Informe "El Reto" enerTIC

NIS2 en infraestructuras críticas: el reto de las energéticas y utilities

enerTIC

Septiembre 2025

Sumario

Resumen ejecutivo

La creciente digitalización del sector energético y de utilities ha traído consigo una transformación sin precedentes en la forma de operar, controlar y supervisar infraestructuras críticas. Sin embargo, este avance también ha multiplicado la superficie de exposición ante amenazas cibernéticas cada vez más sofisticadas, persistentes y con potencial de impacto sistémico. En este escenario, la directiva europea NIS2 no llega como un simple ajuste normativo, sino como una palanca de cambio estructural: redefine responsabilidades, endurece exigencias y sitúa la ciberseguridad en el corazón de la resiliencia operativa.

Este informe parte de una constatación clave: muchas organizaciones del sector necesitan apoyo para traducir la norma a su realidad concreta. No basta con conocer la directiva: hay que comprender qué implica en términos de estrategia, organización, tecnología y cultura. NIS2 no puede afrontarse como un ejercicio reactivo ni como una simple auditoría. Exige decisiones valientes, inversiones con sentido y, sobre todo, una nueva forma de pensar y gobernar la ciberseguridad.

Con este objetivo, el informe desarrolla un **decálogo de recomendaciones y reflexiones** que sintetiza las claves para afrontar con garantías el nuevo marco regulatorio. Desde el cambio de mentalidad necesario en la alta dirección, hasta la adaptación de estructuras internas, la gestión del Shadow IT, la interoperabilidad de entornos OT o la redefinición del rol de los terceros, cada punto ha sido diseñado para aportar valor real, práctico y replicable. No se trata de una receta genérica, sino de una hoja de ruta construida desde el conocimiento técnico y el entendimiento del contexto energético actual.

El informe no solo ayuda a **cumplir la normativa**, sino que muestra cómo la aplicación de estas recomendaciones puede traducirse en beneficios tangibles: anticipación ante amenazas, madurez organizativa, reducción de costes de gestión, mejora de la supervisión, automatización de respuestas, y mayor confianza en el ecosistema operativo y regulador. Las organizaciones que adopten un enfoque proactivo no solo evitarán sanciones o incidentes, sino que estarán mejor posicionadas para liderar en un entorno cada vez más exigente.

Además del decálogo, el informe incluye un bloque de **resultados esperados** que permite visibilizar el impacto operativo y estratégico de aplicar sus recomendaciones, y un anexo con los **marcos normativos y técnicos** fundamentales —como la propia NIS2, el ENS, IEC 62443 o ISO 27001— que ofrecen referencias sólidas para guiar su implementación.

En definitiva, este documento aspira a ser una guía para actuar antes de que lo exija la urgencia, y para convertir el cumplimiento en una oportunidad de mejora. Porque en un sector donde la continuidad del servicio, la confianza de la ciudadanía y la estabilidad de los sistemas dependen cada vez más de la seguridad digital, prepararse no es solo una obligación: es un imperativo estratégico.

Reconocimientos

Este informe ha sido posible gracias a la colaboración de los miembros del Comité y de su Presidente, cuya experiencia y compromiso han enriquecido el análisis y las conclusiones aquí presentadas.

COMITÉ DE EXPERTOS DE INNOVACIÓN PARA LA EFICIENCIA EN INFRAESTRUCTURAS IT DEL SECTOR ENERGÉTICO

Presidente

Claudio Fernández López
BABEL

Miembros titulares

Andoni Saiz Alvaro
AYESA

Gonzalo Valle
IFS

Pedro Puche
SAS

Ignacio Moreno Arias
TELESPAZIO IBÉRICA

Jhon Medina
NTT DATA

Guillermo Viguera
CIC CONSULTING

Javier Mazo Torres
VASS

Jaime Pérez Pissarra
EXPERIS

Otros expertos participantes

Rafael Bolivarl
ENAGÁS

Introducción

La transformación digital del sector energético y de las utilities ha **supuesto enormes avances en eficiencia operativa, automatización de procesos y optimización del uso de los recursos**. La incorporación de tecnologías digitales en redes inteligentes, sistemas SCADA, plataformas de análisis de datos y dispositivos IoT ha permitido a las organizaciones ser más ágiles, sostenibles y competitivas. Gracias a estas herramientas, las compañías pueden mejorar la calidad del servicio, optimizar la gestión de la demanda y reducir su huella ambiental. Además, este proceso de modernización se alinea con los objetivos estratégicos de descarbonización y transición energética impulsados desde Europa.

