CyberGEN

Plan de Ciberseguridad IESE

Contenido

1. Introducción

CyberGEN es el plan de transformación de dos años de duración para reforzar la ciberseguridad OT de las instalaciones de generación de IESE (Iberdrola Energía Sostenible España): parques eólicos, plantas fotovoltaicas, baterías, centrales hidráulicas/bombeos, ciclos combinados, instalaciones de hidrógeno verde y centrales nucleares. Su finalidad es proteger las infraestructuras, reducir el riesgo cibernético y reforzar la continuidad operativa y la resiliencia energética.

2. Situación actual

El sector energético se apoya en infraestructuras industriales y redes de comunicación concebidas para garantizar una generación eficiente y fiable. La evolución de estas instalaciones exige complementar su desarrollo con medidas de protección capaces de responder a los retos actuales y futuros.

La digitalización ha incrementado la conectividad y, con ella, la exposición de los entornos industriales a amenazas cibernéticas. Los accesos remotos, la participación de proveedores y la convergencia IT/OT amplían la superficie de ataque de las instalaciones de generación.


BBC

Iran-linked hackers behind cyber attack that shut down power plant, reports say

Fuente: BBC-23/08/2026


EL ESPAÑOL

Apagón nacional en Polonia: Rusia lanzó un ciberataque masivo para dejar al país sin luz ni calefacción en Nochevieja

Fuente: El Español 20/11/2025

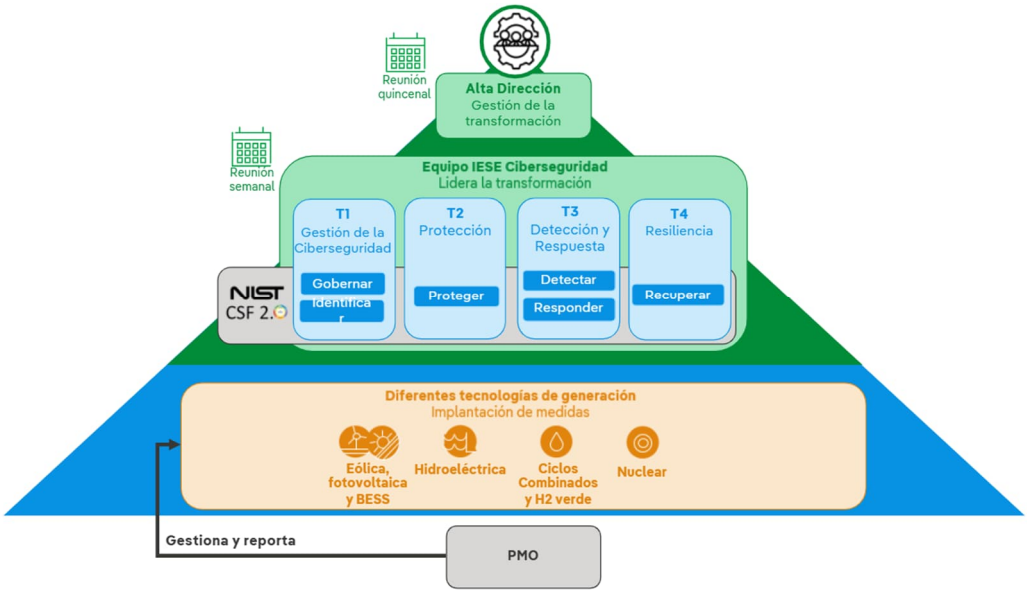
Las plantas operan con tecnologías, arquitecturas y fabricantes diversos. Un incidente en estos sistemas puede afectar a la operación, generar pérdidas económicas y, especialmente, comprometer la seguridad de las personas.

A este contexto se suma una mayor exigencia regulatoria y de protección de infraestructuras críticas. CyberGEN responde a esta necesidad mediante capacidades de prevención, detección, respuesta y recuperación orientadas a preservar la continuidad del negocio y la resiliencia de los activos energéticos.

NIS2 Network & Information Systems Directive

Information Security Management ISO 27001 Certified

3. Plan de transformación



CyberGEN, con horizonte 2025-2027, establece un modelo integral de ciberseguridad para las distintas tecnologías de generación. El plan articula una estrategia común en torno a cuatro pilares: gobierno y gestión de la ciberseguridad, protección de activos, detección y respuesta ante incidentes, y resiliencia.

El foco del plan se centra en la implantación de herramientas de ciberseguridad y en una gestión del riesgo que permita priorizar las actuaciones con mayor impacto. En este marco, los principales objetivos son:

- Implantar herramientas de ciberseguridad en las instalaciones, como firewalls, IDS y plataformas SIEM.
- Desplegar el Centro de Operaciones de Seguridad (SOC).
- Completar el inventario de activos de todas las plantas.
- Certificar los principales procesos de ciberseguridad conforme a la norma ISO/IEC 27001.

3.1. Gobierno y gestión de la ciberseguridad

Uno de los objetivos prioritarios de CyberGEN es preparar a IESE para afrontar las nuevas exigencias regulatorias en materia de ciberseguridad. El plan permite anticipar y abordar los requisitos de la Directiva NIS2 y del Código de Red de Ciberseguridad del sector eléctrico (NCCS), reforzando el gobierno, la gestión de riesgos, la protección, la supervisión, la notificación y la respuesta ante incidentes. Asimismo, CyberGEN incluye la implantación del sistema de gestión de la seguridad de la información y la obtención de la certificación ISO/IEC 27001, como base para estructurar los procesos, acreditar su aplicación y consolidar la mejora continua.

