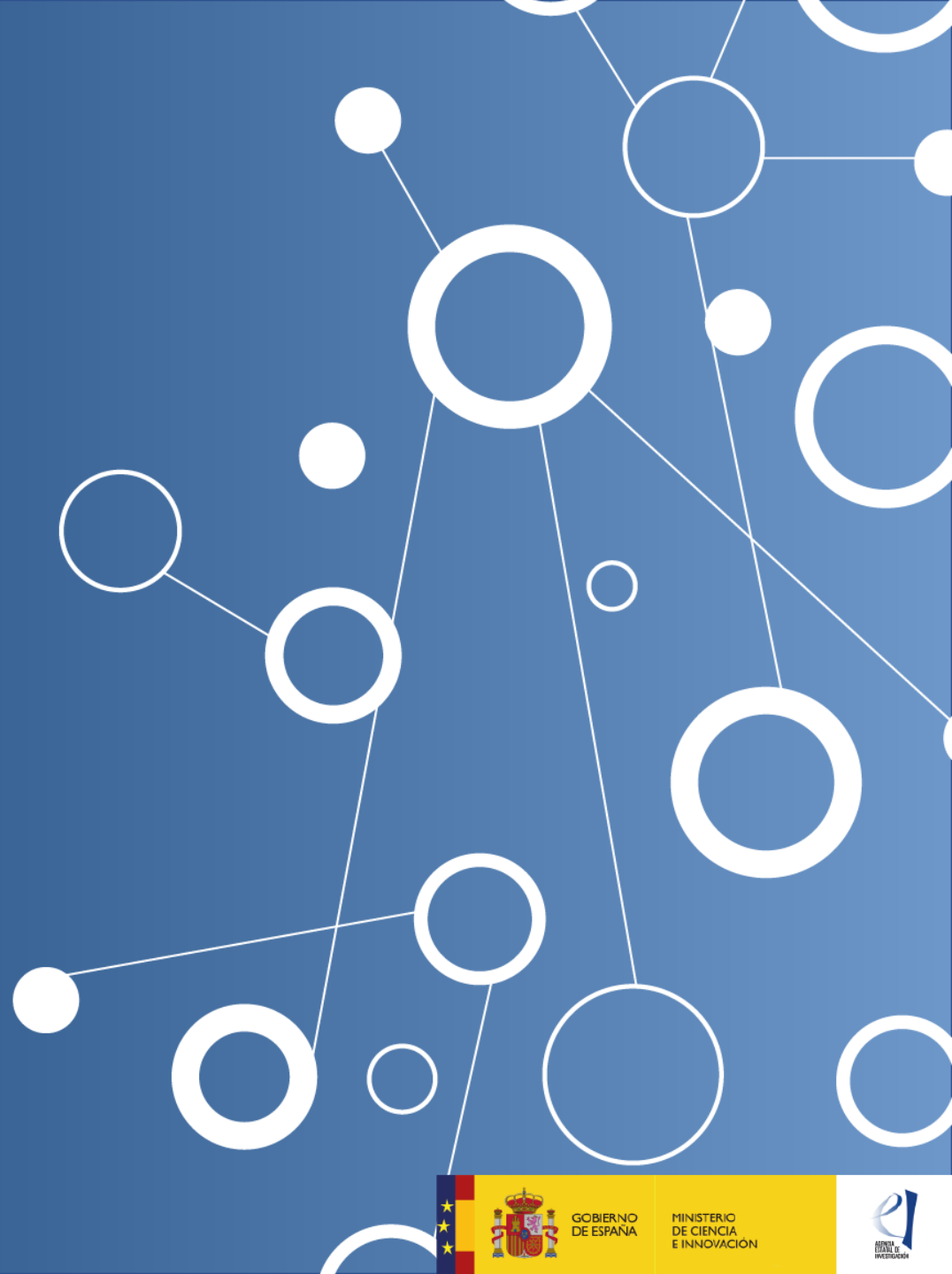
Presentación de resultados

- Almacenamiento
- Ciberseguridad

FUTURED – PLATAFORMA ESPAÑOLA DE REDES ELÉCTRICAS

Madrid, 4 de febrero de 2026
Agencia Estatal de Investigación
C/ de Torrelaguna, 58, Cdad. Lineal, 28027 Madrid

FutuRed



GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

Programa

11:25 – 12:10 Pausa café

12:10 – 14:00 – GT Ciberseguridad

12:10 - 13:00 Presentación del documento “Retos de los nuevos modelos de la Ciberseguridad en el sector eléctrico.”