Sin embargo, **esta progresiva digitalización también ha incrementado la superficie de exposición a ciberamenazas cada vez más complejas y persistentes**. A medida que crece la interconexión entre los entornos IT y OT, también lo hace la posibilidad de que un fallo de seguridad, una mala configuración o una brecha no detectada tenga consecuencias a gran escala. Los ataques ya no solo persiguen comprometer la confidencialidad de los datos, sino que buscan interferir en la operativa de los sistemas, alterar la disponibilidad del servicio o incluso causar daños físicos en infraestructuras críticas. La sofisticación de los atacantes y la profesionalización del cibercrimen exigen una respuesta igualmente avanzada, coordinada y proactiva.

Esta situación es especialmente preocupante en el contexto de un sector esencial como el energético, donde **cualquier interrupción del suministro puede tener efectos en cascada sobre la economía, los servicios públicos y la vida cotidiana** de millones de personas. Las redes eléctricas, los sistemas de control industrial y las infraestructuras de generación y distribución forman parte de un ecosistema complejo y heterogéneo, en el que conviven tecnologías de distinta generación, múltiples proveedores y una creciente presión para integrar nuevas capacidades digitales.

Frente a este panorama de riesgo, **las instituciones europeas han reforzado el marco regulatorio con la aprobación de la directiva NIS2**, que amplía significativamente el alcance y la exigencia respecto a su predecesora. Esta nueva normativa introduce requisitos más estrictos en materia de gobernanza, gestión de riesgos, control de la cadena de suministro y respuesta ante incidentes, además de establecer un régimen sancionador más severo. Aunque su transposición en España aún no se ha completado, se prevé su entrada en vigor antes de que finalice el año, sin contemplarse periodos de adaptación.

Energía y utilities no solo **son estratégicos: son esenciales e irremplazables para el funcionamiento de la sociedad**. En un escenario en el que la continuidad del negocio depende cada vez más de entornos digitales interconectados, garantizar la resiliencia frente a las ciberamenazas se convierte en una prioridad de primer orden. Cumplir con los nuevos marcos normativos ya no es solo una obligación legal: es una necesidad para asegurar la sostenibilidad operativa y la confianza de los ciudadanos, clientes y reguladores.

Identificación del reto

La directiva NIS2 supone un cambio de paradigma en la forma en que las organizaciones del sector energético y de utilities deben entender y gestionar la ciberseguridad. A diferencia de su predecesora, **NIS2 amplía notablemente el alcance tanto sectorial como funcional**, imponiendo requisitos más exigentes en ámbitos como la gobernanza, la gestión de riesgos, la supervisión de la cadena de suministro y la respuesta ante incidentes. En este nuevo marco, no solo están obligadas a cumplir las grandes compañías, sino también una parte importante del tejido empresarial que hasta ahora no se veía directamente afectada por este tipo de normativas.

Para muchas empresas, especialmente aquellas de menor tamaño o con menor madurez en materia de ciberseguridad, la adaptación a NIS2 representa un reto considerable. No se trata únicamente de ajustar procesos o actualizar documentación: **exige un cambio organizativo profundo, una revisión de las responsabilidades, una evaluación rigurosa de los riesgos y una estrategia clara para elevar los niveles de resiliencia** en entornos cada vez más digitalizados y expuestos. La gestión de activos, la interoperabilidad entre sistemas, la visibilidad sobre entornos OT y la concienciación del personal son solo algunos de los aspectos críticos que deben abordarse de forma inmediata y estructurada.

Además, **la urgencia es un factor clave**. Aunque la transposición de la directiva al ordenamiento jurídico español aún no se ha materializado, su entrada en vigor se espera antes de final de año y no contempla periodos transitorios. Esto significa que muchas organizaciones disponen de un margen de tiempo muy limitado para cumplir con todos los requisitos. No hacerlo no solo supone un incumplimiento legal: implica dejar desprotegidas infraestructuras esenciales y asumir un conjunto de riesgos que pueden comprometer la viabilidad del negocio.

Los riesgos derivados de no abordar este reto de forma adecuada son múltiples y, en muchos casos, acumulativos. A continuación, se enumeran los principales:

1. Riesgo de sanciones económicas y legales graves

- Multas de hasta 10 millones de euros o el 2% del volumen de negocio global anual.
- Posibilidad de imposición de medidas correctivas, suspensión de operaciones o retirada de licencias.