3.2. Identificación y protección de activos

La identificación y categorización de instalaciones, procesos y activos proporciona una visión clara de qué debe protegerse, cómo se protege y qué mejoras deben abordarse.

El aumento de las capacidades de protección de activos y sistemas es esencial para mejorar la ciberseguridad. Entre las actuaciones clave se incluyen:

- Revisión de las arquitecturas de los sistemas OT y mejora del aislamiento y la segmentación de las redes de las instalaciones.
- Revisión de los accesos de terceros, implantación de autenticación multifactor (MFA) y uso de soluciones de acceso seguro, como la gestión de accesos privilegiados (PAM).
- Implantación de soluciones de protección y detección de malware, como Endpoint Protection o EDR.

3.3. Detección y respuesta ante incidentes

Las soluciones de monitorización OT permiten conocer lo que sucede en los entornos industriales y mejorar la capacidad de detección. Entre las medidas previstas se encuentran la instalación de sistemas IDS y la implantación de plataformas SIEM/SOAR que centralicen los eventos y las alarmas de los sistemas OT.

Los simulacros y ejercicios impulsados por CyberGEN preparan a los equipos para responder con rapidez y coordinación ante posibles incidentes.

3.4. Resiliencia

La resiliencia completa el modelo mediante medidas destinadas a mantener o recuperar la operación ante situaciones adversas, protegiendo la prestación de un servicio esencial para la sociedad.

4. Valores de CyberGEN

4.1. Oficina de Ciberseguridad

CyberGEN se articula en torno a una Oficina de Ciberseguridad con autoridad y respaldo de la dirección y, por tanto, con capacidad para definir, coordinar y supervisar los procesos de ciberseguridad OT. El respaldo de la dirección facilita la priorización, la asignación de recursos y la adopción de las medidas necesarias para proteger los entornos de generación.

4.2. Visión y gestión del riesgo como eje principal

La gestión del riesgo orienta las decisiones del plan. Identificar, evaluar y priorizar amenazas permite concentrar los esfuerzos en las iniciativas con mayor impacto y mantener la actuación alineada con las necesidades del negocio.

4.3. Homogeneidad para la heterogeneidad

CyberGEN establece un marco común para tecnologías de generación con características y necesidades diferentes. Este enfoque permite aplicar criterios homogéneos sin perder de vista las particularidades de cada entorno.

4.4. Pensamiento global, ejecución local

La estrategia y la coordinación se gestionan de forma centralizada, mientras que la implantación se adapta a la realidad de más de 400 plantas distribuidas por el territorio. Los centros de control y los equipos operativos desempeñan un papel esencial en su ejecución local.

4.5. Mejora continua como principio de evolución

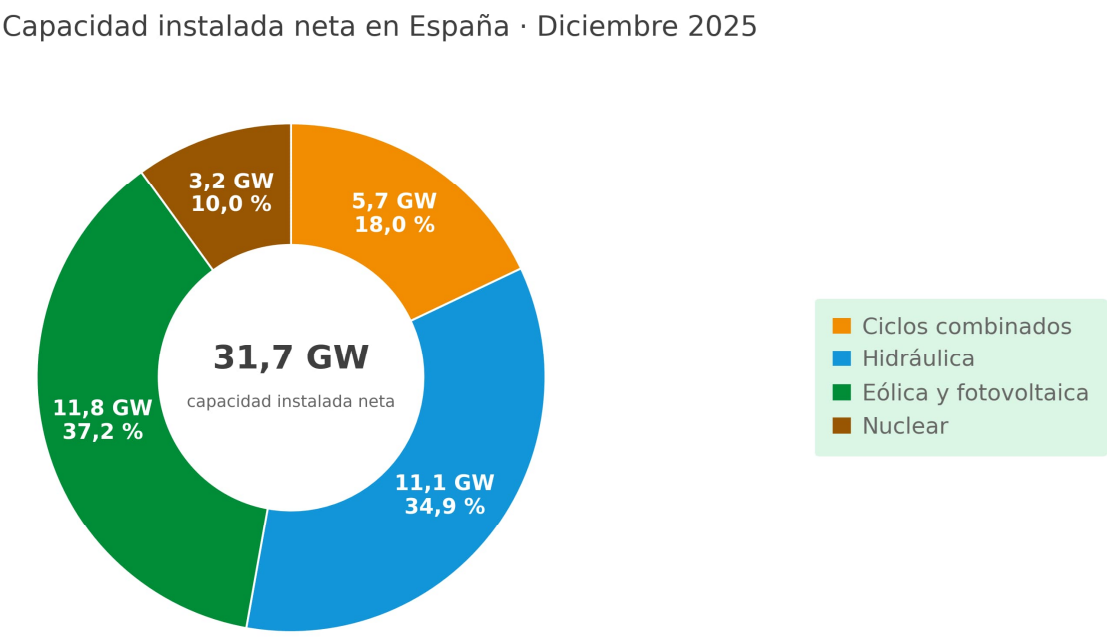
Los procesos de ciberseguridad se revisan y mejoran de forma periódica. Este enfoque permite incorporar lecciones aprendidas, adaptarse a nuevas amenazas y mantener la capacidad de respuesta ante un entorno tecnológico en evolución.

5. Indicadores de éxito

- Más de 400 instalaciones protegidas en todo el territorio español.

- Cobertura de las principales tecnologías de generación:
  - Eólica, fotovoltaica y BESS.
  - Hidráulica.
  - Ciclos combinados y plantas industriales.
  - Nuclear.

- 31,7 GW de generación protegida.



- Incremento del 30 % en el nivel de madurez, de acuerdo con los criterios del NIST CSF 2.0.