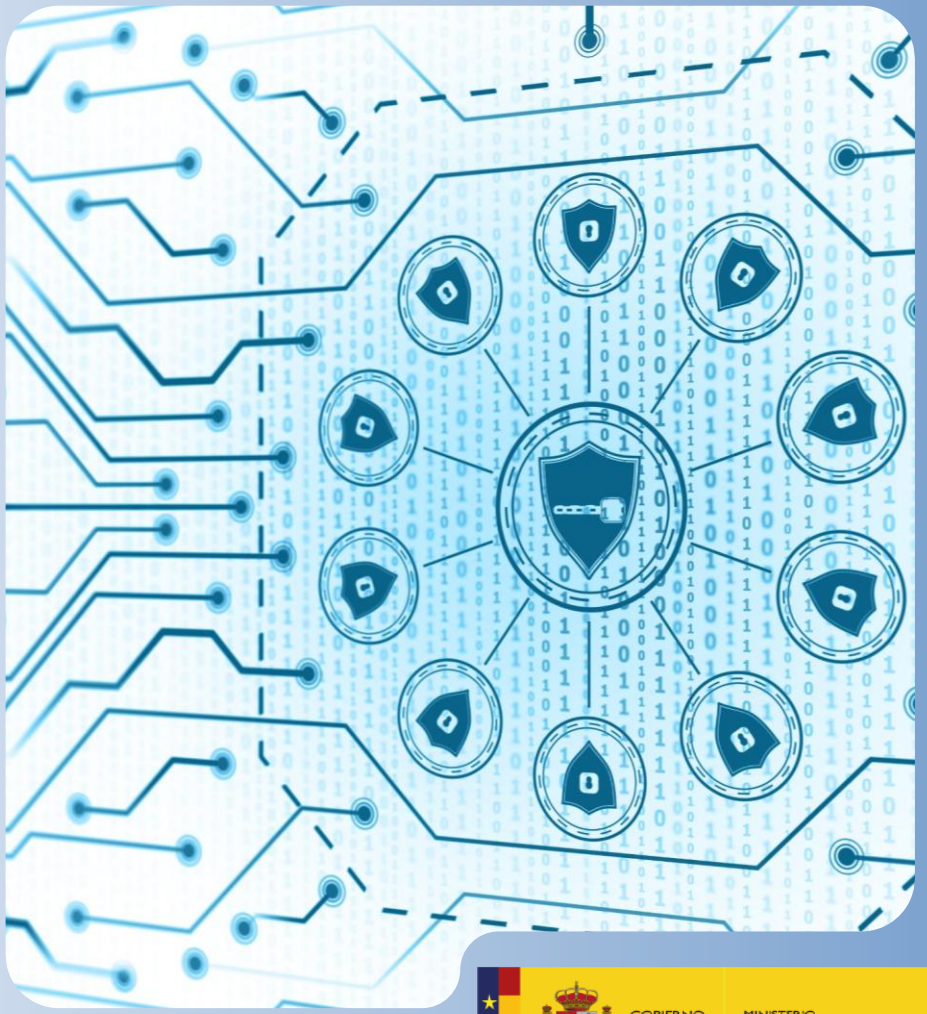
D. Iago Crespo. UFD
D. Luis Álvarez. Itelsis
D. Leonardo Hervás Hermida, Director General. CIDE
D. Miguel Ángel Sánchez Rodríguez. Arteche

13:00 - 14:00 – Mesa redonda

Modera: Francisco Ramírez. Naturgy
D. Carlos García Fernández, Sub. Adjunto de la Sub. de Energía Eléctrica CNMC
D. Mikel Vergara. Tecnalia
D. Ramón Gallart. ASEME
D. Ian Gallardo. Ormazábal