2. Riesgo de interrupción del servicio energético

- Un incidente de seguridad puede afectar la disponibilidad de la red, la distribución de energía o el funcionamiento de infraestructuras críticas.
- Esto puede derivar en cortes de suministro con impactos económicos, sociales y políticos.

3. Riesgo reputacional y pérdida de confianza

- La exposición mediática tras un incidente puede dañar la imagen de marca, afectar la relación con clientes y generar desconfianza entre los inversores.
- Las organizaciones que no cumplan con NIS2 serán percibidas como negligentes o poco fiables.

4. Riesgo de quedar fuera de la cadena de suministro

- Las grandes compañías del sector y las administraciones exigirán cumplimiento normativo a todos sus proveedores.
- No adaptarse puede significar perder contratos o no poder participar en licitaciones públicas.

5. Riesgo de obsolescencia tecnológica y organizativa

- La falta de adaptación impide evolucionar hacia modelos de gestión más resilientes y maduros.
- No revisar la gobernanza ni los procesos puede perpetuar malas prácticas e ineficiencias.

6. Riesgo de desalineación entre entornos IT y OT

- Sin una estrategia común, se mantienen silos organizativos y tecnológicos que dificultan la detección y respuesta ante incidentes.
- La falta de coordinación puede ser explotada por atacantes para escalar dentro de la organización.

7. Riesgo de brechas de seguridad no detectadas (Shadow IT y activos invisibles)

- Sin una gestión adecuada de activos, el riesgo de que existan dispositivos o software fuera del control del área de seguridad se multiplica.
- Esto crea puntos ciegos que pueden ser aprovechados para comprometer el sistema.

8. Riesgo de no identificar vulnerabilidades en la cadena de suministro

- La normativa obliga a evaluar también los riesgos derivados de terceros.
- Un proveedor débil en seguridad puede ser la puerta de entrada a todo el ecosistema.

9. Riesgo de no cumplir con los tiempos regulatorios

- La entrada en vigor será inminente y no se prevé un periodo de adaptación.
- Las empresas que no estén preparadas a tiempo tendrán muy difícil una reacción eficaz.

10. Riesgo de impactos acumulativos por falta de preparación

- Un incidente no gestionado puede desencadenar una cadena de consecuencias: caída del servicio, multas, pérdida de clientes, litigios, daño reputacional...
- La falta de una estrategia integrada agrava los efectos de cualquier fallo.

El panorama que se desprende de esta lista de riesgos no debe interpretarse como una alarma exagerada, sino como un **reflejo realista de las vulnerabilidades existentes en un sector estratégico**, que opera bajo una creciente dependencia digital y una presión normativa sin precedentes. La directiva NIS2 no solo incrementa las exigencias, sino que también deja más expuestas a las organizaciones que no actúen a tiempo: cualquier brecha, por pequeña que sea, puede tener consecuencias sistémicas en la continuidad del servicio y la confianza del mercado.

Además, la propia configuración del ecosistema energético y de las utilities, caracterizado por una alta interdependencia entre operadores, proveedores tecnológicos, integradores y terceros, **hace que el incumplimiento de uno solo de estos eslabones ponga en riesgo al conjunto**. No se trata únicamente de cumplir la ley, sino de contribuir de forma colectiva a la seguridad del sistema en su conjunto. La cadena es tan fuerte como su eslabón más débil, y NIS2 hace explícito que la responsabilidad no termina en el perímetro de la organización.

Por otro lado, el momento actual también representa una oportunidad para madurar. Abordar este reto permite profesionalizar la función de ciberseguridad, clarificar responsabilidades internas, alinear mejor IT y OT, e introducir prácticas que fortalecen la resiliencia de forma transversal. **Aunque el esfuerzo puede ser significativo, también lo es el beneficio**: organizaciones más preparadas, más confiables y más sostenibles en el tiempo.

Con esta perspectiva, el comité ha identificado una serie de recomendaciones clave que **buscan servir de guía para avanzar en la adaptación a NIS2**, especialmente para aquellas compañías —y sus proveedores— que todavía no han iniciado este camino o se encuentran en fases incipientes. Estas recomendaciones, agrupadas en forma de decálogo, no pretenden ser un checklist cerrado, sino una hoja de ruta práctica, flexible y orientada a la acción.

Reflexiones para afrontar la adaptación a NIS2

La adaptación a la directiva NIS2 no puede abordarse como un trámite administrativo ni como un ejercicio de cumplimiento aislado. Supone, en realidad, un proceso de transformación profunda que impacta en las estructuras de gobernanza, los modelos de gestión tecnológica, la cultura organizativa y la relación con los entornos externos, especialmente en un sector tan interconectado y crítico como el energético. En este contexto, el comité ha elaborado un conjunto de reflexiones técnicas que buscan aportar una visión realista, aplicada y útil para aquellas organizaciones que aún están construyendo su hoja de ruta frente a este nuevo marco normativo.

Este decálogo no pretende ser una guía cerrada ni un checklist estándar. Cada organización parte de un nivel de madurez distinto, opera con arquitecturas y restricciones específicas, y se enfrenta a realidades regulatorias y de mercado particulares. Por ello, las reflexiones que aquí se recogen deben entenderse como puntos de apoyo sobre los que construir un enfoque propio, adaptado a cada entorno, pero alineado con las exigencias estructurales que impone NIS2.

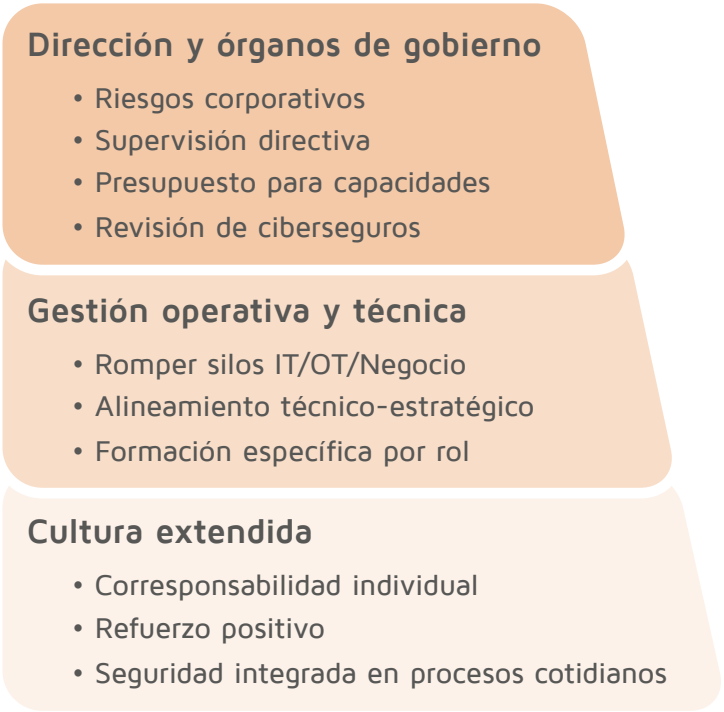
A lo largo de los diez apartados que siguen, se abordan cuestiones críticas como la gestión de la cadena de suministro, la visibilidad sobre activos IT y OT, el diseño de marcos de gobernanza transversales, la formación y concienciación del personal, o la interoperabilidad tecnológica. Todos ellos son elementos clave para garantizar la resiliencia operativa, el cumplimiento normativo y, sobre todo, la sostenibilidad de las infraestructuras energéticas en un entorno digital cada vez más expuesto.

Con este decálogo, el comité no busca dictar soluciones únicas, sino ofrecer una base sólida de análisis desde la experiencia técnica y el conocimiento compartido, sobre la que las organizaciones puedan desarrollar su propio modelo de adaptación a NIS2 con garantías.

1. Gobernar desde la seguridad: cambio de mentalidad y cultura organizativa

La ciberseguridad ya no es técnica: es estratégica, transversal y de alta dirección

Tres niveles para transformar la cultura de ciberseguridad



El primer gran reto para abordar la aplicación de NIS2 en el sector energético y de utilities no es ni técnico ni legal, sino profundamente organizativo: **un cambio de mentalidad** que permita integrar la ciberseguridad como una función estratégica, transversal y medible. Durante años, la seguridad digital ha sido concebida en muchas organizaciones como un conjunto de medidas técnicas, con escasa visibilidad en los órganos de decisión, dependencia casi exclusiva del área IT, y presupuestos reactivos que solo crecen tras un incidente o por exigencia de auditorías.

Este enfoque resulta ahora no solo insuficiente, sino incompatible con el modelo de gobernanza que propone NIS2, que sitúa la ciberseguridad al mismo nivel que otras obligaciones críticas del negocio. Las empresas ya no pueden alegar desconocimiento o delegación operativa. La directiva establece **responsabilidades explícitas para la alta dirección**, incluyendo posibles sanciones personales en caso de omisión, y exige una implicación activa en el diseño, supervisión y financiación de la estrategia de ciberseguridad. Esto no se traduce en una mera firma o en la revisión de un informe: implica asumir la seguridad digital como una línea más del gobierno corporativo, con planificación, seguimiento y control efectivo.

Este cambio es especialmente **urgente** en el contexto actual, en el que muchas organizaciones aún están a la espera de la transposición de la directiva al marco normativo español. A pesar de que todavía puedan existir dudas sobre la aplicación concreta o los sujetos obligados, la orientación general es clara, y el tiempo para adaptarse es limitado. Postergar decisiones estratégicas por esperar al BOE puede dejar a las organizaciones en una posición vulnerable, tanto desde el punto de vista del cumplimiento como del riesgo real al que se enfrentan.

Desde esta perspectiva, el primer paso es reconstruir la narrativa interna: **la ciberseguridad no es una barrera, es un habilitador**. Permite garantizar la continuidad del servicio, minimizar el impacto de incidentes, proteger la confianza del mercado y operar conforme a exigencias regulatorias crecientes. Este cambio discursivo debe ir acompañado de mecanismos de gobernanza concretos: interlocutores con peso en la estructura directiva, métricas comprensibles por el negocio, indicadores de madurez y riesgo alineados con los objetivos de continuidad, sostenibilidad y crecimiento de la organización.

Tres niveles para transformar la cultura organizativa

Un modelo eficaz de cambio de mentalidad debe avanzar en tres niveles simultáneos:

Alto nivel (dirección y órganos de gobierno):

- Incluir la ciberseguridad en el mapa de riesgos corporativos.
- Establecer un comité específico o canalizar la supervisión desde el comité de auditoría o riesgos.
- Asignar presupuesto no solo para herramientas, sino para capacidades: personas, procesos, tiempo.
- Revisar la oferta de seguros específicos para ciberamenazas, su cobertura real y los criterios de elegibilidad-exclusión.

Nivel intermedio (gestión operativa y técnica):

- Romper los silos entre IT, OT y negocio, generando estructuras mixtas y responsabilidad compartida.
- Crear espacios regulares de alineamiento entre áreas técnicas y estrategia corporativa.
- Diseñar planes de formación y concienciación que no se limiten a lo genérico, sino que se adapten al rol, sector y entorno tecnológico específico.

Nivel base (cultura extendida en toda la organización):

- Promover una cultura de corresponsabilidad donde cada empleado entienda el impacto de sus decisiones.
- Implementar mecanismos de refuerzo positivo: reconocimiento, gamificación, evaluación.
- Integrar la seguridad en procesos cotidianos: proyectos, compras, relaciones con terceros.

En el sector energético, este cambio debe contemplar específicamente la cultura técnica y operativa de los entornos OT, donde la seguridad ha sido tradicionalmente secundaria frente a la disponibilidad. Es habitual encontrar plantillas con fuerte orientación a la operación continua, y donde las medidas de seguridad se perciben como potenciales amenazas a la estabilidad de los procesos. Este sesgo debe ser abordado desde el liderazgo, traduciendo los objetivos de ciberseguridad a parámetros que tengan sentido en entornos industriales: evitar paradas imprevistas, mantener la integridad de datos operacionales, garantizar el cumplimiento normativo o evitar sanciones que comprometan contratos clave. Este reto se amplifica con la **proliferación de sensores y dispositivos conectados**, especialmente en redes de baja tensión, que incrementan de forma exponencial el perímetro de exposición. Cada uno de estos dispositivos representa una posible puerta de entrada, en un ecosistema donde aún no existe una estandarización clara. Comprender y visibilizar esta realidad técnica forma parte del cambio de mentalidad que se exige.

Un ejemplo concreto: en una empresa eléctrica con operación distribuida, la dirección puede activar una política que vincule la evaluación de desempeño de los responsables de planta con el cumplimiento de controles básicos de ciberseguridad (segmentación de red, autenticación fuerte, actualizaciones críticas). En paralelo, puede introducirse un sistema de alertas automatizadas que eleve a nivel corporativo cualquier desviación o riesgo no tratado durante más de un periodo definido, vinculando estas alertas con el sistema de gestión de riesgos global. De esta forma, la seguridad deja de ser reactiva para convertirse en parte estructural del modelo de negocio.

Finalmente, este cambio de mentalidad es la base sobre la que se apoya todo lo demás. **Sin una cultura madura, sin liderazgo convencido y sin una narrativa compartida**, el resto de medidas —tecnológicas, legales, organizativas— quedan limitadas a respuestas parciales. Solo una cultura que reconoce la ciberseguridad como elemento crítico podrá evolucionar hacia un modelo de resiliencia integral, que cumpla con los requisitos de NIS2 y, al mismo tiempo, refuerce la posición competitiva de la organización en un entorno cada vez más incierto y regulado. En este camino, la relación con la administración pública no debe entenderse solo como cumplimiento formal, sino como **una oportunidad para generar valor conjunto**. La creación de una comunidad activa en torno a la ciberseguridad sectorial, el intercambio de buenas prácticas o la participación en espacios de coordinación como la Oficina de Coordinación de Ciberseguridad pueden reforzar tanto la capacidad de respuesta como la innovación conjunta. **Ver más allá de NIS2** es entender que la verdadera razón para actuar no es evitar una sanción, sino reducir el riesgo real en un entorno hiperconectado, cada vez más complejo y vulnerable.

2. Adelantarse al BOE: adaptación proactiva en base a borradores

No esperar al texto definitivo es la única forma de llegar a tiempo (y bien)

Una de las lecciones más importantes que deja la experiencia con normativas anteriores —como el RGPD, la NIS original o el Esquema Nacional de Seguridad— es que la pasividad regulatoria tiene costes. Esperar a la publicación oficial, a la entrada en vigor, o a las primeras sanciones para actuar, no solo reduce el margen de maniobra, sino que obliga a improvisar medidas de alto impacto en plazos irrealistas. En el caso de NIS2, este enfoque reactivo no es solo ineficaz: es directamente peligroso.

La directiva europea está aprobada desde enero de 2023, y aunque su transposición en España sigue en proceso, los principios fundamentales están definidos. No hay espacio para alegar desconocimiento, y mucho menos para justificar inacción. Lo que está en juego no es simplemente el cumplimiento formal, sino la preparación de toda la organización para operar en un entorno regulado, complejo y con tolerancia cero a las brechas de seguridad que afecten a servicios esenciales.

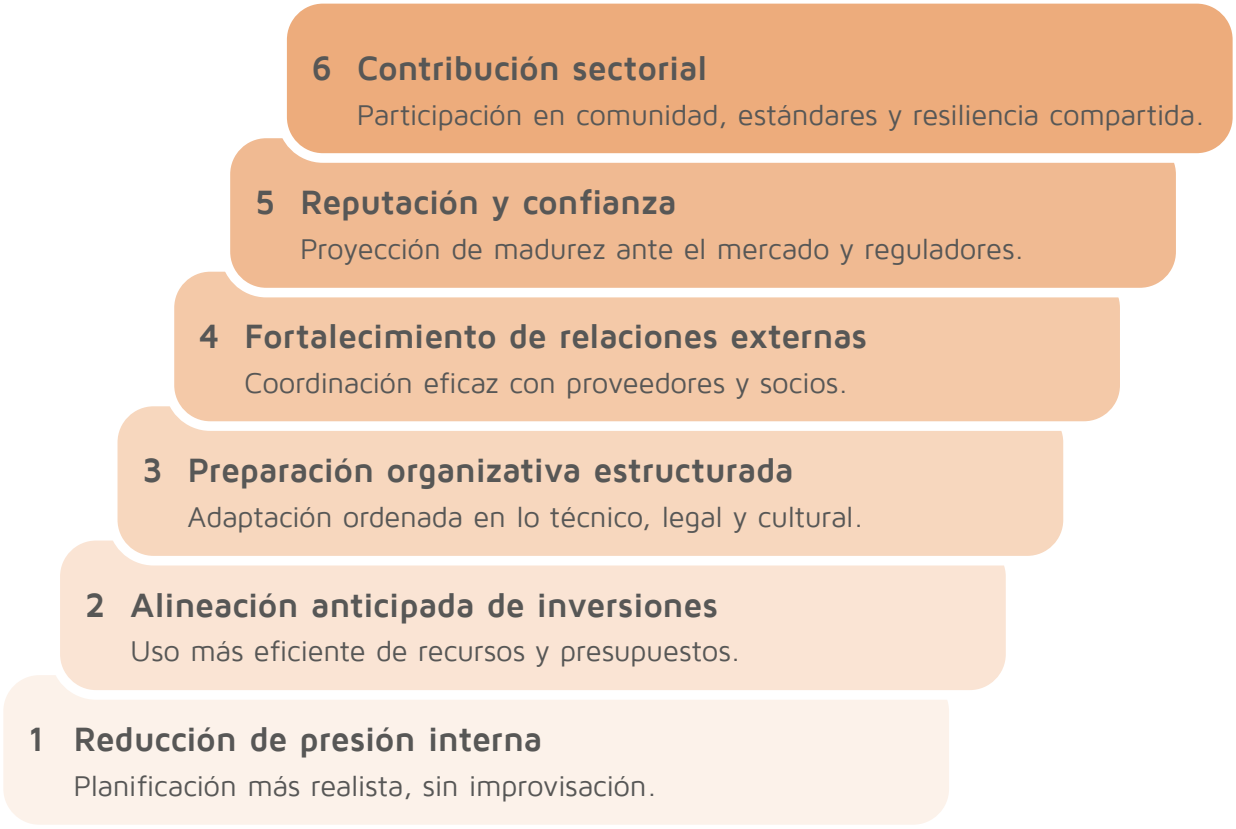
El enfoque adecuado es, por tanto, **activar cuanto antes un proceso de adaptación estructurado**, tomando como referencia los textos comunitarios, los borradores del anteproyecto de ley español y los estándares ya alineados con el espíritu de NIS2. Esta estrategia tiene múltiples ventajas:

- Reduce la presión sobre los equipos de cumplimiento.

- Permite alinear inversiones con antelación.
- Facilita la anticipación de cambios organizativos de calado.
- Aporta ventaja competitiva al demostrar madurez y solvencia ante clientes, proveedores y reguladores.

Más aún: anticiparse es una forma de demostrar liderazgo. NIS2 no debe verse como una imposición externa, sino como una oportunidad para reforzar la postura de ciberseguridad y modernizar la gobernanza de riesgos digitales. Las organizaciones que actúan desde la responsabilidad, antes de que la ley las obligue, proyectan una imagen sólida y confiable, lo que se traduce en ventajas reputacionales, mejor relación con auditores y reguladores, y mayor confianza en su ecosistema.

Ventajas de una adaptación proactiva a NIS2



Desde un punto de vista operativo, la anticipación ofrece tres beneficios directos:

Planificación realista

Iniciar los trabajos con tiempo permite hacer un análisis de brechas riguroso, detectar cuellos de botella organizativos, priorizar acciones en función del riesgo real y escalonar la inversión en tecnología o consultoría. En lugar de correr detrás de una fecha legal, se puede construir una hoja de ruta alineada con los procesos internos y con los plazos razonables que exige el cambio cultural y técnico.

Coordinación con terceros

Muchas de las obligaciones de NIS2 afectan a elementos que no están bajo control directo de la organización: integradores, fabricantes, proveedores cloud, empresas de mantenimiento, etc. Cuanto antes se actúe, más margen habrá para renegociar contratos, definir cláusulas de ciberseguridad, establecer

responsabilidades compartidas y garantizar que todos los actores clave están alineados con los nuevos requisitos.

Ganancia de tiempo para el cambio cultural

La adaptación a NIS2 no es solo técnica. Requiere formar, sensibilizar y movilizar a la organización en su conjunto. Y eso no se consigue con un boletín interno ni con una charla puntual. Se necesita tiempo para que las nuevas prácticas se asienten, para construir una narrativa coherente sobre el riesgo digital, y para implicar de verdad a las personas en la transformación que la norma exige.

Este enfoque es especialmente relevante en sectores como el energético y de utilities, donde la complejidad técnica, la heterogeneidad de entornos OT y la existencia de múltiples capas de subcontratación hacen que los cambios regulatorios sean difíciles de aplicar con carácter retroactivo. En muchos casos, la única forma de aplicar medidas exigidas por NIS2 —como la segmentación de redes, el control de acceso granular o la gestión activa de la cadena de suministro— es rediseñar procesos completos o invertir en tecnologías específicas. Nada de eso se hace en una semana.

La falsa sensación de "esperar al texto definitivo" puede acabar dejando a la organización en una situación crítica: sin tiempo para reaccionar, sin recursos disponibles en el mercado (consultores, auditores, integradores saturados), y con la presión añadida de cumplir con una norma que, una vez transpuesta, no incluirá moratorias relevantes. La directiva no está pensada para dar margen: está pensada para cambiar el modelo de responsabilidad.

Por eso, más que una recomendación, **la adaptación proactiva es una exigencia de supervivencia**. Las organizaciones que lleguen tarde no solo se enfrentarán a sanciones, sino a una pérdida real de capacidad operativa y reputacional. NIS2 no es un trámite. Es una llamada a actuar. Y en este terreno, quien espera, pierde.

Anticiparse también es construir

No todas las organizaciones parten del mismo nivel de madurez. Mientras algunas grandes compañías ya cuentan con marcos de ciberseguridad consolidados, otras —especialmente medianas o con menor exposición previa al cumplimiento normativo— se enfrentan al reto de construir capacidades desde cero. Para estas últimas, anticiparse no es solo una ventaja competitiva, sino una condición necesaria para evitar improvisaciones, errores críticos o inversiones mal dirigidas.

Además, la anticipación permite ordenar y profesionalizar la respuesta organizativa:

- Identificar responsables.
- Establecer mínimos de gobernanza.
- Priorizar acciones.
- Coordinarse con los actores clave del ecosistema.

Esto resulta especialmente valioso en un entorno como el energético, donde la densidad de proveedores y la presencia de entornos OT incrementan la complejidad técnica y contractual de cualquier adaptación. Adelantarse no es solo responder antes: es responder mejor.

Por último, actuar con antelación también es una vía para **generar comunidad y conocimiento compartido**. Colaborar con otras organizaciones del sector permite:

- Compartir buenas prácticas y aprendizajes.
- Participar en espacios de coordinación sectorial.
- Contribuir a definir estándares y enfoques comunes.
- Fortalecer la resiliencia colectiva frente a amenazas compartidas.

Adaptarse a NIS2 no es solo una cuestión de cumplimiento: es una oportunidad para reforzar las capacidades internas, construir alianzas y avanzar en la madurez digital del conjunto del sector.

3. Alineamiento normativo y análisis de brechas: construir sobre lo existente

Conocer el punto de partida real para avanzar sin duplicar esfuerzos ni improvisar

Elementos clave de un análisis de brechas eficaz

Antes de hablar de cumplimiento, **es necesario hablar de contexto**. La mayoría de organizaciones del sector energético y de utilities no parten de un folio en blanco: llevan años avanzando en la consolidación de políticas de seguridad, han superado auditorías externas y trabajan bajo marcos reconocidos como ISO/IEC 27001, IEC 62443, el Esquema Nacional de Seguridad o incluso la ya derogada directiva NIS1. Este recorrido previo no debe ignorarse —ni duplicarse— al aplicar NIS2. El verdadero reto es entender en qué punto se está, qué lagunas existen y cómo construir una estrategia de cumplimiento a partir de lo ya implantado.

El primer paso es, por tanto, un **análisis de brechas riguroso, contextualizado y útil**. No basta con revisar listas de requisitos. Se trata de confrontar los procesos, controles, estructuras de gobierno y capacidades reales de la organización con los mandatos específicos de la nueva normativa. El resultado debe ser algo más que una tabla comparativa: debe reflejar el grado de madurez de cada componente crítico, identificar prioridades y señalar caminos de integración entre marcos normativos. Un análisis eficaz debe:

- Basarse en una visión completa de los entornos IT y OT.
- Evaluar el nivel de madurez de cada dominio: prevención, detección, respuesta, recuperación.
- Identificar responsables y estructuras de decisión por ámbito.
- Priorizar acciones en función del riesgo y del impacto operativo.
- Proponer soluciones viables, no solo detectar carencias.

Aquí, la experiencia previa en cumplimiento juega a favor, pero también puede ser una trampa. Muchas organizaciones han enfocado sus sistemas de gestión exclusivamente en el ámbito IT, dejando fuera —o tratando de encajar a la fuerza— los entornos operacionales. NIS2 rompe esa barrera. