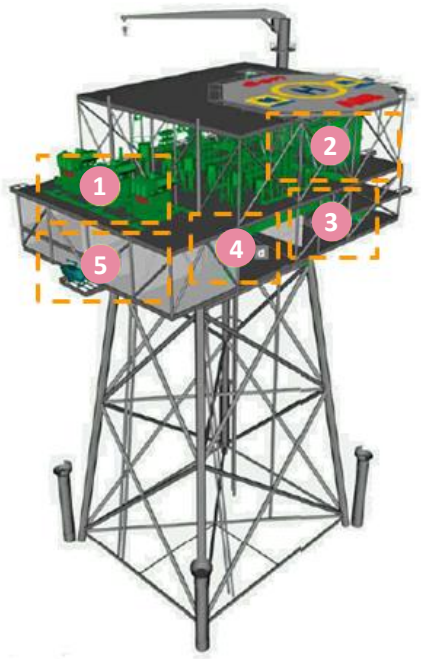
Certificaciones

- **Normativa IEC 61131 - 3**
- **Protocolo IEC 61850 y IEC 61400 – 25**
- **Normativa EN 600068–2–6 / EN 60068-2-27/29**
- **Normativa EN 61000-6-2 / EN 61000-6-4 / EN 61000-1-9**
- **IEC 61131 Lenguajes de programación**

Fuente: Análisis Minsait

…siendo suministrados, en la mayoría de los casos, por los grandes fabricantes internacionales como ABB, GE Fanuc, Siemens

4 La subestación eléctrica está formada por áreas de alimentación y de conversión, todas ellas supervisadas por un sistema SCADA



Fuente: Análisis Minsait

Componentes Subestación

1. **Área de alimentación AC**
2. **Convertidores**
3. **Válvulas HVDC**
4. **Área de alimentación DC**
5. **Sistema de refrigeración**

SCADA

- **Mediante PLC´s y MTU´s**
- **Informes y gráficos avanzados**
  - Curva de potencia
  - Pérdidas de producción
  - Disponibilidad

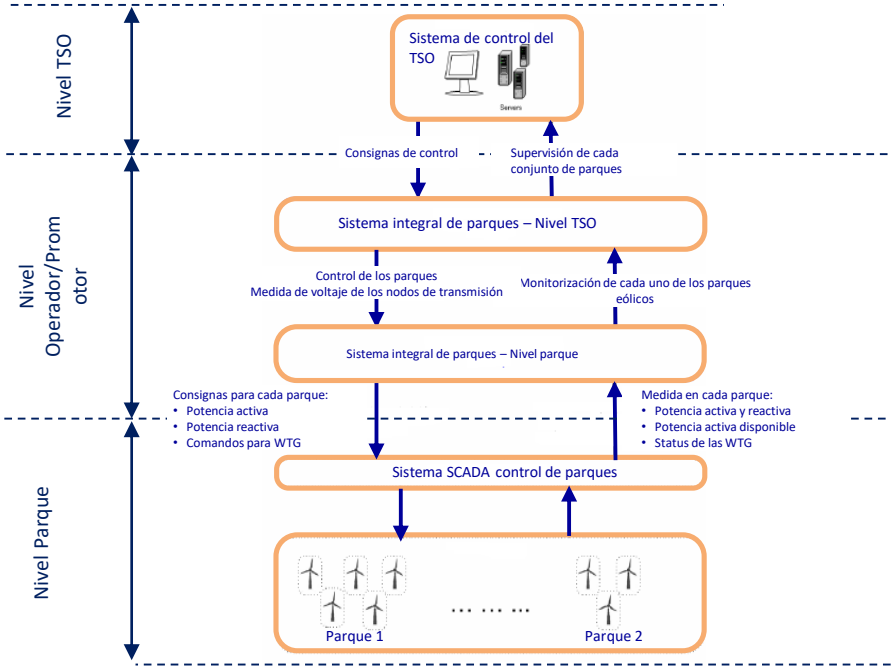
Automatización de la subestación eléctrica

Generación, transmisión y automatización de la alimentación	• Control automático del voltaje / tensión • Detección de fallo de interruptores • Sincronismo • Indicador de posición de llave / manivela
Automatización de la distribución de energía	• Transferencia de buses de carga y descarga • Reducción de la carga • Algoritmo de control de distribución
Aplicaciones avanzadas de seguimiento / monitoreo de AC	• Alarmas de dispositivos AC • Dispositivo de grabación digital de errores • Calidad de la potencia
Servicios de comunicación	• Terminal virtual • Nodo de mantenimiento de la subestación
Otras aplicaciones	• Registro y almacenamiento de datos • Resumen y reducción de datos • Conversión de formatos

Estos SCADA son implementados, en su parte hardware, por sistemas PLC y módulos de I/O similares a los empleados en las WTG desarrollados por los principales fabricantes como ABB, Siemens o Areva T&D

5 El sistema de gestión integral permite a los operadores la integración completa de todos los activos de generación eólica…

Arquitectura del sistema



Nota: TSO – Transmission System Operator – Operador de red eléctrica
Fuente: Análisis Minsait

Modo de operación

- El sistema se estructura en dos capas de aplicación, el nivel TSO y el nivel parque. EL TSO se responsabiliza principalmente de los aspectos de seguridad en red y el nivel parque interactúa entre el nivel TSO y sus clientes (los parques)
- Durante el funcionamiento normal del sistema, el TSO envía consignas de control a los operadores de los parques. Siguiendo estas consignas, los sistemas de gestión integral de parques controlan sus respectivos parques de acuerdo con las señales de control recibidas. Al mismo tiempo, la información de supervisión es enviada desde los parques al sistema de gestión, y de éste al TSO.
- El TSO debe recibir toda la información relacionada con la generación de electricidad con el objeto de poder realizar predicciones de potencia y ocupación para los diferentes parques (potencia activa, reactiva…)
- El flujo de información es el siguiente:
  - La consigna de control se envía desde el nivel TSO al nivel parque en función de los parámetros TSO
  - Dicha consigna incluye parámetros de seguridad de red proporcionados por los TSO. De acuerdo a esos parámetros el sistema de gestión calcula las consignas de control respecto a la potencia activa y reactiva, así como el voltaje
  - El nivel parque envía dichas consignas y monitoriza el comportamiento del parque de acuerdo a los parámetros enviados

…favoreciendo la optimización de los recursos disponibles y un mayor control de las actividades de operación y mantenimiento

5 La incorporación del parque eólico a la red eléctrica se realiza mediante la ejecución de un software de control que gestiona todos los requisitos de conexión a dicha red

Funciones del sistema

- Supervisión de un parque igual que si estuviera conectado en local, es decir la monitorización del parque en tiempo real
- Recogida eventual de datos históricos, estadísticos, alarmas y eventos
- Cargar la aplicación de control en las WTG
- Modificar parámetros de control individuales en los aerogeneradores
- Ejecutar comandos: parar, arrancar, reponer máquina
- Generar informes de supervisión y control
- Suministrar información a otras aplicaciones
- Comunicarse con los operadores de red, enviar datos solicitados y recibir consignas de control
- Asegurar la correcta conexión de los diferentes parques eólicos a la red eléctrica

Certificaciones y normativas

- IEC 61850. Communication networks and systems in substations
- IEC 61850_7_410. Renewables power plants - Communication for monitoring and control
- IEC 61850_7_420. Communications Systems for Distributed Energy Resources (DER)
- IEC 61400_25. Communications for monitoring and control of wind power plants
- IEC 60870-5-101/104 y DNP3 – protocolos de comunicación con PLC y RTUs

Principales parámetros del sistema

Huecos de Tensión	• Permite amortiguar los picos de corriente y soportar de forma directa las elevadas corrientes del hueco • Reduce el riesgo de disminuir la producción en periodos críticos de baja demanda (no hay discontinuidad en el control) • Comportamiento equivalente a máquina de generación síncrona
Regulación Potencia Reactiva	• El PLC controla todas las variables implicadas en la generación de potencia reactiva • Nunca supera las condiciones límite establecidas para cada aerogenerador • Decide el valor máximo que puede generar en cada momento dependiendo de la potencia activa que esté produciendo
Regulación Potencia-Frecuencia	• Algoritmo instalado en cada aerogenerador (opcional) para que el controlador pueda establecer una referencia de potencia en base a unos valores parametrizados y de la lectura individual
Regulación Potencia Activa	• Permite la regulación y limitación de potencia activa del parque • Maximiza la producción y contribuye a la estabilidad de la red • Control individual de las turbinas
Comunicación SCADA y señales	• Posibilidad de enviar y recibir señales entre el parque eólico y el operador del sistema
Regulación de Tensión	• Se debe actuar sobre la potencia reactiva del parque para mantener la tensión en el punto de conexión sobre un valor de referencia fijado

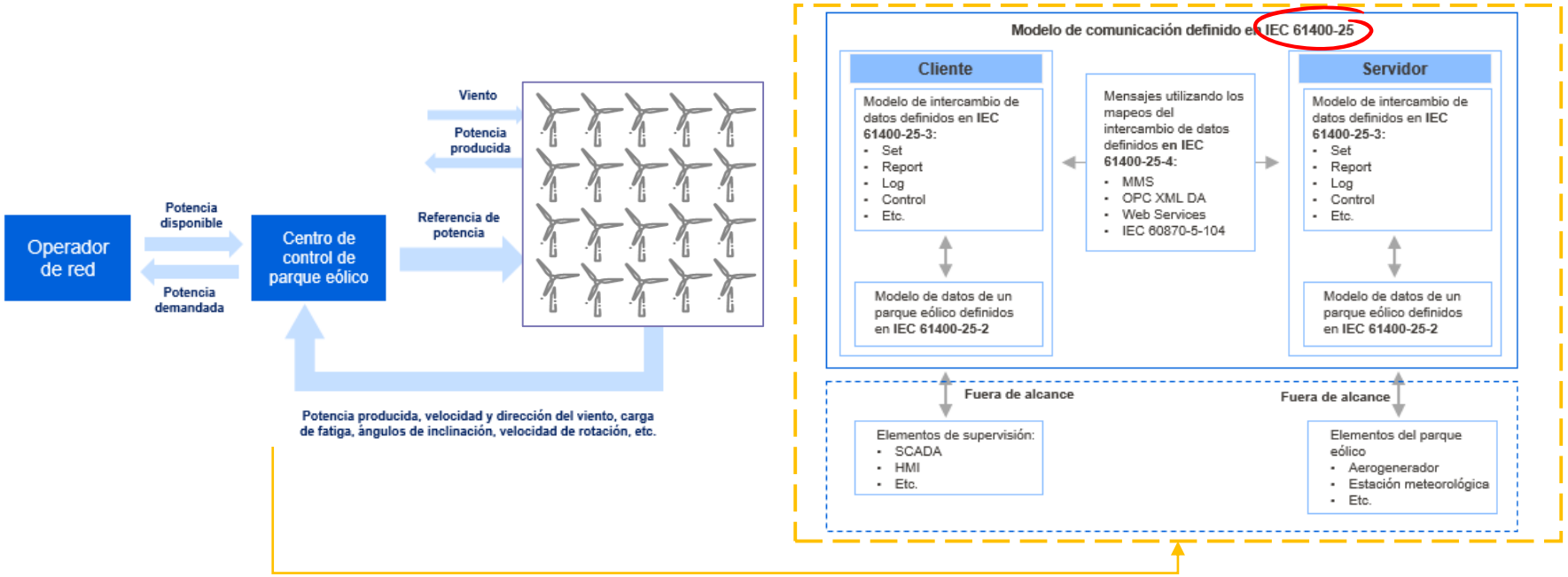
Fuente: Análisis Minsait

Infraestructura de las redes en parques eólicos

02

- Sistema de control de un parque eólico: funciones y objetivos
- Red de control de operaciones

La serie IEC 61400-25 solo define cómo modelar la información, el intercambio de información y la asignación a protocolos de comunicación específicos

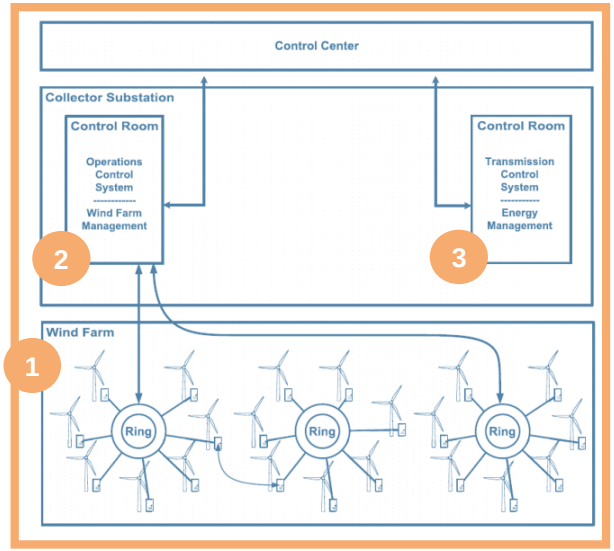


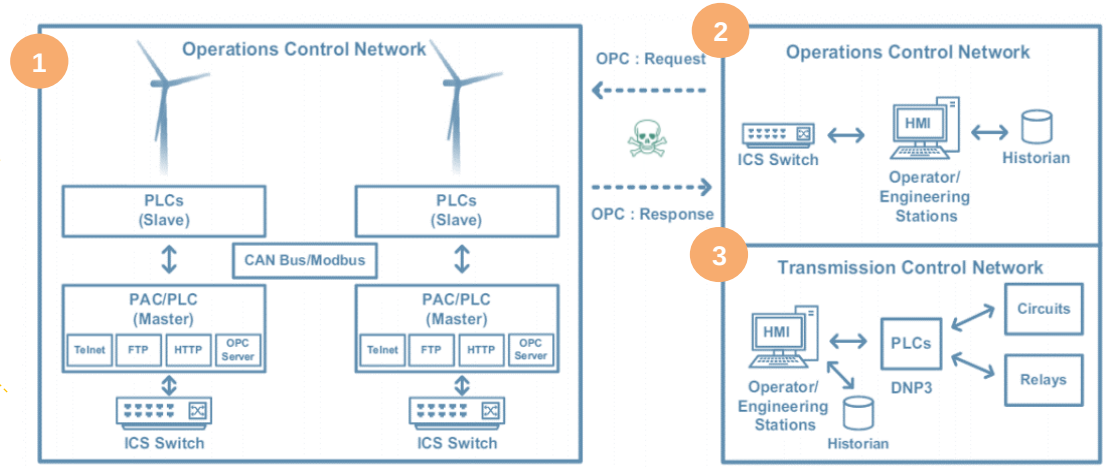
Fuente: Análisis Minsait

La serie IEC 61400-25 excluye la definición de cómo y dónde implementar la interfaz de comunicación, la interfaz del programa de aplicación y las recomendaciones de implementación

Si un atacante ingresara a la red, podría provocar un ataque al interceptar una solicitud de OPC desde el HMI hasta las turbinas para crear una solicitud maliciosa

Red de control de operaciones de parques eólicos





La intromisión de un hacker en la red podría suponer el cambio de la producción máxima de generación de energía, la modificación del estado de funcionamiento de la turbina eólica (encendido, apagado o inactivo), o incluso un apagado de emergencia

Normativas y estándares regulatorios

03

- Estándares regulatorios y voluntarios enfocados en Norteamérica
- Estándares regulatorios y voluntarios enfocados en Europa
- Estándares regulatorios y voluntarios de aplicación internacional

Cuadro resumen de los estándares por región y tipo de actividad (IT, eléctrico/energía e industrial)

		IT	Eléctrico/ Energía	Industrial
 Norteamérica	• **NERC–CIP:** Protección contra Infraestructuras Críticas		4	
	• **NIST** Framework for Improving Critical Infrastructure Cybersecurity	4	4	4
 Europa	• Plataforma de Ciberseguridad Experta en Energía (**EECSP**)	4	4	
	• **GDPR** – General Data Protection Regulation	4	4	
	• Directiva sobre la seguridad de las redes y los sistemas de información (**NIS**)	4	4	
Internacional	• **IEC 61400-25**: Communications for Monitoring & Control of Wind Plants	4	4	
	• **IEC 61850:** Communication Networks and Systems in Substations	4	4	
	• **ISO/IEC TR 27019** - Process control systems used by the energy utility industry	4	4	
	• **ISA/IEC 62443** - Industrial Automation & Control Systems Security			4
	• **IECRE:** Sistema IEC para la certificación de estándares (Energía Renovables)		4	
	• **ISO/IEC 15408-1**: Information technology - Security techniques	4		

Nota: (España: LPIC – Protección de Infraestructuras Críticas)
(Alemania: BDEW – German Association of Energy and Water Industries)

La necesidad de estándares de seguridad cibernética y mejores prácticas que aborden la interoperabilidad, la usabilidad y la privacidad continúa siendo crítica…

Ejemplos de estándares regulatorios y voluntarios

Enfocado en América del Norte

1. **NERC–CIP -001 to -009: Bulk Electrical System (>75 MW; >100 kVa)**
2. **NIST Framework for Improving Critical Infrastructure Cybersecurity (also NIST 800- 53 for Federal Info Systems/Orgs and 800-82 for ICS Security)**
3. **Energy Sector Cybersecurity Framework Implementation Guidance (January 2015, U.S DOE)**
- 2017 Presidential Executive Order on Strengthening the CS of Federal Networks & Critical Infrastructure
- Canada National Electric Grid Security & Resilience Action Plan - 2016
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) – US Dept. of Homeland Security
- UL 2900: Software Cybersecurity for Network-Connectable Products
- IEC 61400-25: Communications for Monitoring & Control of Wind Plants
- IEC 61850: Communication Networks and Systems in Substations
- CA Rule 21 & HI 14H: Interconnection for DER; references to UL 1741 SA
- SunSpec Alliance: DER Cybersecurity workgroup

Fuente: UL Transaction Security

…para un sector como el energético en el que NIST (Instituto Nacional de Estándares y Tecnología), IEC (International Electrotechnical Commission) y NERC (Corporación Americana para la Seguridad Eléctrica) son los principales organismos certificadores a nivel global

1 North American Electric Reliability Corporation (NERC) es una autoridad reguladora cuyo propósito es salvaguardar la confiabilidad de los sistemas de energía a granel norteamericanos

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

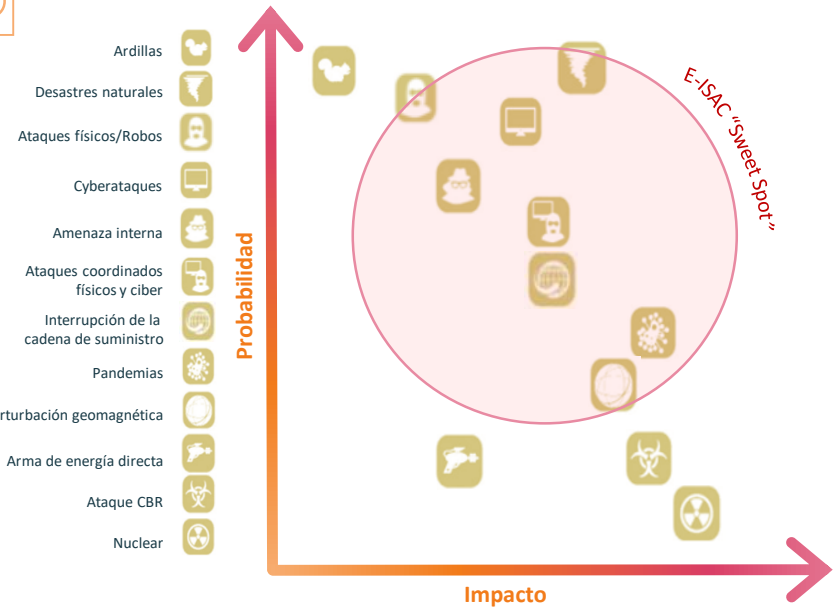
Centro de intercambio y análisis de información sobre electricidad

- NERC desarrolla estándares de **resiliencia y seguridad para los sistemas de control y automatización eléctricos** en Norteamérica; estos estándares son impulsados por la propia industria y acreditados por la ANSI
- El **Centro de análisis e intercambio de información sobre la electricidad (E-ISAC)** reúne y analiza datos de seguridad, comparte datos apropiados con las partes interesadas, coordina la gestión de incidentes y comunica las estrategias de mitigación con las partes interesadas

Productos y servicios ofrecidos por E-ISAC

- Portal seguro que admite la colaboración en un entorno de equipo virtual
- Análisis de datos
- Informes diarios y semanales centrados en analistas
- Informes mensuales y anuales centrados en el liderazgo
- Boletines cibernéticos
- Boletines físicos
- Informes de evaluación sobre temas específicos
- Acciones intersectoriales
- Informes de vulnerabilidad
- Seminarios web mensuales
- Ejercicio bienal de seguridad de la red (GridEx)
- Conferencia anual de seguridad de la red (GridSecCon)
- Programa de Intercambio de Información de Riesgo de Ciberseguridad (CRISP)

Amenazas dirigidas a la red eléctrica



Fuente: E-ISAC Long-Term Strategic Plan

El E-ISAC sirve como el principal canal de comunicaciones de seguridad para la industria eléctrica y mejora la capacidad de la industria para prepararse y responder a las amenazas cibernéticas y físicas, vulnerabilidades e incidentes

1 NERC CIP constituye un conjunto de estándares de ciberseguridad, de obligado cumplimiento, para compañías relacionadas con el subsector eléctrico de la alta tensión en EEUU

¿Qué protege NERC?

Sistema eléctrico a granel
- Plantas de generación
- Estaciones de transmisión
- Líneas de transmisión
- Torres de transmisión

Activos Críticos
- Plantas de generación
- Estaciones de transmisión
- Centros de control

Activos cibernéticos
- Sistemas de control de supervisión y adquisición de datos (SCADA)
- Sistemas de gestión de energía (EMS)
- Sistemas de control distribuido de planta (DCS)

Estándares NERC-CIP

- **CIP-002:** Identificación de activos cibernéticos
- **CIP-003:** Controles en la gestión de la seguridad
- **CIP-004:** Personal y formación/capacitación
- **CIP-005**: Perímetros de seguridad electrónica (ESP)
- **CIP-006:** Perímetros de seguridad física (PSP)
- **CIP-007:** Gestión de seguridad de sistemas
- **CIP-008:** Informes de incidentes y planificación de respuesta
- **CIP-009:** Plan para la recuperación de activos cibernéticos de carácter crítico
- **CIP-010:** Gestión del cambio de configuración y vulnerabilidad
- **CIP-011:** Protección de la información
- **CIP-014:** Seguridad física

EE.UU. México (Baja California) Canadá

- Los Estados Unidos de América, Canadá y una parte de Baja California en México **están bajo la responsabilidad** de NERC. Los operadores de sistemas de energía en esa región deben cumplir con sus estándares de seguridad que incluyen el escaneo de red en busca de vulnerabilidades de seguridad
- Las **sanciones por incumplimiento** con NERC CIP pueden incluir multas, sanciones u otras acciones contra entidades cubiertas. Como NERC es una organización transnacional, las sanciones varían de un país a otro

En 2006 la comisión federal para la regulación de la energía en los Estados Unidos (FERC), en calidad de representante del Gobierno, encargó a la NERC la tarea de desarrollar dichos estándares

1 NERC CIP establece una serie de normas que conforman un marco de ciberseguridad para la protección de activos cibernéticos críticos

Requisitos y normas exigidos por el plan NERC CIP

Identificación de activos cibernéticos críticos

Controles de gestión de seguridad

Personal y Entrenamiento

Perímetro de seguridad electrónica

Seguridad física de activos cibernéticos

Gestión de seguridad de sistemas

Informe de incidentes y planificación de respuesta

Planes de recuperación de activos críticos

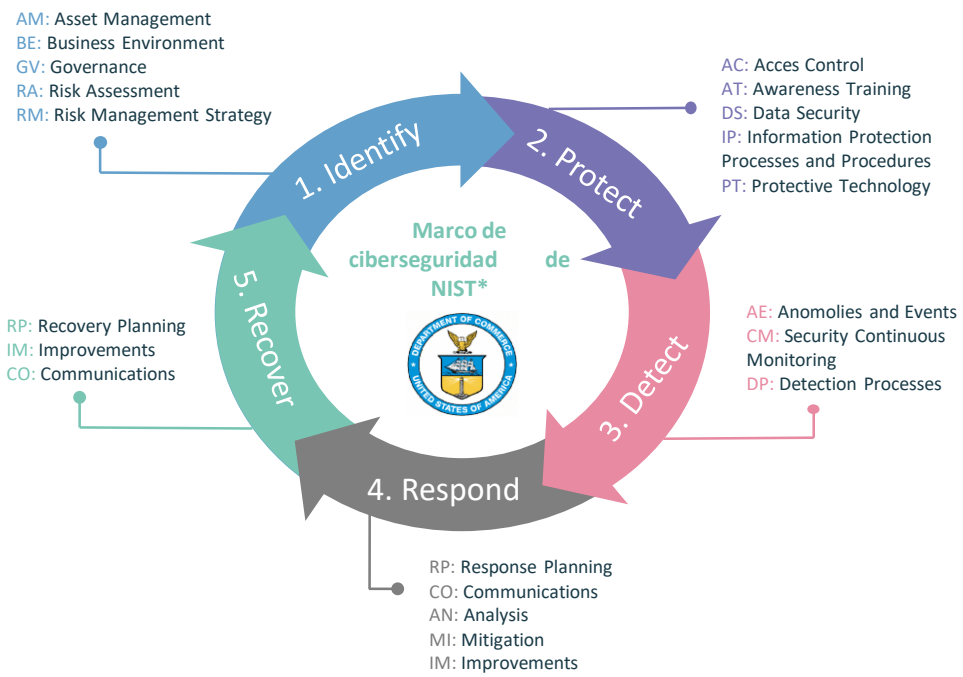
- Implementado por Entidades Regionales
- Obligatorio y exigible
- Auditorías de cumplimiento y controles al azar
- Riesgo de Sanciones
- Criterios de bajo, medio, alto impacto
- Actividades trimestrales y anuales
- Establece requisitos mínimos

Con activos cibernéticos nos referimos a aquellos dispositivos que utilizan un protocolo enrutable o son de acceso telefónico y que controlan o afectan al sistema eléctrico a granel

2 El Marco de ciberseguridad desarrollado por NIST es adoptado voluntariamente por empresas de todos los sectores de la industria, así como por los gobiernos federales, estatales y locales

Pautas para el establecimiento de un sólido programa de seguridad

- **Crear una empresa de seguridad totalmente integrada** con una sólida estructura de gestión
- **Mantener monitoreo continuo de estado de seguridad**, administración de parches de software y actualización de herramientas
- **Incluir controles cibernéticos de la cadena de suministro** para componentes, software, adquisiciones y acceso remoto del proveedor
- **Administrar incidentes, informes y recuperación**, y colabore sobre lecciones aprendidas y mejores prácticas
- **No olvidar la seguridad física** (CCTV, acceso controlado, alarmas de puerta, detección de intrusos)
- **Obtener asesoramiento de seguridad independiente**, detección, pruebas y servicios de capacitación de expertos



*National Institute of Standards and Technology (U.S. Department of Commerce)

El Instituto Nacional de Estándares y Tecnología (NIST) ha publicado recientemente una nueva versión de su Marco de Ciberseguridad enfocándose en las industrias vitales para la seguridad del país, incluida la energía, la banca, las comunicaciones y la base industrial de defensa

2 El NIST cuenta con el Computer Security Resource Center, proveedor de recursos sobre seguridad de la información y de guías y estándares tanto para el gobierno como para la industria

La Guía para la Seguridad de los Sistemas de Control Industrial (ICS)

- Las medidas de protección utilizadas en las áreas de IT (antivirus, Firewall, IDS…) están diseñadas para una infraestructura de IT "de negocio" pero no son útiles para un entorno de operaciones industriales (OT, por las siglas en inglés de *Operational Technology*)
- La **última actualización de la guía del NIST** adapta los controles de seguridad IT para establecer una **convergencia** entre ambos entornos: **IT/OT**

Actividades actuales en la Seguridad de los Sistemas de Control Industrial

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

- El ICS-CERT opera dentro del **Centro Nacional de Ciberseguridad e Integración (NCCIC)**
- ICS-CERT coordina incidentes de seguridad relacionados con **sistemas de control** e **intercambio de información** con agencias y organizaciones federales, estatales y locales, la comunidad de inteligencia y los constituyentes del sector privado, incluidos proveedores, propietarios y operadores
- Como componente funcional del NCCIC, el ICS-CERT proporciona capacidades operacionales enfocadas para la **defensa de los entornos del sistema de control** contra amenazas cibernéticas emergentes
- El **enfoque** en **sistemas de control de ciberseguridad** proporciona un camino directo para la coordinación de actividades para todos los miembros de la comunidad

ISA99 Industrial Automation and Control Systems Security Standards

- El comité de desarrollo de normas ISA99 reúne a expertos en ciberseguridad industrial de todo el mundo para **desarrollar estándares ISA** sobre seguridad del **sistema de control y automatización industrial** (IACS)
- El trabajo ISA99 está siendo estandarizado por IEC en la producción de la serie multi-estándar **IEC 62443**
- Todos los estándares ISA-62443 están organizados en 4 categorías generales: General, Políticas y Procedimientos, Sistema and Componentes
- El objetivo del comité es mejorar la confidencialidad, la integridad y la disponibilidad de los componentes o sistemas utilizados para la automatización o el control, y proporciona criterios para la **adquisición** e **implementación de sistemas de control seguros**

National SCADA Test Bed (NSTB)

- **El Banco Nacional de Pruebas de Control y Adquisición de Datos (SCADA)** es un recurso patrocinado por la Oficina del DOE de Entrega de Electricidad y Fiabilidad Energética (OE) para **ayudar a asegurar los sistemas de control de energía** de EE.UU.
- Combina lo último en instalaciones de pruebas de sistemas operacionales con investigación, desarrollo y capacitación para descubrir y abordar las vulnerabilidades de seguridad críticas y las amenazas al sector de la energía. El NSTN busca:
  - Identificar y mitigar las vulnerabilidades existentes
  - Facilitar el desarrollo de estándares de seguridad
  - Servir como una entidad independiente para probar los sistemas SCADA y las tecnologías relacionadas del sistema de control
  - Identificar y promover mejores prácticas de ciberseguridad
  - Incrementar la conciencia sobre la seguridad de los sistemas de control dentro del sector de la energía

La última versión de la Guía publicada por NIST incluye una nueva visión sobre como ajustar los controles de seguridad IT tradicionales para adaptarlos a los requisitos de rendimiento, fiabilidad y seguridad de los sistemas industriales (ICS)

2 Las iniciativas relacionadas con la Ciberseguridad Industrial, suelen carecer del componente regulatorio que caracteriza a las iniciativas de Protección de Infraestructuras Críticas…

Iniciativas realizadas en materia de Ciberseguridad Industrial

Modelo de madurez de capacidades en ciberseguridad del sector eléctrico

Denominado **ES-C2M2** (Electricity Subsector Cybersecurity Capability Maturity Model), permite la evaluación de las capacidades de seguridad de una organización, facilitándole la priorización de sus inversiones en seguridad.

Proceso de Gestión de Riesgos de Ciberseguridad (Cybersecurity Risk Management Process)

Es una guía desarrollada en colaboración con el **NIST** (National Institute of Standards and Technology) y **NERC** (North American Reliability Corporation) cuyo objetivo es facilitar a las organizaciones, sin importar su tamaño o estructura, la aplicación de procesos eficientes, y adaptados a su entorno, para la gestión del riesgo. La guía puede utilizarse para implantar nuevos programas de seguridad o complementar las políticas, procedimientos y guías existentes en la organización.

Programa de ciberseguridad para sistemas de distribución energética (Cybersecurity For Energy Delivery Systems Program)

El objetivo de este programa es ayudar a los propietarios de activos del sector energético (electricidad, petróleo y gas) mediante el **desarrollo de soluciones de ciberseguridad** adecuadas para este entorno. Las actividades de este programa se encuadran en las siguientes áreas:

- Construcción de una cultura de ciberseguridad
- Análisis y Monitorización del riesgo
- Desarrollo e implantación de nuevas medidas de protección para reducir el riesgo
- Gestión de incidentes
- Sostenimiento de mejoras en seguridad

ENERGYSEC
SECURING CRITICAL INFRASTRUCTURE

- EnergySec es otra de las organizaciones más involucradas en el desarrollo de iniciativas de ciberseguridad Industrial
- Se trata de una organización sin ánimo de lucro cuyo objetivo es ayudar a las empresas del sector eléctrico a mejorar la seguridad de sus infraestructuras tecnológicas
- Esta labor la logran principalmente mediante servicios de asesoramiento, formación y concienciación

NTSB
An Independent United States Federal Government Agency

- El NSTB es un programa promovido por el Departamento de Energía de EE.UU. cuyo objetivo es mejorar la seguridad de los sistemas SCADA y diseñar sistemas de control más resistentes
- Esto lo consigue mediante el análisis de sistemas de control en busca de ciber-vulnerabilidades, la realización de cursos y talleres formativos sobre mecanismos de mitigación de vulnerabilidad en sistemas de control y la participación en conferencias mediante las que comparten el conocimiento obtenido a través de sus actividades

…esto supone que las iniciativas de Ciberseguridad Industrial tengan un carácter más universal y sus efectos no se restrinjan a una zona geográfica o política determinada, pudiendo ser aprovechadas por toda la comunidad tanto del ámbito industrial como del de la ciberseguridad

3 El Marco de Ciberseguridad del Sector de la Energía define herramientas y procesos de seguridad cibernética específicamente para su uso en el sector de la energía

- En enero de 2015, la colaboración entre el Departamento de Energía de EE. UU. (DOE) y las industrias de electricidad, petróleo y gas produjo la **Guía de Implementación del Marco de Ciberseguridad del Sector de la Energía**, que define herramientas y procesos de seguridad cibernética específicamente para su uso en el sector de la energía
- En la Guía se recomienda el **Modelo de Madurez de la Seguridad Cibernética del Subsector de Electricidad (ES-C2M2)**, desarrollado para abordar las características únicas del sector eléctrico y que ayuda a las organizaciones eléctricas de todo tipo a evaluar y realizar mejoras en sus programas de seguridad cibernética

Visión general del ES-C2M2

- **Desafío:** desarrollar capacidades para gestionar amenazas dinámicas y comprender la postura de ciberseguridad de la red
- **Enfoque:** desarrollar un modelo de madurez y una encuesta de autoevaluación para desarrollar y medir las capacidades de ciberseguridad
- **Resultados:** un modelo escalable, específico del sector, creado en asociación con la industria

Objetivos del ES-C2M2

- **Fortalecer las capacidades de ciberseguridad**
- Permitir la **evaluación comparativa** de las capacidades de ciberseguridad
- **Compartir conocimientos** y mejores prácticas
- Habilitar acciones **priorizadas** e inversiones en ciberseguridad

Fuente: Cyber Security Strategy for the Energy Sector

La Ley de protección de las redes cibernéticas y la Ley de promoción de la protección de la seguridad cibernética nacional son dos leyes aprobadas también en 2015 y destinadas a mejorar el intercambio de información entre el sector privado y las agencias gubernamentales

3 La Guía de Implementación del Marco de Ciberseguridad del Sector de la Energía proporciona una amplia cobertura de los dominios de ciberseguridad y gestión de riesgos

Prácticas y estándares asociados a la categoría de control de acceso remoto

Función	Categoría	Prácticas para administrar el acceso remoto	Estándares
PROTECCIÓN	Control de acceso remoto	El acceso telefónico para el mantenimiento del proveedor se habilita según sea necesario y se desactiva cuando se completa la ventana de mantenimiento	NIST SP 800-53 Rev 4 AC-17
		Acceso remoto solo autorizado a través de servicio VPN encriptado	NIST SP 800-53 Rev 4 AC-17 (1)
		Actividad de acceso remoto registrada y monitoreada	NIST SP 800-53 Rev 4 AC-17 (2)
		Acceso al servicio VPN restringido a dispositivos aprobados por la organización	NIST SP 800-53 Rev 4 AC-19
		Todos los intentos de conexión no autorizados a VPN se registran	NIST SP 800-53 Rev 4 AC-20
		Inhabilitación inmediata de la cuenta VPN tras la terminación del empleado	NIST SP 800-53 Rev 4 AC-20 (1)

Fuente: Energy Sector Cybersecurity Framework Implementation Guidance

El Control de Acceso engloba todo acceso a los activos y las instalaciones asociadas y se limita a los usuarios, procesos o dispositivos autorizados, y a las actividades y transacciones autorizadas

3 El subsector de electricidad tiene estándares personalizados o enfoques de ciberseguridad que muchas organizaciones pueden usar voluntariamente o por requerimiento...

Ejemplos de enfoques de gestión de riesgos de ciberseguridad disponibles en el sector energético y el subsector eléctrico

Nombre	Resumen
Ejemplo de Enfoques de Gestión de Riesgos de Ciberseguridad en el sector energético	
Modelo de madurez de capacidad de ciberseguridad (C2M2), subsector de electricidad y versiones específicas del subsector de petróleo y gas natural	Se utiliza para evaluar las capacidades de ciberseguridad de una organización y priorizar sus acciones e inversiones para mejorar la ciberseguridad
Revisión de la resistencia cibernética (CRR)	Evalúa las prácticas de resiliencia operativa y de ciberseguridad de una organización en diez dominios
Herramienta de Evaluación de Seguridad Cibernética (CSET)	Guía a los usuarios a través de un proceso paso a paso para evaluar sus sistemas de control y las prácticas de seguridad de la red de tecnología de la información en comparación con los estándares reconocidos de la industria
Lineamientos del proceso de gestión de riesgos de ciberseguridad (RMP) del sector eléctrico	Permite a las organizaciones aplicar procesos de administración de riesgos efectivos y eficientes y adaptarlos para cumplir con los requisitos de su organización
Ejemplos de enfoques de Gestión de Riesgos de Ciberseguridad del subsector de electricidad	
Estándares de protección de infraestructura crítica (CIP)	Los Estándares CIP de la Corporación de Confiabilidad Eléctrica de América del Norte (NERC) proporcionan un conjunto de requisitos regulatorios de ciberseguridad para ayudar a asegurar los activos del sistema de energía que operan y mantienen la red eléctrica a granel
Interagency Report (IR) 7628, Guidelines for Smart Grid Cyber Security	Las directrices del Instituto Nacional de Estándares y Tecnología (NIST) presentan un marco analítico para desarrollar estrategias efectivas de ciberseguridad adaptadas a sus características, riesgos y vulnerabilidades en particular relacionadas con la red inteligente

Fuente: Energy Sector Cybersecurity Framework Implementation Guidance

…algunos como el C2M2 tienen versiones personalizadas para diferentes subsectores y son ampliamente aplicables por el sector energético, pudiendo ser compatibles con la implementación del Marco de ciberseguridad (NIST 2014)

Normativas y estándares regulatorios

03

- Estándares regulatorios y voluntarios enfocados en Norteamérica
- Estándares regulatorios y voluntarios enfocados en Europa
- Estándares regulatorios y voluntarios de aplicación internacional

En mayo de 2018 entró en vigor la Directiva de la UE sobre Seguridad de Redes y Sistemas de Información (Directiva NIS)…

Ejemplos de estándares regulatorios y voluntarios

Enfocado en Europa

1

- La **Directiva NIS** (junto a la GDPR) es la **única ley con respecto a ciberseguridad para la UE**. Los estados miembros pueden implementar sus propias reglas de seguridad cibernética
- "La Estrategia de Ciberseguridad de la Unión Europea" (CSSEU) lanzada en 2013, establece un sistema para que los participantes públicos / privados contribuyan con las mejores prácticas
- Se adopta la Agenda Europea de Seguridad 2015-2020, siguiendo las indicaciones del CSSEU
- Se aprueba la Directiva sobre Seguridad de Redes y Sistemas de Información (NIS) (2015).
- Se crea la Plataforma de Ciberseguridad Experta en Energía (EECSP). En 2017, EECSP desarrolló un marco general, sin una línea de tiempo
- Se adopta el Reglamento General de Protección de Datos (GDPR) (2016), que establece normas estrictas para todas las empresas de la UE con respecto a la privacidad y la seguridad de los datos personales
- Asociaciones como SolarPower Europe y Wind Europe establecieron en 2017 objetivos para la protección de datos y CS (acciones específicas en etapas formativas)
- El organismo de estandarización CENELEC/ETSI, debido al mandato M490, ha desarrollado a través de diferentes grupos de trabajo un estudio de priorización de estándares de seguridad

*Todas las siglas se corresponden a la denominación de los estándares y organismos en inglés

…una nueva ley (que convivirá con el GDRP) diseñada para aplicar normas mínimas de buenas prácticas que permitan mejorar la seguridad general para los proveedores de servicios esenciales

1 El Grupo de cooperación NIS se creó para garantizar la cooperación estratégica y el intercambio de información entre los Estados miembros en materia de ciberseguridad

¿En qué consiste?

- La directiva contempla **cuatro objetivos principales**:
  - Administrar el riesgo de seguridad
  - Protección contra ciberataques
  - Detectar eventos de ciberseguridad
  - Minimizar el impacto de los incidentes
- Dentro de estos, se abarca todo, desde la gestión pública hasta la gestión de riesgos, la seguridad de la cadena de suministro, la capacitación del personal, los controles de seguridad, la gestión de activos o la recuperación y respuesta ante incidentes
- Legislaciones derivadas de la Directiva NIS instan a los Estados miembros a estar equipados y preparados para dar respuesta a incidentes de gran escala, por ejemplo, a través de un Equipo de Respuesta a Incidentes de Seguridad Informática (**CSIRT**) y una autoridad nacional competente en la materia
- En teoría, **al igual que ocurre con el GDPR**, se pueden aplicar multas por infracciones graves de hasta un millón de euros o el 4% del volumen del negocio global anual
- La creación de la Directiva NIS se debe a que las empresas están **cada vez más expuestas** a un mayor riesgo de ataque. Los defectos del software, los puertos de red abiertos, los cambios de archivos no detectados, la autenticación deficiente y los protocolos de red inseguros están listos para ser explotados por aquellos que tengan el conocimiento adecuado

Mapa del estado de transposición de la Directiva NIS en los Estados Miembros de la UE

La implantación sectorial de la Directiva NIS es uno de los objetivos del relanzamiento del Plan Estratégico de Ciberseguridad Europeo revisado en 2017 por la Comisión Europea

1 Las normas que se muestran a continuación son aplicadas por los operadores de todos los sectores energéticos a los que se refiere la Directiva NIS

Normas internacionales y buenas prácticas aplicables a todos los sectores energéticos

Estándares	Buenas prácticas
• ISO 27001: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos • ANSI / ISA, Serie ISA-62443: Seguridad para sistemas de control y automatización industrial • Marco NIST para mejorar la ciberseguridad de infraestructuras críticas	• Medidas detalladas - Seguridad cibernética para sistemas de control industrial - ANSSI (Francia) • Guía de Buenas Prácticas de Control de Procesos y SCADA • Seguridad - CPNI • Requisitos de seguridad del sistema AMI actualizados - UCAIUG: AMI-SEC-ASAP • Documento técnico de BDEW - Requisitos para controles seguros y sistemas de telecomunicaciones - Bundesverband der energie un Wasserwirtschaft • Requisitos básicos de seguridad de la información para el control de procesos, la seguridad y los sistemas de soporte de las TIC - OLF • Veinte controles críticos para una defensa cibernética efectiva: pautas de auditoría de consenso • Catálogo de Seguridad de Sistemas de Control: Recomendaciones para Desarrolladores de Estándares - USA DHS • 21 pasos para mejorar la seguridad cibernética de las redes SCADA - US DOE

- **ISO 27001 Revisión 2013**, el estándar más extendido a nivel mundial que cubre todos los aspectos de los sistemas de gestión de seguridad de la información en todos los sectores
- **ISA / IEC 62443,** una serie de estándares que definen procedimientos para implementar sistemas de control y automatización industrial de seguridad electrónica (IACS). Esta guía se aplica a los usuarios finales, los integradores de sistemas, los profesionales de la seguridad y los fabricantes de sistemas de control responsables de la fabricación, el diseño, la implementación o la administración de sistemas de control y automatización industrial
- El **marco de ciberseguridad de NIST**, que a pesar de que no es obligatorio incluso en los EE. UU., suele ser seguido por operadores de la UE que trabajan más allá del territorio de la UE, ya que es un buen punto de referencia para los requisitos de ciberseguridad

De acuerdo con algunos operadores de energía, las normas más frecuentemente aplicables para el sector energético, en su totalidad, son ISO 27001 e ISA / IEC 62443

1 Las normas que se muestran a continuación son aplicadas por los operadores del sector eléctrico al que se refiere la Directiva NIS

Normas internacionales y buenas prácticas aplicables al subsector eléctrico

Estándares	Buenas prácticas
• **Guía NIST SP800-82** para seguridad de sistemas de control industrial (ICS) • **ISO 27019** - Pautas de gestión de seguridad de la información basadas en ISO / IEC 27002 para sistemas de control de procesos específicos de la industria de servicios de energía • **NERC CIP Series** "Seguridad cibernética de protección de infraestructura crítica": CIP – 002 a CIP 011 • IEEE STANDARD 1402-2000 - Guía IEEE para seguridad física y electrónica de subestaciones de energía eléctrica • IEC 61850 - Automatización de la utilidad eléctrica	• Modelo de ciberseguridad, madurez de la capacidad de ciberseguridad del subsector de electricidad (esc2m2) - Departamento de Energía de EE. UU **(DOE)** • **NISTR 7628** - Pautas para la seguridad cibernética de redes inteligentes: vol. 1, Estrategia de ciberseguridad de Smart Grid, arquitectura y requisitos de alto nivel • Medidas de seguridad adecuadas para Smart Grids - **ENISA** • Mejores prácticas para el manejo de la seguridad de redes inteligentes cibernéticas - **Comisión de Energía de California**

- **NIST SP 800-82 Rev. 2**, la guía para la seguridad de los sistemas de control industrial (ICS) que proporciona orientación sobre cómo asegurar los sistemas de control industrial (ICS) y generalmente los operadores de la UE lo siguen como una buena práctica
- **ISO 27019** es la guía de gestión de seguridad de la información basada en ISO / IEC 27002 para sistemas de control de procesos específicos de la industria de servicios públicos de energía
- **NERC CIP** (North American Electric Reliability Corporation, protección de infraestructura crítica) es un conjunto de requisitos para el sistema eléctrico a granel de Norteamérica. También es seguido por operadores de la UE que extienden su negocio en los EE. UU.

Tanto la normativa NIST SP 800-82, la ISO 27019 como la NERC CIP cuentan con estándares que cubren Análisis de riesgos de seguridad de sistemas de información, Criptografía, Seguridad física y ambiental, y Procedimientos de mantenimiento de seguridad de TI

Normativas y estándares regulatorios

03

- Estándares regulatorios y voluntarios enfocados en Norteamérica
- Estándares regulatorios y voluntarios enfocados en Europa
- Estándares regulatorios y voluntarios de aplicación internacional

Las dos principales organizaciones en lo referido a estándares internacionales son la ISO (Organización Internacional de Normalización) y la IEC (Comisión Internacional Electrotécnica Comisión)

Ejemplos de estándares regulatorios y voluntarios

Enfocado en Europa

1. **IEC 61400** is an International Standard published by the International Electrotechnical Commission regarding wind turbines
2. International standard **IEC 61400-25** (Communications for monitoring and control of wind power plants)
3. Standard **IEC 61850** Communications for the control and Protection systems of electrical substations, Smart Grids, Electric Vehicle and Renewable Energies
4. **IECRE – Renewable Energy** (IEC System for certification to standards relating to equipment for use in renewable energy applications
5. **ISO/IEC TR 27019** - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
6. **ISO/IEC 15408-1**: Information technology -- Security techniques -- Evaluation criteria for IT security
7. **ISA/IEC 62443:** Industrial Network and System Security
8. **IEC 60870-5-101:** Standard for power system monitoring, control & associated communications for telecontrol, teleprotection, and associated telecommunications for electric power systems

*Todas las siglas se corresponden a la denominación de los estándares y organismos en inglés

El IEC publica Estándares internacionales y evaluación de conformidad para todas las tecnologías eléctricas, electrónicas y relacionadas mientras que la ISO se encarga de la creación de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización

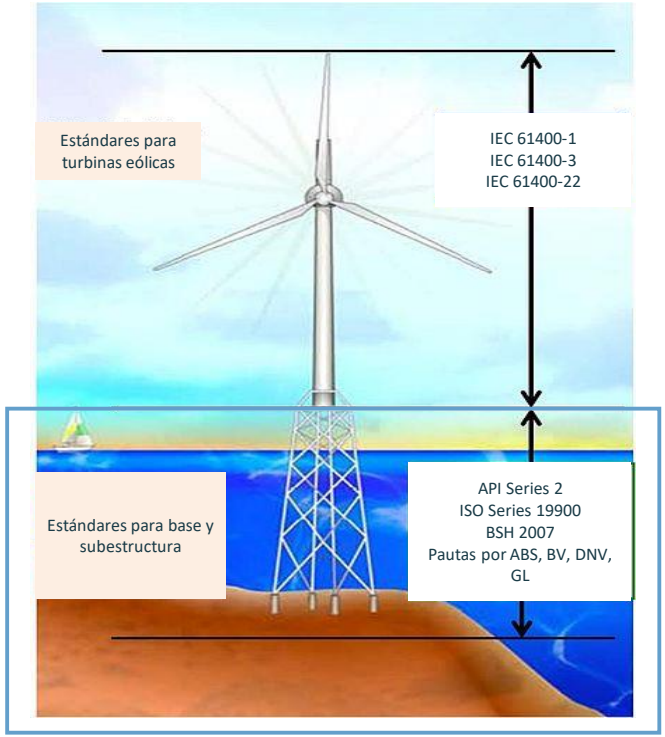
1 IEC 61400 es un estándar internacional publicado por la Comisión Electrotécnica Internacional (IEC) para el diseño de turbinas eólicas

- El 61400 es un conjunto de requisitos de diseño realizados para garantizar que las turbinas de viento estén diseñadas adecuadamente contra **daños por peligros dentro de la vida útil planificada**
- El estándar se refiere a la mayoría de los **aspectos de la vida útil de la turbina** desde las condiciones del sitio antes de la construcción, a los componentes de la turbina que se están probando, ensamblados y operados
- **Turbinas eólicas pequeñas** (de un área de barrido de hasta 200 m^2): las trata una norma **IEC 61400-2** algo simplificada (para este tipo de turbinas también se puede usar el estándar **IEC 61400-1**)

Para las **turbinas offshore de EE.UU.** son necesarios más estándares, los más importantes son:

- ISO 19900, Requisitos generales para estructuras costa afuera
- ISO 19902, estructuras costa afuera de acero fijo
- ISO 19903, estructuras marinas de hormigón fijas
- ISO 19904-1, Estructuras flotantes en alta mar - monocasco, semisumergibles y largueros
- ISO 19904-2, Estructuras flotantes en el mar - Plataformas de tensión y piernas
- API RP 2A-WSD, práctica recomendada para la planificación, el diseño y la construcción de plataformas fijas de acero en alta mar: diseño de tensión de trabajo

Aplicabilidad de los estándares de diseño existentes para turbinas eólicas marinas



2 En lo referente a seguridad, dentro de la norma internacional IEC 61400 destaca el subconjunto 61400-25 (Comunicaciones para monitoreo y control de plantas de energía eólica)

- IEC 61400-1: 2005 + AMD1: 2010 Requisitos de diseño
- IEC 61400-2: 2013 Pequeñas turbinas eólicas
- IEC 61400-3: 2009 Requisitos de diseño para aerogeneradores marinos
- IEC 61400-4: 2012 Requisitos de diseño para cajas de engranajes de turbinas eólicas
- IEC 61400-11: 2012 Técnicas de medición del ruido acústico
- IEC 61400-12-1: 2005 Mediciones del rendimiento energético de las turbinas eólicas productoras de electricidad
- IEC 61400-12-2: 2013 / COR1: 2016 Potencia de las turbinas eólicas generadoras de electricidad basadas en anemometría de góndolas / Corrigendum 1
- IEC 61400-12-1: mediciones lidar 2017
- IEC 61400-13: 2015 Medición de cargas mecánicas
- IEC TS 61400-14: 2005 Declaración del nivel aparente de potencia acústica y valores de tonalidad
- IEC 61400-21: 2008 Medición y evaluación de las características de calidad de energía de las turbinas eólicas conectadas a la red
- IEC 61400-22: prueba de conformidad 2010 y certificación
- IEC 61400-23: 2014 Ensayos estructurales a escala real de palas de rotor
- IEC 61400-24: 2010 Protección contra rayos
- **IEC 61400-25-1** 2006 Comunicaciones para monitoreo y control de plantas de energía eólica - Descripción general de principios y modelos
- **IEC 61400-25-2:** 2015 Comunicaciones para monitoreo y control de plantas de energía eólica - Modelos de información
- **IEC 61400-25-3**: 2015 Comunicaciones para monitoreo y control de plantas de energía eólica - Modelos de intercambio de información
- **IEC 61400-25-4:** 2008 Comunicaciones para monitoreo y control de plantas de energía eólica - Mapeo al perfil de comunicación
- **IEC 61400-25-5:** 2006 Comunicaciones para monitoreo y control de plantas de energía eólica - Pruebas de conformidad
- **IEC 61400-25-6:** 2010 Comunicaciones para monitoreo y control de plantas de energía eólica - Clases de nodos lógicos y clases de datos para monitoreo de condición
- IEC TS 61400-26-1: 2011 Disponibilidad basada en tiempo para sistemas de generación de turbinas eólicas
- IEC TS 61400-26-2: 2014 Disponibilidad basada en la producción para turbinas eólicas
- IEC 61400-27-1: 2015 Modelos de simulación eléctrica – Aerogeneradores

2 La norma internacional IEC 61400-25 proporciona un intercambio de información uniforme para el monitoreo y control de las plantas de energía eólica

El estándar IEC 61400-25 es una base para simplificar los roles que tienen que jugar la turbina eólica y los sistemas SCADA

- La serie estándar IEC 61400-25 proporciona una solución para el acceso a la información de la planta de energía eólica con nombres de datos y semántica estandarizados. Ofrece la posibilidad de adquirir soluciones de monitoreo y control como partes separadas, y de usar un sistema único para almacenar, analizar y presentar información sobre la energía eólica.

El uso de una solución de comunicación estándar es beneficioso para todas las partes: vendedores, integradores de sistemas y el cliente

- El costo adicional de desarrollar y mantener soluciones específicas de proveedores afecta tanto a los proveedores como a los integradores de sistemas y el cliente
- Una solución de comunicación estándar reduce el costo de integración y mantenimiento para todas las partes involucradas
- Los proveedores tienen la oportunidad de enfocar su negocio principal: la creación de instalaciones para el funcionamiento eficiente y optimizado de turbinas eólicas al incluir una solución de comunicación estándar en su cartera de productos

El uso del estándar IEC 61400-25 facilita la operativa a empresas dedicadas a labores de mantenimiento suponiendo un ahorro de costes

- Un acceso uniforme a la información operativa e histórica de las unidades de generación de turbinas eólicas es un requisito previo para una operación y un mantenimiento eficientes y efectivos de las plantas de energía eólica con una combinación de turbina eólica de diferentes proveedores y aerogeneradores en varios pasos evolutivos

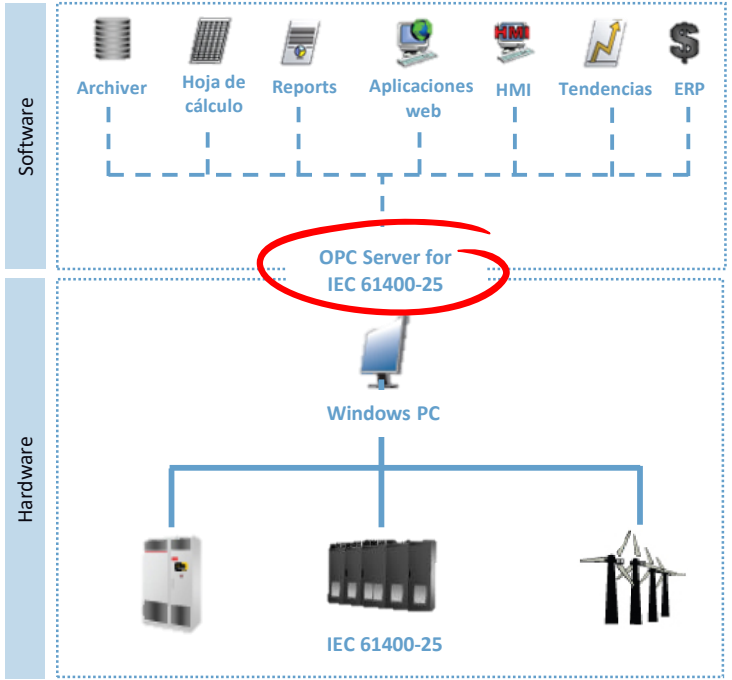
Grupo de usuarios de IEC 61400-25 (2016)

ENSOTEST, VATTENFALL, SIEMENS, TOSHIBA Leading Innovation, SENVION wind energy solutions, Vestas, e·on, ENERCON ENERGY FOR THE WORLD, RWE The energy to lead, TÜV SÜD, natcon7, bachmann., DONG energy, Statkraft, ALSTOM, DNV·GL DNV KEMA is now DNV GL, Netted Automation GmbH Information & Communication Systems, (Q-Technology, Dinamarca), TRIANGLE MICROWORKS, INC.

Fuente: IEC 61400-25 user group

Se recomienda a utilities, fabricantes, proveedores de servicios e integradores de sistemas interesados en cuestiones específicas de interoperabilidad que comiencen a operar bajo el estándar IEC 61400-25

2 IEC-61400-25 define los requisitos de comunicaciones para las plantas de energía eólica (la mayoría de los parques eólicos utilizan servicios de mensajes OPCXML-DA)



- El estándar ha especificado **cinco mapeos** (IEC 61400-25-4) a las pilas de protocolos de comunicación con el fin de abordar las necesidades reales de negocios de energía eólica para la comunicación
- Las asignaciones especificadas en la parte de IEC 61400-25 comprenden un mapeo de servicios web basados en:
  - ✓ Servicios web basados en SOAP
  - ✓ OPC XML-DA
  - ✓ DNP3
  - ✓ IEC 60870-5-104
  - ✓ IEC 61850-8-1 MMS

El **OPC** es un estándar de comunicación en el campo del control y supervisión de procesos industriales, que ofrece una interfaz común para comunicación que permite que componentes de software individuales interactúen y compartan datos

- Este servidor OPC permite monitorear y controlar las turbinas eólicas en sus plantas de energía eólica, así como compartir estos datos con cualquier aplicación compatible con OPC, como historiadores, HMI y SCADAs de forma segura
- El servidor se conecta a múltiples dispositivos al mismo tiempo, donde las operaciones de lectura y escritura con estos dispositivos se optimizan para entregar los datos necesarios en tiempo real

Ventajas del servidor OPC

- Seguridad OPC
- Redundancia de comunicación del dispositivo
- Procesamiento avanzado de etiquetas
- Alarma y eventos
- Máxima interoperabilidad
- Modo de simulación

Fuente: MatrikonOPC Server Advantage

El servidor IEC 61400-25 OPC proporciona conectividad a cualquier aerogenerador compatible con el estándar IEC 61400-25

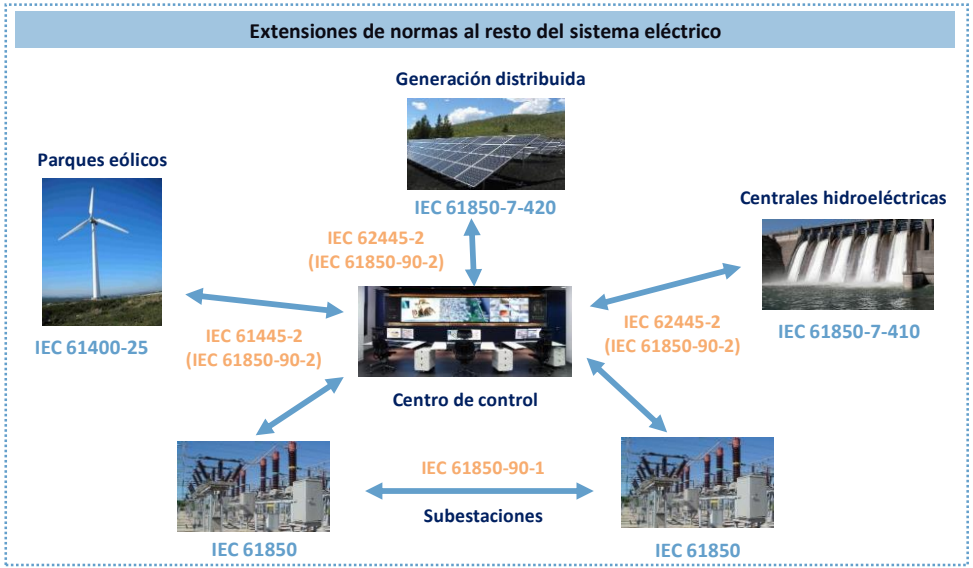
3 IEC 61850 es un estándar internacional que define protocolos de comunicación para dispositivos electrónicos inteligentes en subestaciones eléctricas

Objetivos IEC 61850

- La norma IEC 61850 define un **estándar de comunicación entre equipos de protección, control y medida dentro de una subestación**
- Objetivos:
  - Desarrollar un estándar internacional para las comunicaciones en el interior de una subestación automatizada
  - Conseguir interoperabilidad entre equipos de diferentes proveedores

Características IEC 61850

- Reducción del cableado convencional
  - LAN en lugar de múltiples cables de cobre
- A prueba de futuro
  - Los servicios y las inversiones serán duraderos a pesar de los rápidos cambios tecnológicos
  - El estándar está diseñado para seguir tanto el progreso en las tecnológicas de comunicación, como los requerimientos que envuelven a estos sistemas



- La norma también define otras propiedades que permiten uniformizar la automatización de las subestaciones:
  - Requerimientos de calidad (fiabilidad, mantenimiento, disponibilidad, seguridad) y condiciones ambientales (IEC 61850-3)
  - Procedimientos de los ensayos de conformidad, aseguramiento de la calidad, documentación requerida, certificación laboratorios de ensayo y requisitos equipos de ensayo (IEC 61850-10)

La adopción de la norma IEC 61850 como estándar es una oportunidad que el sector eléctrico no debería desaprovechar, ya que ofrece una reducción de costos desde el diseño hasta la operación y el mantenimiento

4 IECRE es el sistema IEC para la Certificación de Normas relacionadas con Equipos para el Uso en Aplicaciones de Energía Renovable

IEC Internacional Electrotécnico Comisión

169 países	20.000 expertos	9.000	1 Millón
con 84 países miembros	junto a > 212 Comités Técnicos	Normas Internacionales en catálogo	de Certificados de Evaluación de Conformidad emitidos

IECRE

El sistema IECRE tiene como objetivo facilitar el comercio internacional de equipos y servicios para su uso en Sectores de Energía Renovable mientras se mantiene el nivel de seguridad requerido

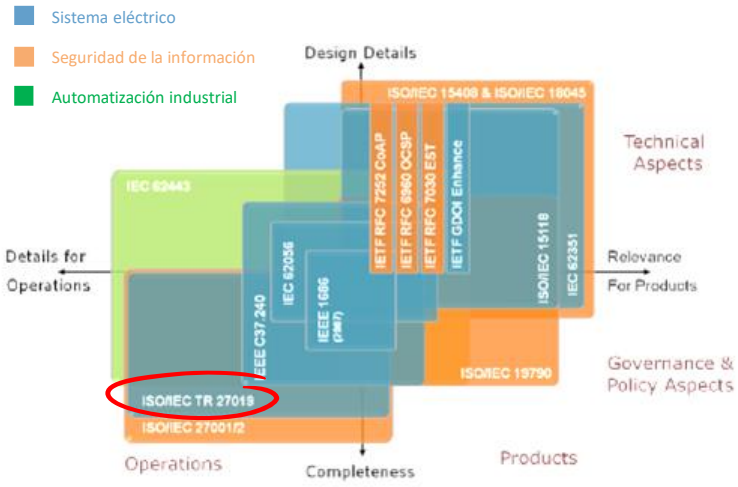
- El sistemas IECRE fue creado en reconocimiento de que la siempre creciente demanda de electricidad y la necesidad de reducir la parte de combustibles fósiles en la generación de energía han llevado a un rápido desarrollo y crecimiento del sector de la ER (energía renovable)
- Su intención es **ofrecer pruebas**, **inspección** y **certificación** para sectores como energía eólica, energía marina y energía FV (fotovoltaica) solar
- El Sistema IECRE se encuentra organizado actualmente en tres sectores:
  - Energía solar FV
  - Energía eólica
  - Energía marina

Lista de certificados IECRE – Energía eólica

Número de certificado	Estándar IEC	Emitido a	Organismo de certificación
IECRE.WE. TC.18.0006-R0	IEC 61400- 1:2005	Vestas Wind Systems A/S	Germanischer Lloyd Industrial Services GmbH
IECRE.WE. TC.16.0001-R0	IEC 61400- 1:2005	Vestas Wind Systems A/S	Germanischer Lloyd Industrial Services GmbH
IECRE.WE. TC.17.0004-R0	IEC 61400- 1:1999	Guangdong Mingyang Wind Power Industry Group Co., Ltd.	China General Certification Center (CGC)
IECRE.WE. TC.17.0003-R0	IEC 61400- 1:2005	Xiang Goldwind Science & Technology Co., Ltd.	China General Certification Center (CGC)
IECRE.WE. TC.16.0002-R0	IEC 61400- 1:2005 +Amd1: 2010	GE Energy GmbH	TÜV NORD CERT GmbH
IECRE.WE. TC.16.0002-R0	IEC 61400- 1:2005	Envision Energy (Jiangsu) Co., Ltd	China General Certification Center (CGC)

5 Los estándares de seguridad de la redes inteligentes están enfocados en tres particularidades: sistema eléctrico, seguridad de la información y la automatización industrial (1/3)

Campo de estándares de seguridad



En EEUU, gran precursor de marcos de referencia, ya se han desarrollado una serie de estándares relacionados con la ciberseguridad

Fuente: European Committe for Electrotechnical Standarcization (CENELEC)

Sistema eléctrico

ISO/IEC TR 27019

Ahora retirado
ISO / IEC TR 27019: 2013

Revisado por
ISO / IEC 27019: 2017

- Aunque se sitúe en el foco eléctrico, la norma IEC 27019 proviene de una base de sistemas de información (IEC 27002) y provee principios y controles específicos para los sistemas de control eléctricos
- El objetivo de ISO/IEC TR 27019:2013 es extender las series ISO/IEC 27000 al dominio de los procesos de automatización y control en el sector eléctrico y, de esta forma, dar soporte a la industria eléctrica en la implementación de un sistema de gestión de la seguridad de la información
- El estándar cubre el proceso de controlar y monitorizar la generación, transmisión, almacenamiento y distribución de energía, en combinación con el control de procesos de soporte. Incluye controles para las siguientes aplicaciones y componentes:

✓ Centro de control: sistema TI y sistema de monitorización, así como el sistema de automatización

✓ Componentes de automatización y controladores digitales tales como PLCs, incluyendo actuadores y sensores

✓ El resto de sistemas TI utilizados en el control del proceso del dominio

✓ Conjunto de tecnologías de comunicación empleadas en el control del proceso del suministro eléctrico (redes, telemetría, aplicaciones de telecontrol y control de remotas)

✓ Medida remota en la última milla

✓ Protección digital y sistemas safety (en productos como los PLCs por ejemplo)

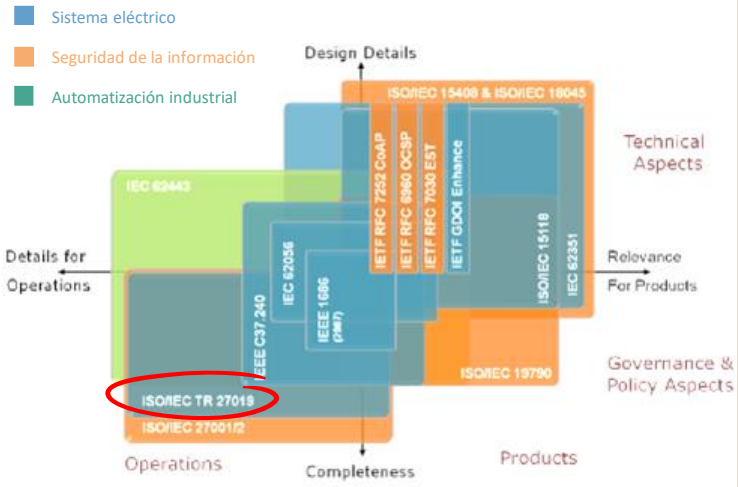
✓ Componentes de distribución DER (Distributed Energy Resources, Recursos de Energía Distribuida) preparados para futuras acometidas

✓ Software, firmware y aplicaciones instaladas en sistemas anteriormente citados

Nota: tanto los sistemas puramente eléctricos (o electromecánicos) como los sistemas de telecomunicaciones quedan fuera de este estándar

6 Los estándares de seguridad de la redes inteligentes están enfocados en tres particularidades: sistema eléctrico, seguridad de la información y la automatización industrial (2/3)

Campo de estándares de seguridad



Europa todavía se encuentra en una reflexión sobre si desarrollar un nuevo estándar de ciberseguridad o analizar las carencias existentes y mejorar los estándares actuales con carácter internacional

Fuente: European Committe for Electrotechnical Standarcization (CENELEC)

Seguridad de la información

ISO/IEC 15408

Previamente	Ahora bajo revisión	Será reemplazado por
ISO / IEC 15408-1: 2005	ISO / IEC 15408-1: 2009	ISO / IEC CD 15408-1

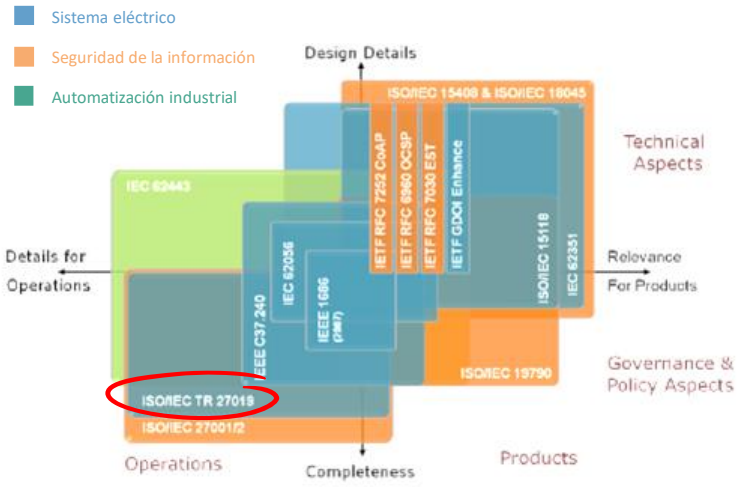
- La ISO/IEC 15408, también denominada Common Criteria (CC) o Criterios Comunes, es un estándar orientado al producto o sistema (no tanto al proceso como la serie ISO 27000) y establece las siguientes verificaciones:
  - ✓ Enfoque en la correcta definición de los requisitos de producto
  - ✓ Así mismo, han de implementarse satisfactoriamente y verificarse
  - ✓ El desarrollo y proceso de documentación deben seguir una directriz estructurada
- Es posible delimitar qué funcionalidades de seguridad se quieren evaluar a través de los perfiles de protección de CC y obtener un nivel de confianza específico (que va desde EAL1 a EAL7)

EAL1	Funcionalmente evaluado
EAL2	Estructuralmente evaluado
EAL3	Metodológicamente evaluado y verificado
EAL4	Metodológicamente diseñado, evaluado y verificado
EAL5	Diseñado y evaluado de forma semi-formal
EAL6	Verificado, diseñado y evaluado de forma semi-formal
EAL7	Verificado, diseñado y evaluado de forma formal

- Para las empresas de servicios públicos y operadoras finales lo importantes es requerir y conocer el nivel de confianza que pueden poseer algunos productos de los proveedores
- En los entornos más críticos de las redes inteligentes (como la comunicación entre el centro de control y las subestaciones) van a incluirse dispositivos de nueva generación de que proporcionen el máximo nivel de confianza

7 Los estándares de seguridad de la redes inteligentes están enfocados en tres particularidades: sistema eléctrico, seguridad de la información y la automatización industrial (3/3)

Campo de estándares de seguridad



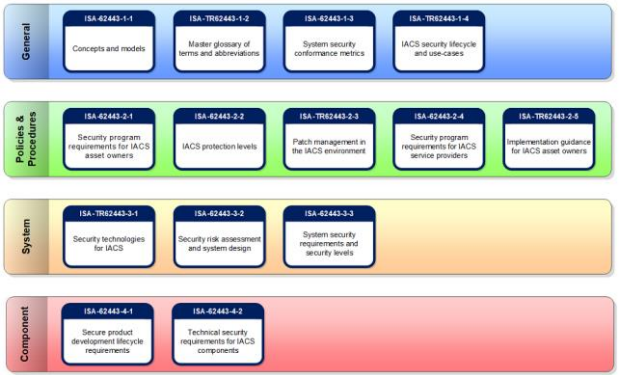
Europa debe definir un conjunto de estándares para el sector eléctrico que aglutine y mejore las referencias actuales y desarrolle nuevos marcos de referencia ante los nuevos retos que surgen con las redes inteligentes

Fuente: European Committe for Electrotechnical Standarcization (CENELEC)

Automatización industrial

ISA/IEC-62443

- La IEC 62443 y su precursor, la ISA 99, son un referente para la seguridad en la automatización y control industrial. Se trata de un set de estándares muy empleado en la industria. Cabe destacar la parte IEC-62443-4-2 que define los requisitos técnicos para la protección de los sistemas de control y automatización industrial
- Los sistemas de fabricación y control incluyen a:
  - ✓ Sistemas de hardware y software tales como DCS, PLC, SCADA, detección electrónica en red y sistemas de monitoreo y diagnóstico
  - ✓ Interfaces internas, humanas, de red o máquina asociadas que se utilizan para proporcionar funciones de control, seguridad y operaciones de fabricación a procesos
- La evaluación de la seguridad recogida por la norma ISA/IEC-62443 se reparte en los siguientes 4 apartados:

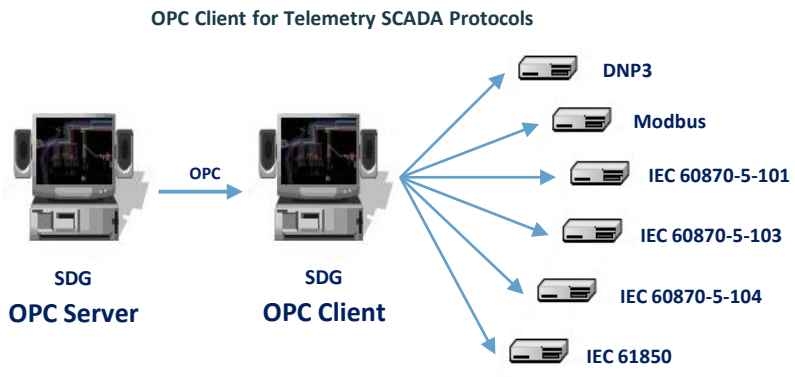


- ✓ General: incluye conceptos generales, modelos y terminologías
- ✓ Políticas y procedimientos: establece el programa de seguridad a los activos del sistema
- ✓ Sistema: Describe la guía segura del diseño del sistema y los requisitos para la integración de los componentes
- ✓ Componentes: Describe los requisitos de seguridad para especificar y diseñar los productos y sus subcomponentes

8 Los protocolos IEC 60870-5-101 e IEC 60870-5-104 son dos tecnologías de comunicación industrial para monitorear sistemas de control, sistemas de energía y comunicaciones asociadas

- **IEC 101 (IEC 60870-5-101)** es una norma internacional preparada por TC57 para la monitorización de los sistemas de energía, sistemas de control y sus comunicaciones asociadas; es totalmente compatible con las normas IEC 60870-5-1 y IEC 60870-5-5 y su uso estándar es en serie y asíncrono para el telecontrol de canales entre DTE y DCE

- El protocolo **IEC 104 (IEC 60870-5-104)** es la versión mejorada del protocolo 60870-5-101, e incluye mejoras en los servicios de la capa de red, de la capa de transporte, de la capa física y de la capa de enlace a fin de proveer la totalidad de accesos a la red.



Protocolo IEC 60870-5-104

- Este protocolo es más servicial, gracias a que permite conectar estaciones de control con subestaciones mediante IP o TCP (un protocolo que sirve para transmitir datos de una manera más segura)
- El IEC 60870-5-104 "pone barreras" a los datos que se comunica y al sistema de configuración definido con IEC 60870-5-101. Esto implica que no todas las funciones que soporta el IEC 60870-5-101 pueden combinarse con el IEC 60870-5-104

Protocolo DNP3

- DNP3, un protocolo industrial diseñado para transmitir datos entre dispositivos inteligentes y estaciones controladoras
- Incluso, el protocolo DNP3 es uno de los más usados en Estados Unidos y Canadá, pero tiene una presencia bastante tímida en Europa

La gran diferencia entre ambos protocolos es que el IEC 60870-5-104 puede transmitir datos de manera simultánea entre servidores y equipos, mientras que el 60870-5-101 no

Sistemas de protección perimetral, anti-intrusión y hurto, videovigilancia avanzada e iluminación son algunos de los sistemas para mejorar la seguridad en parques eólicos y huertos solares

Background

- La proliferación de nuevas infraestructuras para la **obtención de energía renovable** ha supuesto en la práctica nuevos desafíos en la seguridad para los que las empresas deben estar preparadas
- La maquinaria e instalación de los parques eólicos o de los huertos solares tiene un importante coste por el empleo de tecnología de última generación, unos bienes que deben ser protegidos del **vandalismo** y del **robo organizado** de materias primas o tecnología
- Cada vez más frecuentes los **intentos organizados de asalto** de estas instalaciones aprovechando la impunidad que aparentemente proporciona su ubicación, generalmente en zonas agrestes y mal comunicadas

Principales soluciones de acceso físico

Sistemas de videovigilancia

- ✓ Los equipos de grabación en **funcionamiento nocturno** gracias a los infrarrojos y empleo de **cámaras con visión térmica**, que localizan cualquier foco de calor que sea similar a un animal o humano
- ✓ **Sistemas de videoanálisis** que permite automatizar muchos comportamientos sospechosos a través del análisis de imágenes

Iluminación disuasoria

- ✓ Sistemas que iluminan un área donde se detecte movimiento no autorizado
- ✓ Sistema de **iluminación infrarroja de leds**, para visión nocturna de bajo consumo que ayuda a localizar a los posibles intrusos

Sistemas anti-intrusión

- ✓ Para la zona interna de la instalación se debe completar el sistema con **detectores volumétricos** de calidad profesional, con doble y triple tecnología de detección y apoyados por **cámaras de vigilancia** que permitan la comprobación rápida de la amenaza

Sistemas de seguridad en parques eólicos

- Además de en cada aerogenerador, la seguridad también debe de establecerse desde un perímetro adecuado alrededor de la torreta, básicamente con un **sistema de detección** que lance una alarma ante una aproximación al molino y en el intento de acceso por la puerta en su base
- En las zonas del interior del aerogenerador establecer sistemas de detección magnética y volumétrica
- El **sistema de videovigilancia** en parques eólicos será el perfecto apoyo para actuar y verificar la amenaza desde un centro de control
- Es interesante disponer de **seguridad privada**, aunque la **seguridad electrónica** (intrusión y video vigilancia, principalmente) es algo básico dadas las grandes extensiones de terreno en las que se distribuyen

Los incidentes más frecuentes siguen siendo los **actos de vandalismo** o la práctica de **actividades peligrosas** como realizar los saltos con paracaídas, fotografiarse en altura o acciones que busquen ensuciar la instalación o quebrantarla

Tabla resumen - Mapeo de medidas de seguridad con estándares específicos de electricidad aplicables a la UE y a EE.UU.

Medida de seguridad	NIST SP-800-82	NIST SP-800-82	NERC CIP
Análisis de riesgos de seguridad del sistema de información	3. Gestión y evaluación de riesgos de ICS 4.5 Implementar un riesgo de seguridad ICS	14.1.4 Marco de planificación de continuidad de negocio	• CIP-002-3 Identificación de activos cibernéticos críticos
Política de seguridad del sistema de información	3.3.1 Vulnerabilidades de políticas y procedimientos	5. Política de seguridad	• CIP-003-6 Cyber Security - Controles de gestión de seguridad • CIP-011-2 Tabla R1 - Protección de la información
Seguridad de los recursos humanos	6.2.1 Seguridad del personal	8. Seguridad de los recursos humanos	• CIP-004 Seguridad Cibernética - Personal y Capacitación • CIP-004-6 Tabla R1 - Programa de concientización sobre la seguridad • CIP-004-6 Tabla R3: Programa de evaluación de riesgos del personal
Configuración de sistemas	6.2.4 Gestión de la configuración	11.4.4 Protección remota de puertos de configuración y diagnóstico	• CIP-007-6 Tabla R1: Puertos y servicios • CIP-010-2 Tabla R1 - Gestión de cambios de configuración
Criptografía	6.3.4.1 Cifrado	12.3 controles criptográficos 15.1.6 Regulación de los controles criptográficos	• CIP-011-2 Seguridad cibernética - Protección de la información
Autenticación e identificación	6.3.2 Control de acceso 6.3.1 Identificación y autenticación	11. Control de acceso	• CIP-007-6 Tabla R5 - Control de acceso al sistema • CIP-004-6 Tabla R4– Programa de gestión de acceso
Acceso remoto	6.3.2 Control de acceso 6.3.1 Identificación y autenticación	11.4 Control de acceso a la red 11.4.4 Protección remota de puertos de configuración y diagnóstico	• CIP-005-5 Tabla R2 - Interactivo • Gestión de acceso remoto
Seguridad física y ambiental	6.2.2 Protección física y ambiental 6.2.7 Protección de medios	9. Seguridad física y ambiental. 9.2 Seguridad del equipo	• CIP-006-6 Cyber Security - Seguridad física de BES Cyber Systems • CIP-014-1 Seguridad Física
Registros de correlación y análisis	5.16 Monitoreo, registro y auditoría	10.2.2 Seguimiento y revisión de servicios de terceros. 10.10.2 Uso del sistema de monitoreo	• CIP-007-6 Tabla R4 - Monitoreo de eventos de seguridad

Iniciativas en materia de ciberseguridad

04

- Estado de la Ciberseguridad Industrial en Euskadi (primer estudio en el sector industrial en una CCAA)
- Casos de empresas contratantes de servicios de ciberseguridad

Las normas para el establecimiento de la Ciberseguridad Industrial más aplicadas por las empresas vascas son la protección de datos personales (con >60%) y la ISO 27001 (con >20%)

Estado de madurez de la ciberseguridad industrial en Euskadi

Nivel de sensibilización

- Un 80% de los responsables de la Ciberseguridad en empresas industriales se consideran normal o bastante **sensibilizados sobre las regulaciones** a las que están sujetas sus empresas y los riesgos de la ciberseguridad. No obstante, un 18% continúan asegurando estar muy poco preocupados

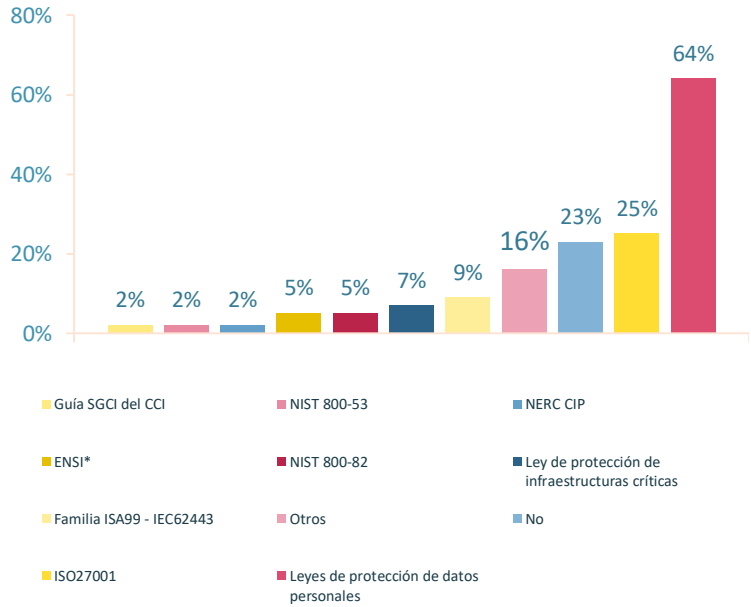
Responsables de la ciberseguridad

- La unidad organizativa de TI Corporativa es la **encargada de velar por la Ciberseguridad** de las empresas industriales en un 70% de los casos, seguida de lejos (entre un 10% y 20%) por las unidades de Seguridad Física, Operaciones, HSE (Riesgo Laboral y Medioambiental) y Automatización de procesos industriales. A pesar de ello, la responsabilidad sobre la Ciberseguridad no recae sobre un único departamento en la mayoría de los casos

Evaluaciones de riesgo

- Cerca de un 40% de las empresas han declarado haber realizado evaluaciones organizativas y un 30% evaluaciones técnicas, mientras que un 18% han llevado a cabo **evaluaciones en base a normativas, como IEC62443-ISA99 o NERC-CIP**

¿Están las empresas utilizando normas y patrones en el ámbito industrial?



De entre aquellas específicas para la Ciberseguridad Industrial, aparecen la guía SGCI del CCI, y las reglamentaciones sectoriales, como NERC CIP enfocada a la protección de infraestructuras críticas de sistemas de energía eléctrica

El principal motivo para el establecimiento de accesos remotos a los sistemas de control industriales de las empresas es la gestión de estos…

Estado de madurez de la ciberseguridad industrial en Euskadi

Plan de gestión de incidentes

- Debido a que los sistemas de protección no son 100% seguros, también es necesario contar con un **plan para la gestión de incidencias de seguridad**, y es aquí donde la industria vasca tiene más trabajo por delante: solo el 12% de las empresas cuentan con un plan definido, desarrollado y probado
- Un 23% más están definiendo el proceso de gestión de incidencias, y en contra se encuentran el 27% que no tiene un plan diseñado y otro 27% que actúa de forma reactiva

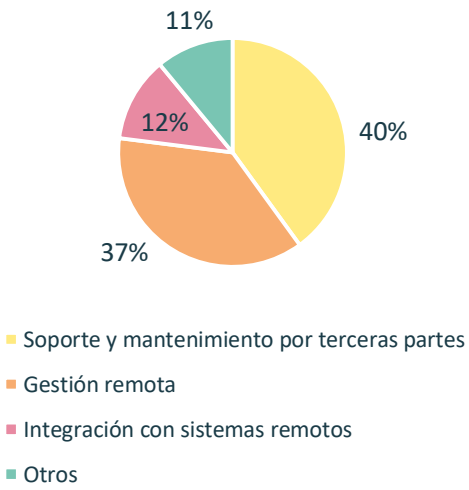
Conexión a Internet

- Un 45% tienen algún elemento conectado permanentemente a internet, mientras que un 30% usan conexiones temporales por petición. La casuística más habitual (dándose en un 80% de los casos), es la posibilidad de **acceder remotamente a la red industrial**, en su mayoría para llevar a cabo tareas de soporte y mantenimiento por terceras partes o para gestiones remotas

Medidas actuales

- Casi todas las empresas encuestadas contaban con algún tipo de medida de Ciberseguridad Industrial: las más habituales son el uso de soluciones automatizadas de **copias de respaldo**, **antivirus** o **firewall convencionales**
- Sin embargo, no siempre las medidas implementadas son las apropiadas, ya que los entornos OT necesitan dispositivos específicamente diseñados para su protección, no siendo siempre válidos aquellos diseñados para entornos IT

Motivo para tener accesos remotos a la red industrial



Fuente: Estudio elaborado por BCSC (Centro Vasco de Ciberseguridad) y CCI (Centro de Ciberseguridad Industrial)

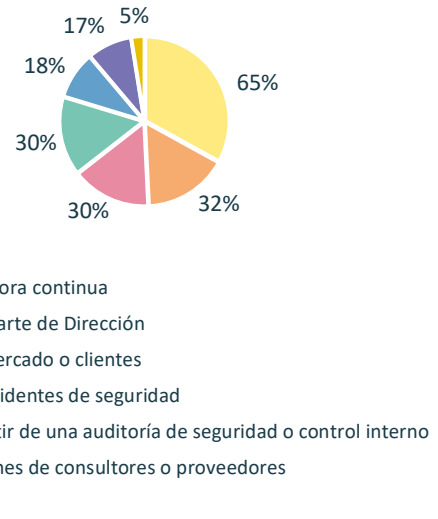
…de ellos, un 37% accede a la red industrial para realizar labores de soporte y mantenimiento en remoto por terceras partes, y para ello, la empresa contratante deberá permitir el acceso a sus equipos fuera de su control, con desconocimiento de uso, estado y nivel de seguridad

Según el estudio del BCSC y CCI, un 85% de las empresas industriales vascas aumentarán el presupuesto y los recursos humanos destinados a la Ciberseguridad a lo largo de 2018

Conclusiones del estado de la Ciberseguridad en la industria vasca

1. La gestión del riesgo en los sistemas de automatización y control está siendo asumida por el área de tecnologías de la información lo que implica que se aborda con una **visión parcial**
2. Es preciso **elevar el nivel de concienciación** frente a la necesidad y las implicaciones de la Ciberseguridad Industrial a **todos los niveles de la organización**
3. Se identifican **dos factores** principales que están **acelerando la digitalización** de la industria en Euskadi y como consecuencia de ello la necesidad de gestionar el riesgo tecnológico especialmente asociado con la ciberseguridad: la **regulación** y la **globalización**
4. El mercado, las empresas y los proveedores de servicios en el ámbito industrial precisan de **profesionales especializados** en la protección de los entornos de producción industrial
5. La mayoría de las organizaciones vascas encuestadas (de todos los sectores de la industria) tienen previsto abordar a lo largo de 2018 iniciativas de Ciberseguridad Industrial, lo que casi con toda seguridad implicará un aumento de los presupuestos destinados a esta materia y es esperable, aunque no es fácil de cuantificar, que se produzca una **elevación del grado de madurez** general (algo muy necesario dados los bajos niveles de protección frente a ciberamenazas que presentan los sistemas actuales de control industrial)

Motivaciones para la ejecución de proyectos de ciberseguridad en el ámbito industrial



Fuente: Estudio elaborado por BCSC (Centro Vasco de Ciberseguridad) y CCI (Centro de Ciberseguridad Industrial)

En cuanto a los motivos por los que las empresas apuestan por implantar soluciones ciberseguras, es significativa la presencia de factores como las exigencias por parte de la Dirección y las necesidades del mercado, lo que revela un incremento de la madurez en la gestión de este riesgo

1

GE Global Research ha recibido fondos federales para desarrollar protecciones de seguridad cibernética para activos energéticos críticos, incluidos los aerogeneradores

Antecedentes

- Con el objetivo de salvaguardar los activos de poder crítico de la nación en la próxima era de la computación cuántica y las redes, equipos interdisciplinarios de científicos e ingenieros de GE Global Research (el negocio de investigación y desarrollo de GE) liderarán tres proyectos con el Departamento de Energía de EE.UU. (DOE)
- El fin último de estos proyectos es desarrollar un **ciberespacio avanzado**: tecnologías de protección que detectan, localizan y neutralizan ataques a sistemas de energía y activos críticos

Empresa

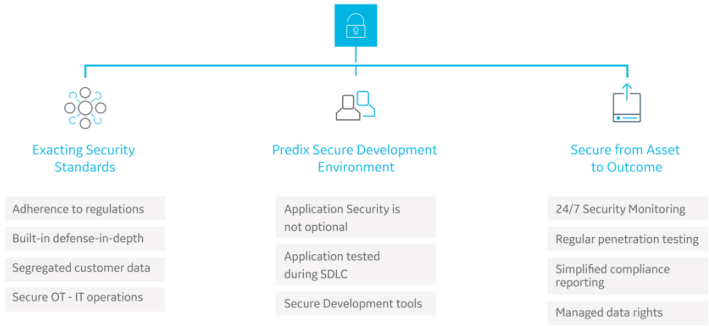
GE Global Research

General Electric

Enfoque y metodología

El plan de la compañía vasca engloba diversas líneas de trabajo:

- Construcción del **primer sistema inmunitario industrial del mundo** que detecta, localiza y neutraliza las amenazas cibernéticas, una presencia invisible que vigila y controla cada parte del sistema de energía y es capaz de cambiar el funcionamiento de dicho sistema para permitir que funcione de manera segura ante un ataque cibernético



Próximos pasos

- GE Global Research y sus socios desarrollarán una variedad de nuevas tecnologías de defensa adaptativa que permiten a los sistemas de generación de energía eólica sobrevivir a ataques cibernéticos sofisticados al mejorar las capacidades de detección, localización y alojamiento de los sistemas de control
- Bajo el **proyecto "Resiliencia Cibernética Física para la Generación de Energía Eólica"** del DOE, GE Global Research trabajará con GE Renewable Energy, Idaho National Labs e Invenergy, para Desarrollar nuevas tecnologías de protección cibernética comercialmente viables y probadas en el campo para sistemas de generación de energía eólica

2

El área de TI de Sidenor está desarrollando un ambicioso plan que engloba diversas líneas de trabajo relacionadas con potenciar y mejorar sus controles de Ciberseguridad

Antecedentes

- Inmersos en pleno proceso de digitalización Sidenor 4.0, el área de ciberseguridad es un importante pilar en el que la compañía está invirtiendo muchos recursos
- En 2018, se ha dado un gran impulso gracias a la concienciación cada vez mayor entre las instituciones, siendo Sidenor una de las empresas reconocidas por el Gobierno Vasco para obtener apoyos de diversa índole para el cumplimiento del Plan de ciberseguridad
- Durante el mes de agosto, se ha llevado a cabo la renovación de la red de Acería de Basauri y de Sistemas

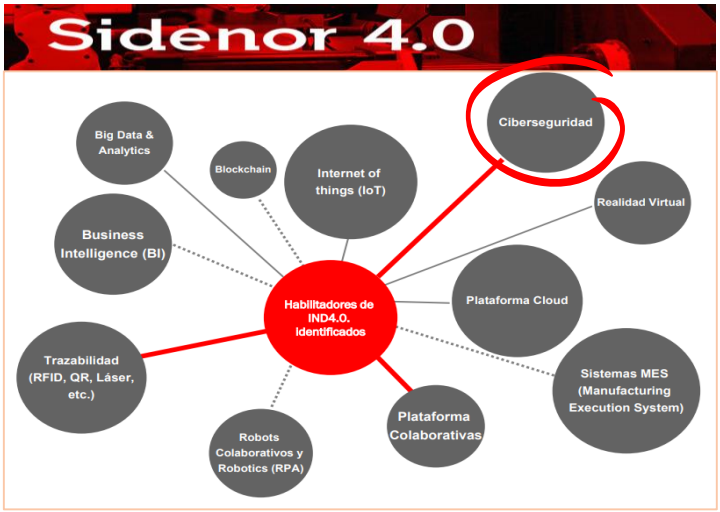
Empresa

Sidenor

Enfoque y metodología

El plan de la compañía vasca engloba diversas líneas de trabajo:

- Revisión del proceso de securización de todos los equipos informáticos
- Actualización de los firewalls y reglas de control de acceso
- Desarrollo de un sistema de monitorización de alertas de seguridad
- Actualización del plan de continuidad de negocio
- Rediseño, segmentación y securización de la red



Próximos pasos

- A lo largo del último trimestre de 2018 se comenzará el proyecto de segmentación y securización de la red, que cuenta con las siguientes medidas:
  - Implantación de diferentes firewalls
  - Creación de reglas de filtrado entre subredes
  - Segmentación de las redes existentes, de manera que se puedan aislar unas de otras y así mitigar la propagación de posibles ataques

3

Invenergy selecciona a GE Renewable Energy para proporcionar seguridad cibernética a toda su flota existente, así como para futuros parques eólicos

Antecedentes

- A medida que las amenazas en línea se multiplican y la red eléctrica se vuelve digital, la **seguridad cibernética** es una de las **principales prioridades** de Invenergy
- Esta creciente preocupación por la ciberseguridad ha llevado a Invenergy a colaborar con el equipo de GE Digital para desarrollar un acuerdo de seguridad cibernética a largo plazo para toda la empresa que satisfaga sus necesidades operativas y que sirva como marco para agregar futuros parques eólicos a la red
- Con un valor de más de $13 millones en diez años, este es uno de los acuerdos de seguridad cibernética más grandes en la historia del Internet industrial

Enfoque y metodología

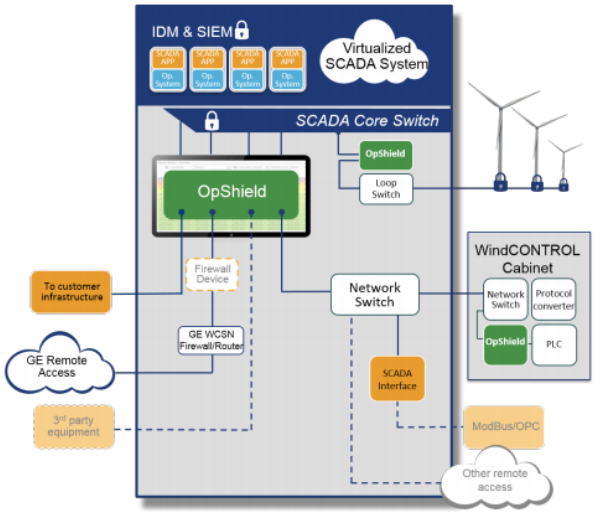
- **Wurldtech**, una compañía de GE, se centra en la seguridad cibernética y en la protección de la tecnología operativa además de la tecnología de la información.
- Este acuerdo incluye:
  - Actualizar los controles heredados de Invenergy, actualizar y proteger la seguridad de su red con Opshield de Wurldtech , una solución de seguridad diseñada especialmente para entornos industriales y de control de procesos
  - Proporción por parte de GE y Wurldtech a Invenergy de mantenimiento, actualizaciones y parches del software durante el período de diez años

Próximos pasos

- El objetivo de GE es poder continuar con el éxito de apoyar a la flota de Invenergy bajo contrato y expandirla a otras flotas de viento, ofreciendo un paquete completo de seguridad cibernética diseñado específicamente para parques eólicos - Wind SCADA Secure Edition
- Esta colección de tecnologías está integrada para construir o mejorar la postura cibernética de la Tecnología Operacional (OT) de los clientes en el entorno interno y externo de la planta eólica

Empresa

Invenergy
& General Electric



4

Siemens firma un protocolo sobre ciberseguridad junto a otras grandes corporaciones en la Conferencia de Seguridad de Múnich de 2018

Empresa

Siemens

Bases del pacto

- Impulsada por Siemens, la Carta de Fideicomiso, como se denomina el protocolo, exige normas y estándares vinculantes para generar confianza en el ámbito de la ciberseguridad y avanzar en la digitalización
- Además de Siemens, el protocolo ha sido firmado por la Conferencia de Seguridad de Munich (MSC), y las compañías Airbus, Allianz, Daimler Group, IBM, NXP, SGS y Deutsche Telekom

Enfoque y metodología

- Este protocolo establece **10 áreas de acción en ciberseguridad** en las que los gobiernos y las empresas deben ser activos
- Este protocolo requiere que la responsabilidad en ciberseguridad sea asumida por los más altos niveles tanto de los gobiernos como de las empresas, con la introducción de un **Ministerio dedicado a ello** (en los gobiernos) y un **director de seguridad** informática en las empresas
- También se exige que las empresas establezcan una **certificación externa e independiente**, obligatoria para infraestructuras críticas, sobre todo, donde se puedan dar situaciones peligrosas

Próximos pasos

- Se busca que, a futuro, las funciones de seguridad y protección de datos se pre-configuren como parte de las tecnologías, y los reglamentos de ciberseguridad se incorporen a los acuerdos de libre comercio
- Los firmantes del protocolo también piden mayores esfuerzos para fomentar la comprensión de la ciberseguridad a través de la **formación** y la **educación continua**, así como iniciativas internacionales

5

La empresa First Wind implementó soluciones de videovigilancia basada en IP, controles de acceso físico y redes conectadas

Antecedentes

- First Wind es una empresa de energía eólica independiente que se dedica exclusivamente al desarrollo, financiamiento, construcción, propiedad y operación de proyectos eólicos para suministro energético a escala comercial en los Estados Unidos
- Entre los desafíos que llevaron a First Wind a contratar los servicios de Cisco destacan:
  - La necesidad de reducir el tiempo que invertía uno de sus operarios en viajar a cada sitio para realizar cambios tales como agregar o eliminar privilegios de acceso de empleados
  - El deseo de centralizar el monitoreo de las cámaras de videovigilancia, con el objetivo de acelerar la detección de incidentes
  - Hacer llegar la red a las subestaciones distantes planteó otro desafío, ya que las condiciones extremas del entorno exigían dispositivos reforzados

Resultados

- First Wind utiliza la solución **Cisco Physical Access Control** para controlar el acceso a puertas exteriores, puertas de subestaciones y laboratorios mediante cámaras de videovigilancia montadas cerca de las puertas y en las áreas de depósito, de modo que la empresa puede monitorear el cumplimiento de las directrices de seguridad
- Para hacer llegar la red a las subestaciones, First Wind contrató los servicios de LookingPoint, partner de Cisco, para implementar **switches** y **routers** Cisco Connected Grid con la que los administradores de redes se ahorran la tarea de aprender una nueva interfaz y herramientas para las redes de subestaciones
- Gracias a la soluciones Cisco Video Surveillance y Cisco Physical Access Manager, First Wind pudo simplificar y mejorar la seguridad física en sus parques eólicos. Resultados:
  - Seguridad física simplificada
  - Menos costos gracias a la consolidación de red
  - Reducción del gasto operativo

Empresa

First Wind

Resumen ejecutivo

First Wind
- Energía
- Boston, Massachusetts

Desafío comercial
- Proteger al personal y la propiedad en ubicaciones distantes
- Simplificar la administración de TI
- Minimizar los costos operativos

Solución de red
- Administración centralizada de sistemas de seguridad física por medio de Cisco Video Surveillance y Cisco Physical Access Control
- Red unificada para todas las aplicaciones de voz, video y de datos de las subestaciones, con switches y routers Cisco Connected Grid

Solución de red
- Administración centralizada de sistemas de seguridad física por medio de Cisco Video Surveillance y Cisco Physical Access Control
- Red unificada para todas las aplicaciones de voz, video y de datos de las subestaciones, con switches y routers Cisco Connected Grid

Análisis de la situación y recomendaciones individualizadas a cada empresa

05

Se llevaron a cabo entrevistas individuales con los principales responsables de los áreas de ciberseguridad de las 4 empresas participantes en el proyecto

• 1 - 12 de Octubre

- Elaboración de un cuestionario con el objetivo de conocer con más detalle los equipos y las soluciones cibernéticas de las que disponen actualmente las empresas
- Con la información recogidas gracias a las respuestas de dicho cuestionario se pudo tener una imagen más nítida sobre la situación actual de cada una de las empresas
- El objetivo de este cuestionario era abordar de las forma más eficiente cada una de las entrevistas

• 15 - 16 de Octubre

- Reunión de 2,5h de duración en las instalaciones de cada una de las empresas participantes en el proyecto con los principales responsables del área de ciberseguridad de cada una de ellas

NORDEX · SIEMENS Gamesa RENEWABLE ENERGY · Ingeteam · CENER | CENTRO NACIONAL DE ENERGÍAS RENOVABLES

• 17 - 26 de Octubre

- Tras enviarles una primera versión sobre nuestro entendimiento de la situación actual en cuanto a sistemas y forma de operar, se dio un plazo de 2-3 días para que nos hicieran llegar cuantas matizaciones, correcciones o sugerencias estimasen conveniente
- Con el feedback recogido se elaboró un documento individual para cada empresa recogiendo un análisis de su situación y posibles recomendaciones y medidas a tomar
- Como se acordó con cada cliente, este documento sería confidencial ya que recogía información relevante sobre la metodología de operación de cada empresa

Tendencias, buenas prácticas y hoja de ruta para futuros proyectos

06

- Retos, tendencias y arquitecturas alternativas
- Buenas prácticas y hoja de ruta para futuros proyectos

Las tecnologías digitales juegan un papel cada vez más relevante dentro de la infraestructura energética lo que ha causado que en los últimos años el sector eléctrico esté más expuesto

¿Qué retos de seguridad se esperan para 2018 para el sector energético?

De la misma manera que la ciberseguridad se actualiza, también lo hacen los hackers, muchas veces al mismo ritmo

- **Incremento de las infecciones de malware generales y accidentales**
  - Según los datos correspondientes al tercer trimestre del año, la creación de malware aumentó, con un total de 20 millones de nuevos ejemplares generados mundialmente
  - Los delincuentes cibernéticos tienen a las empresas de energía en el punto de mira, por ello en 2018 continuaremos viendo un aumento de las infecciones de malware generales y accidentales en las redes industriales

- **CaaS (Crimen como servicio)**
  - Este es otro tipo de amenaza que comenzaremos a ver en mayor medida este año. En 2017 aumentaron los delitos cibernéticos, específicamente en casos de crimen como servicio. Esta tendencia se mantendrá en 2018 y las organizaciones que se dedican a esto irán diversificando aún más su forma de trabajo, expandiendo sus operaciones a mercados globales

- **Ciberespionaje industria**
  - El robo de información podría tener otra finalidad. Más allá de pedir dinero por devolver lo robado, los ataques de ransomware contra empresas de energía podrían dar pie al ciberespionaje industrial. Los delincuentes podrían utilizar la información robada para preparar nuevos ataques dirigidos al sector

Fuente: PandaLabs, laboratorio anti-malware de Panda Security

Los sistemas de las empresas energéticas aún son demasiado vulnerables, por ello se están tomando diferentes acciones para mejorar la seguridad

Nuevas tendencias de seguridad para el sector energético

Las acciones enfocadas a mejorar la seguridad de sector energético se dirigen a:

- Protección del negocio
- Prevención de interrupciones y pérdidas de datos
- Capacidad de reacción

British Solar Renewables

British Solar Renewables

- Empresas como British Solar Renewables están desarrollando acciones enfocadas a mejorar la seguridad de sector energético: su director ha asegurado que están tomando **medidas para incluir la seguridad cibernética en todos sus diseños, soluciones y actividades**

BERKELEY LAB

Berkeley Lab

- Berkeley Lab anunció en 2017 el lanzamiento un proyecto para **mitigar las vulnerabilidades cibernéticas** en **paneles solares** integrados en la red
- El proyecto, que el Departamento de Energía (DoE) está financiando actualmente con 2,5 millones de dólares en tres años, desarrollará herramientas para detectar y combatir ciertos tipos de ciberataques en la red

Fuente: PrimeStone

El creciente interés en la tecnología industrial del sector de la energía está descubriendo puntos vulnerables que antes no eran evidentes porque el control de supervisión y adquisición de datos (SCADA) u otros sistemas no se comunicaban con las redes informáticas tradicionales

El entorno OT requiere un vigor mucho más fuerte para protegerse contra los ataques que puedan provenir de Internet

Pautas para conseguir un entorno de operaciones bien definido y protegido

- El SCADA del parque eólico debe existir dentro de su propio entorno de red, sin acceso directo a Internet desde esa red
- La red SCADA debe estar separada del resto de la red corporativa a través de tecnologías (es decir, firewall, DMZ) que limitan el tráfico permitido entre los dos a solo eso con una designación especial
- El acceso del usuario al entorno de red OT debe controlarse y examinarse con frecuencia para garantizar que solo aquellos que requieren acceso tengan acceso
- Las listas de acceso deben ser revisadas a intervalos regulares por la alta gerencia; el acceso extraño y los empleados que se hayan ido deben eliminarse de inmediato
- El tráfico dentro de la "red" de SCADA debe ser monitoreado de cerca con sofisticadas capacidades de detección de intrusos para identificar cualquier actividad sospechosa

Dentro del entorno corporativo, existen subredes con barreras de seguridad más flexibles, debido a los requisitos de intercambio de datos y del sistema entre los departamentos; al contrario de lo que sucede en los sistemas de TI que suelen estar fortificados con firewalls, servidores proxy y servicios de detección de intrusos

Buenas prácticas en seguridad cibernética para tecnologías de energías renovables (1/4)

Análisis de situación

Las empresas de energía renovable deben realizar evaluaciones integrales de su postura actual de ciberseguridad

- En relación a la realización de **evaluaciones exhaustivas** de su postura actual de ciberseguridad por parte de las empresas existen varias opciones tanto para la autoevaluación como para la evaluación externa
- El Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. ofrece una **guía gratuita** para evaluar e implementar un marco de ciberseguridad para los fabricantes
- La Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA) está trabajando para **estandarizar las prácticas de seguridad en toda la Unión Europea** (UE). Ofrecen guías de cumplimiento en su sitio web, incluido el marco de gobernanza para la normalización europea y la definición de ciberseguridad.
- La UE también ofrece copias gratuitas de su Directiva sobre seguridad de redes y sistemas de información, disponible en varios idiomas
- Otras opciones de evaluación de seguridad incluyen proveedores externos, la Herramienta de Evaluación de Ciberseguridad del Consejo Federal de Exámenes de Instituciones Financieras (FFIEC) y la contratación de profesionales de TI con CISSP, CISM, CISA, ISO / IEC 27001:2013, CRISC o Certificaciones QSA / ISA

Fuente: US National Institute of Standards and Technology (NIST)
EU Directive on Security of Network and Information Systems

Las empresas de energías renovables deben realizar evaluaciones exhaustivas de su postura actual de ciberseguridad antes de cualquier inversión en soluciones de seguridad de terceros o internas

Buenas prácticas en seguridad cibernética para tecnologías de energías renovables (2/4)

Actualización de activos

Los sistemas actualizados proporcionan una última línea de defensa cuando fallan otras medidas de seguridad, por lo que es fundamental que la infraestructura de TI esté actualizada y el personal esté capacitado para reconocer las amenazas

- Los sistemas actualizados proporcionan una última línea de defensa cuando fallan otras medidas de seguridad. Después de que se lanza un parche de software, los cibercriminales pueden estar listos para explotar sistemas no parcheados en menos de 24 horas.
- Las siguientes **mejores prácticas** pueden ayudar a mantener los sistemas actualizados:
  - Educar a los empleados sobre los peligros de los sistemas y software obsoletos
  - Limitar la cantidad de sistemas que utilizan software de uso frecuente como JAVA, Flash y los complementos del navegador
  - Usar software o servicios de administración de parches y actualización de TI para la implementación masiva de actualizaciones
  - Habilitar la aplicación automática de parches a los activos de TI cuando sea posible
  - Servicio de redes separadas Traiga su propio dispositivo (BYOD) de las redes críticas del sistema
  - Supervisar continuamente la infraestructura de los sistemas que están desactualizados
- Para mitigar los riesgos, es aconsejable aplicar un parche a un sistema de prueba cargado con las aplicaciones críticas de su organización y verificar que nada se rompa durante o después del proceso de actualización antes de enviar el parche al entorno de producción

Fuente: Experts Explain Why Software Patching is Key for Your Online Security (Zaharia, 2016)

Mantener actualizados tanto los recursos humanos capacitados como la infraestructura de TI es fundamental - los sistemas actualizados proporcionan una última línea de defensa cuando fallan otras medidas de seguridad

Buenas prácticas en seguridad cibernética para tecnologías de energías renovables (3/4)

Gestión de acceso

El acceso a sistemas y datos confidenciales debe gestionarse adecuadamente

- Una reciente encuesta del sector energético del NIST revela que las **responsabilidades de gestión de identidad y acceso** (IdAM) a menudo son **descentralizadas y desorganizadas** dentro de las compañías energéticas. Esto crea dificultades para mantener el control de acceso sobre los sistemas internos y expone a las empresas a mayores riesgos de seguridad.
- El control de acceso efectivo requiere que los administradores tengan una visión general centralizada de todas las políticas de acceso actuales. Los administradores requieren la capacidad de otorgar o restringir rápidamente el acceso en respuesta a un entorno dinámico. Los empleados deben tener acceso suficiente para realizar su trabajo, nada más.
- La política de control de acceso puede basarse en numerosos modelos que incluyen entre otros:
  - Control de acceso basado en atributos (ABAC)
  - Control de acceso discrecional (DAC)
  - Control de acceso basado en identidad (IBAC)
  - Control de acceso basado en organizaciones (OrBAC)
  - Control de acceso basado en roles (RBAC)

Fuente: Identity and Access Management for Electric Utilities (NIST, 2015)

Los ataques no se limitan a piratear a terceros, pueden también ocurrir internamente: los nombres de usuario y las contraseñas de los sistemas de control y monitoreo deben cambiarse y los niveles de acceso deben revisarse periódicamente y reasignarse cuando un empleado abandona la empresa

Buenas prácticas en seguridad cibernética para tecnologías de energías renovables (4/4)

Detección avanzada

Las nuevas herramientas, incluida la inteligencia artificial y el aprendizaje automático, pueden ayudar a mantener una sólida seguridad a medida que los ciberataques y los entornos operativos se vuelven más complejos

- La mayor adopción de herramientas de **inteligencia artificial** (IA) y **aprendizaje automático** (ML) está revolucionando varias industrias. Muchos intentar aprovechar alguna forma de AI / ML para analizar la entrada y predecir la salida deseada.
- AI "aprender a leer" Big Data, las computadoras pueden crear algoritmos útiles basados en miles de millones de casos de prueba
- Por ejemplo, la versión 2015 de CylancePROTECT (una compañía que aprovecha AI / ML en sus soluciones de seguridad de punto final) puede detectar y prevenir tanto GoldenEye (lanzada en 2016) como WannaCry ransomware (lanzada en 2017) antes de que puedan ejecutarse
- Esto indica que los sistemas de seguridad automatizados e inteligentes de AI / ML ofrecerán las mejores soluciones a medida que los ciberataques y los entornos operativos se vuelvan más complejos
- Una ventaja adicional es que la prevención predictiva puede crear un **"espacio para respirar"** durante el cual se pueden planear y extender los parches al tiempo que se mantiene una postura de seguridad sólida

Fuente: Petya Returns as Goldeneye Strikes Germany, (Cylance, 2016)
26 TITAN SI Tests: WannaCry Ransomware vs. 8 AV solutions, (Yong, 2017))

Dentro del sector de la seguridad, las empresas innovadoras han aprovechado el poder predictivo de AI / ML para combatir las amenazas informáticas actuales y futuras

La hoja de ruta para futuros proyectos en ciberseguridad pasa por mantener una adecuada segmentación y mejorar los inseguros protocolos típicos de los sistemas SCADA

21 pasos para mejorar la ciberseguridad de las redes SCADA

- Identificar todas las **conexiones** a redes SCADA
- Desconecte las **conexiones innecesarias** a la red SCADA
- Evaluar y fortalecer la seguridad de cualquier conexión restante a la red SCADA
- Mejore las redes SCADA **eliminando** o deshabilitando **servicios innecesarios**
- No confíe en protocolos propietarios para proteger su sistema
- Implementar las características de seguridad provistas por los vendedores de dispositivos y sistemas
- Establezca controles fuertes sobre cualquier medio que se use como **puerta trasera** en la red SCADA
- Implementar sistemas de detección de intrusos internos y externos y establecer un **monitoreo de incidentes** las **24 horas del día**
- Realice **auditorías técnicas** de dispositivos y redes SCADA, y de cualquier otra red conectada, para identificar problemas de seguridad
- Realice encuestas de seguridad física y evalúe todos los **sitios remotos conectados a la red SCADA** para evaluar su seguridad
- Establecer *SCADA "Equipos Rojos"* para identificar y evaluar posibles escenarios de ataque
- **Definir** claramente los **roles**, responsabilidades y autoridades de seguridad cibernética para los gerentes, administradores del sistema y usuarios
- Documente la arquitectura de la red e identifique los sistemas que sirven para **funciones críticas** o que contienen información confidencial que requiere niveles adicionales de protección
- Establecer un proceso de **gestión de riesgos** riguroso y continuo
- Establecer una estrategia de protección de red basada en el principio de **defensa en profundidad**
- Identificar claramente los requisitos de seguridad cibernética
- Establecer procesos de gestión de configuración efectivos
- Llevar a cabo **autoevaluaciones de rutina**
- Establecer **copias de seguridad** del sistema y **planes de recuperación** ante desastres
- El liderazgo organizacional superior debe establecer expectativas para el desempeño de seguridad cibernética y responsabilizar a las personas por su desempeño
- **Establecer políticas** y realizar **capacitación** para minimizar la probabilidad de que el personal revelará involuntariamente información sensible sobre el diseño del sistema SCADA, las operaciones o los controles de seguridad

La adopción de buenas prácticas, normas y estándares constituyen una hoja de ruta de gran valor, pero el desafío a la hora de aplicarlas es la transformación del “qué hacer” al “cómo hacerlo”

minsait by Indra

impact to go

Eduardo Inchaurza
einchaurza@minsait.com

Lourdes Garrote
lgarrote@minsait.com

Henao, 4, 4ºA
48009 Bilbao
Spain

T +34 944 818 561
F +34 944 240 752
www.minsait.com