Grupo de trabajo de Ciberseguridad

Retos de los nuevos modelos de Ciberseguridad en el sector eléctrico



FutuRed

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

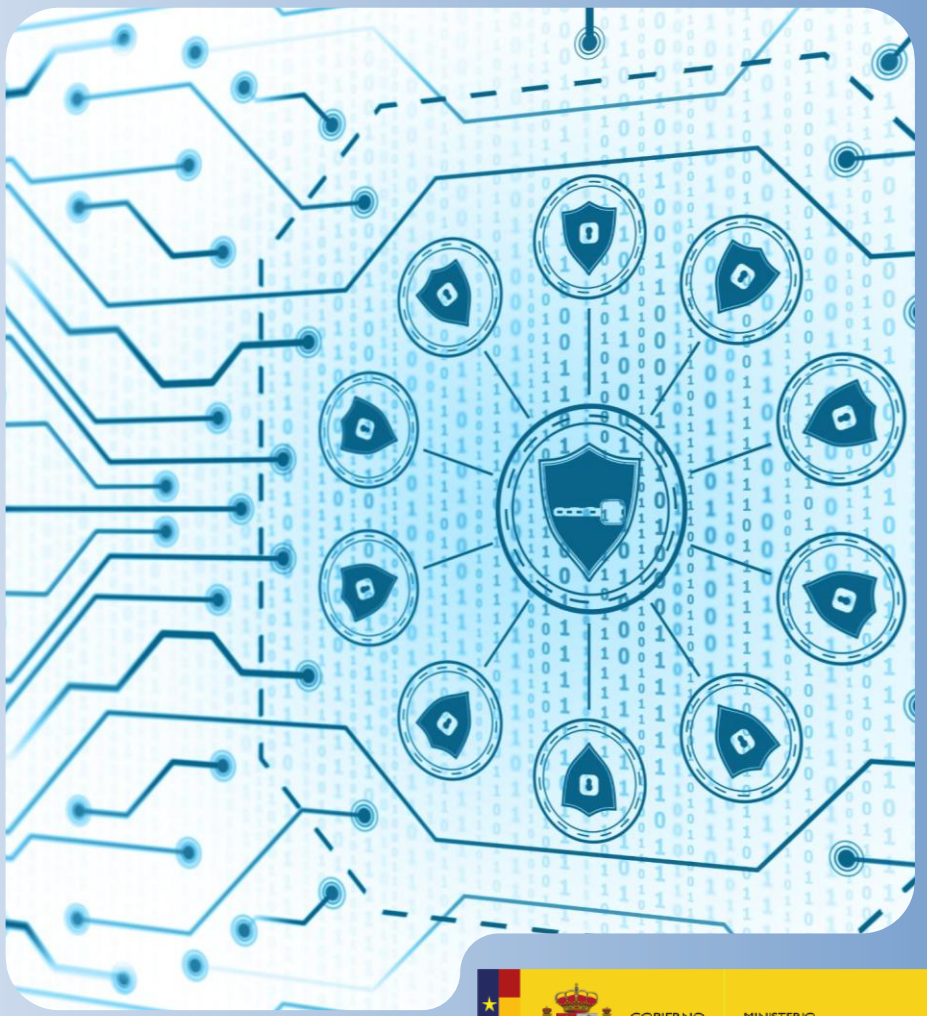
Grupo de trabajo de Ciberseguridad

Retos de los nuevos modelos de Ciberseguridad en el sector eléctrico

INTRODUCCIÓN

D. Iago Crespo Taboada

ufd
Grupo Naturgy



FutuRed

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

Introducción: Transición energética y digitalización

Transformación digital del sector eléctrico

- Digitalización acelerada como parte clave de la transición energética.
- Integración masiva de tecnologías emergentes: IoT, IA, cloud, contadores inteligentes, redes 5G.
- Aumento drástico de datos generados, gestionados y compartidos a través de aplicaciones y dispositivos.
- Reducción de costes operativos y aumento de eficiencia, pero también incremento de superficie de ataque, que generan nuevos riesgos adicionales.
- Cooperación sectorial

FutuRed

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN

Introducción: Nuevas amenazas, mayor exposición

- Complejidad y vulnerabilidad
  - Mayor interconexión → Mayor exposición → Aumento de vulnerabilidades
  - Aumento de incidentes a nivel global y profesionalización del ciberdelito: ransomware, phishing, APT.

- Amenazas digitales complejas:
  - Impacto geopolítico sobre infraestructuras críticas.
  - Los ataques ya no son aislados: ecosistema criminal organizado.

FutuRed

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

Introducción: Impulso regulatorio

- Nuevo paradigma regulatorio:
  - UE como líder en regulación: NIS2, Directiva de Resiliencia, Reglamento CRA, GDPR, NCCS.
  - Búsqueda de armonización, resiliencia y protección de infraestructuras esenciales.

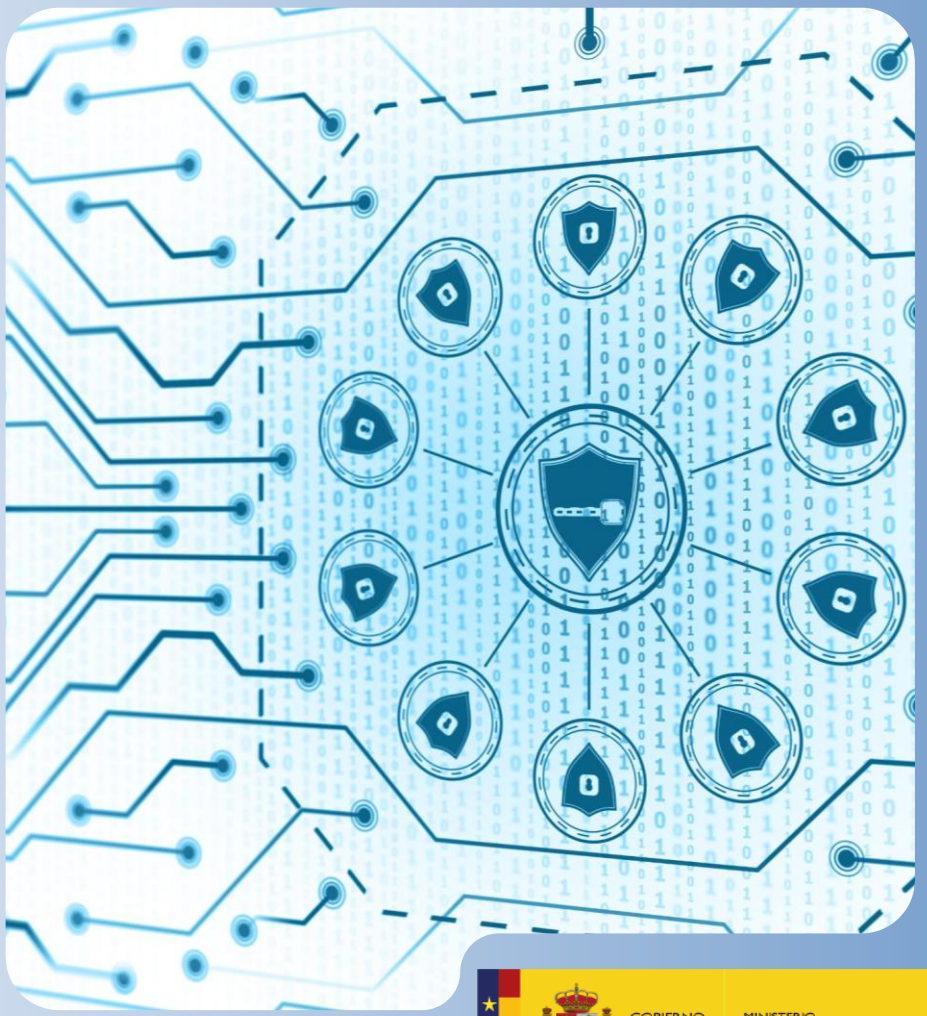
- Gobernanza:
  - La ciberseguridad es una prioridad en la alta dirección.
  - Gestión de riesgos, cumplimiento y resiliencia, con la eficiencia en las propias operaciones de la distribución:
    - Anticipar riesgos derivados de la innovación y la hiperconectividad
  - La regulación como motor de inversión, madurez y estandarización en ciberseguridad con foco la resiliencia.

Grupo de trabajo de Ciberseguridad

Retos de los nuevos modelos de Ciberseguridad en el sector eléctrico

Distribuidoras. Enfoque

D. Leonardo Hervás Hermida



FutuRed

cide

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

El sistema eléctrico ha cambiado

La red eléctrica ya no es un sistema aislado ni unidireccional.

- **De red cerrada → a ecosistema conectado**
- **De operación aislada → a integración IT–OT**
- **De pocos actores → a múltiples agentes**

Más agentes, más decisiones, más riesgo

La complejidad del sistema multiplica el riesgo.

Red interactiva, decisiones distribuidas

- **Generadores**
- **Autoconsumidores**
- **Agregadores**
- **Vehículos eléctricos**
- **Baterías**

Convergencia IT–OT: el nuevo perímetro

El principal cambio no es la amenaza, es el perímetro.

El riesgo ya no está donde estaba antes

- **Interconexión IT–OT**
- **SCADA, Historians, cloud**
- **Accesos remotos**
- **Telemedida e IoT**

Impacto sistémico y económico

La distribución eléctrica es una infraestructura sistémica.

- **Electrificación del transporte**
- **Dependencia de servicios esenciales**
- **Nuevos modelos de negocio**

Qué deben hacer las empresas

Esto exige gestión real del riesgo.

El sector **sabe lo que hay que hacer** y es responsable

- **Factor humano**
- **Cadena de suministro**
- **Sistemas legacy**
- **IT–OT**
- **Capacitación**
- **Herramientas y procedimientos**
- **Zero Trust**
- **Gobernanza IT–OT**
- **Preparación para incidentes**

El papel clave del regulador

La ciberseguridad exige un marco claro…

No es solo un problema empresarial

- **Negocio 100 % regulado**
- **Marco claro**
- **Retribución alineada**
- **OPEX y márgenes importan**
- **Evitar incentivos perversos**

y capacidad para entenderlo

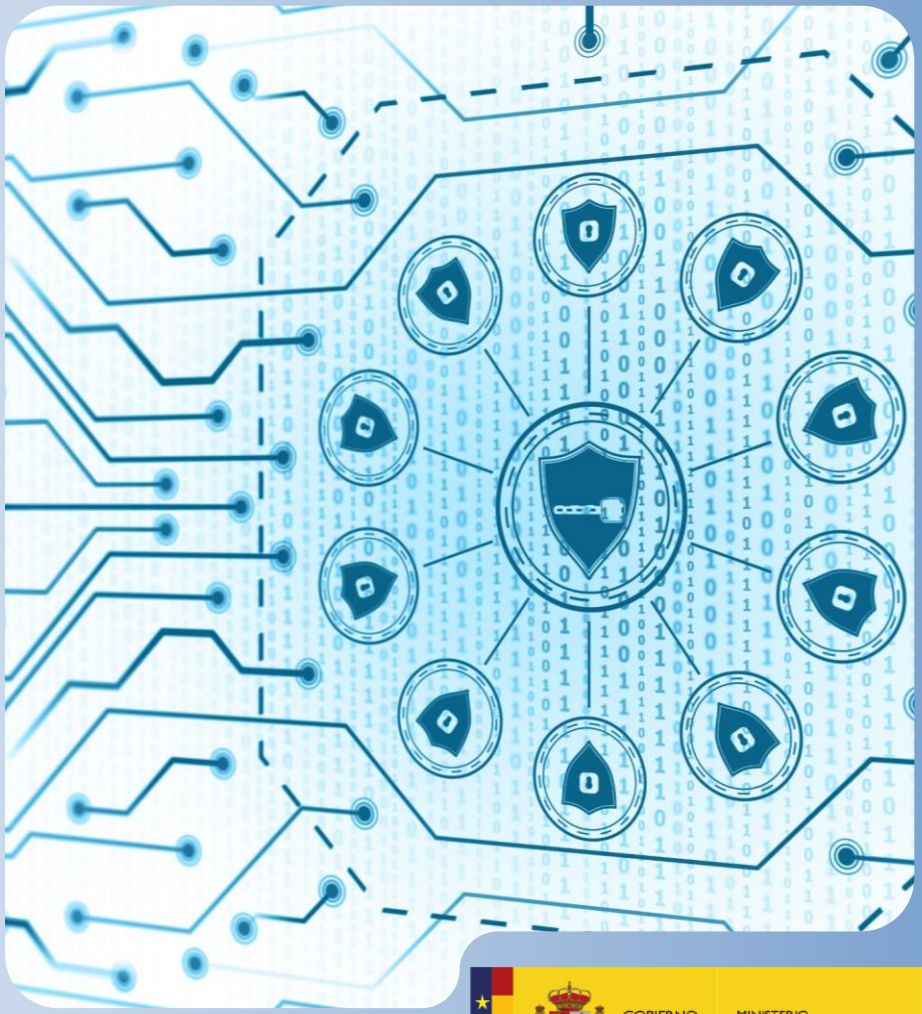
El regulador requiere también recursos especializados

Grupo de trabajo de Ciberseguridad

Retos de los nuevos modelos de Ciberseguridad en el sector eléctrico

Fabricantes e Integradores

D. Miguel Ángel Sánchez Rodríguez



arteche

FutuRed

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

Enfoque Fabricantes e Integradores

Ciberseguridad durante todo el ciclo de vida de los productos

¿Qué comprende el ciclo de vida?

Idea/necesidad -> Diseño y Desarrollo -> Pruebas -> Despliegue -> Operación -> Mantenimiento -> Retirada

Requiere acciones en:

- Proceso de desarrollo
- Proceso de operación y mantenimiento
- Producto
- Cadena de suministro.

Enfoque Fabricantes e Integradores

Ciberseguridad en proceso de desarrollo de componentes

- Ciberseguridad desde las etapas más tempranas, alineado con IEC 62443-4-1 y CRA
- Diseño y desarrollo seguro: Bastionado, Theat Model, análisis de seguridad del código, vulnerabilidades terceros
- Pruebas específicas de ciberseguridad: Basadas en riesgos y Pruebas de Intrusión.

Enfoque Fabricantes e Integradores

Requisitos tecnológicos de producto y certificaciones

- Estándares clave:
  - IEC 62351 para seguridad de protocolos en sector eléctrico.
  - IEC 62443 para sistemas y componentes industriales.
  - Certificación CRA para productos con elementos digitales.

- Requisitos: Control de acceso, Integridad, Confidencialidad, Flujos de datos restringidos, respuesta a eventos, disponibilidad

- Integración de secure elements en los dispositivos, como TPM, criptochips, HSM.

- Protocolos seguros en comunicaciones y monitorización (ej.: TLS, SNMPv3).

Enfoque Fabricantes e Integradores

Gestión de la cadena de suministro

- Normativas como NIS2, IEC 62443 requieren gestión de riesgos de fabricantes e integradores.
- Evaluación y auditoría de **procesos** de fabricantes e integradores como parte crítica del riesgo del operador.
- Auditorías, pruebas de intrusión y validación de conformidad de los **productos**.
- **Colaboración e intercambio de información** entre actores de la cadena de valor para resiliencia eficaz.

Enfoque Fabricantes e Integradores

Impacto económico para fabricantes/integradores

- Fuertes inversiones, y en aumento:
  - Cambio de procesos internos y cultura
  - Nuevos perfiles altamente especializados, escasos (ciberseguridad industrial - OT)
  - Formación particularizada y soporte a toda la plantilla
  - Diseño y desarrollo seguro: más esfuerzo horas y herramientas
  - Pruebas y certificaciones
  - Mantenimiento

No es opcional:

- Ventaja competitiva mediante cumplimiento regulatorio, calidad y seguridad del producto.

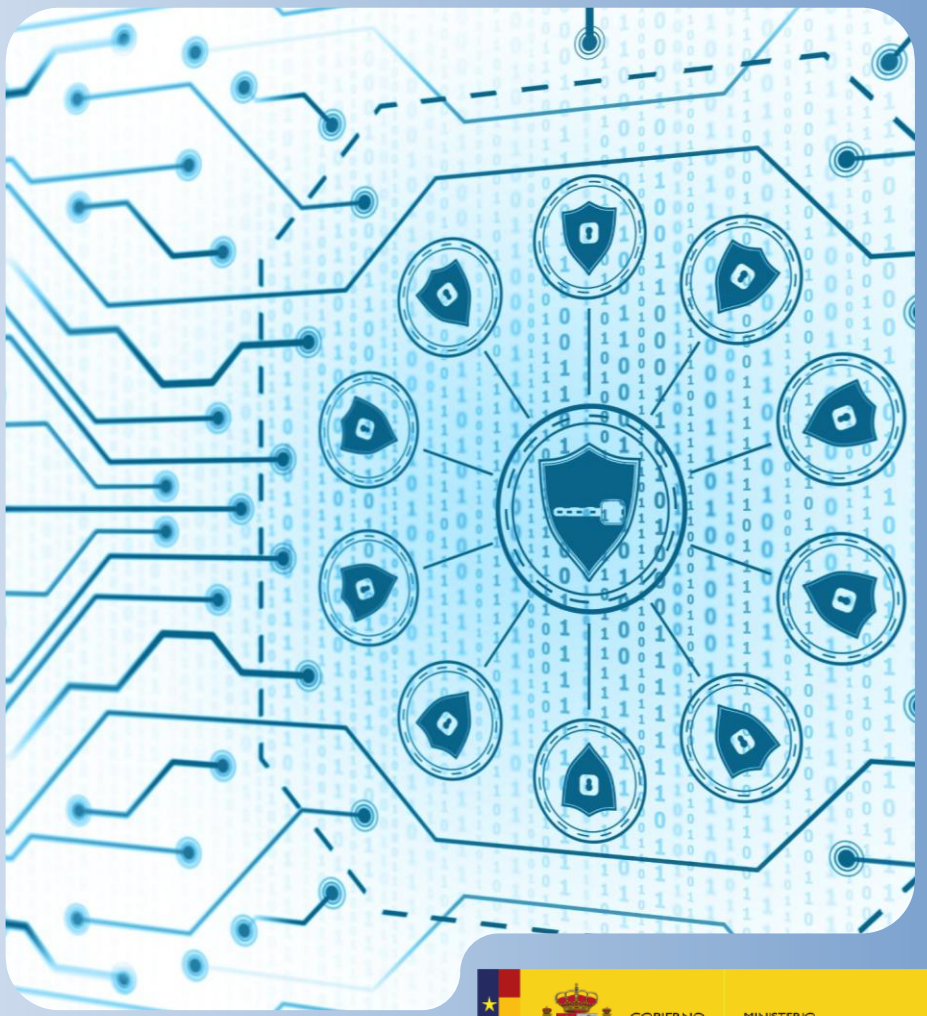
- Exigencia del mercado que empresas y productos cumplan normativas y requisitos del sector energético.

Grupo de trabajo de Ciberseguridad

Retos de los nuevos modelos de Ciberseguridad en el sector eléctrico

Conclusiones

D. Luis Álvarez Patiño



FutuRed

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN


Ciberseguridad: base de la transformación del sector eléctrico
• Digitalización acelerada del sistema eléctrico
• Más eficiencia → Más interconexión → Más exposición
• Amenazas crecientes y profesionalizadas
• Ciberseguridad = continuidad de suministro
La transición energética solo es viable
con una base sólida de ciberseguridad

De proyectos puntuales a inversión sostenible

- **La ciberseguridad** es un proceso continuo
- **OPEX estructural**, no solo **CAPEX**
- **Monitorización**, actualización, respuesta, mejora
- **Reconocimiento del TOTEX** en ciberseguridad

Sin modelo económico sostenible no hay resiliencia real


Un ecosistema interdependiente
Security by Design
Cadena de suministro segura
Fabricantes
Distribuidoras
Integradores
Proveedores
Regulador
Auditorias y certificaciones
Intercambio de información
La cadena es tan fuerte como su eslabón màs débil

FutuRed

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

FutuRed

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

Apuntes finales

La digitalización demanda ciberseguridad.

La ciberseguridad
implica continuidad de negocio y suministro.

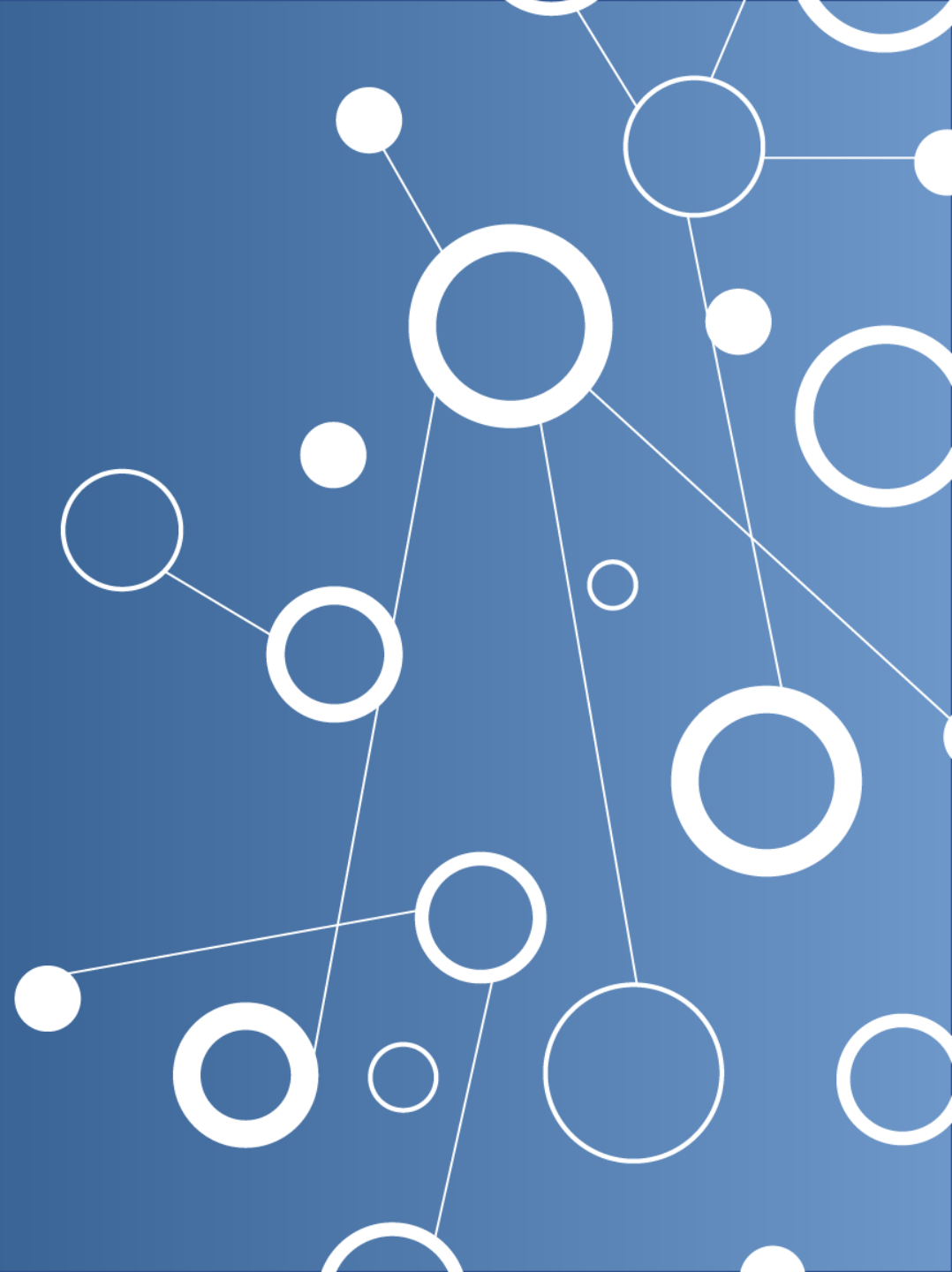
Invertir de forma planificada
es siempre más barato qué reaccionar.

La resiliencia del sector depende de todos.

FutuRed

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

Muchas gracias por su atención



FutuRed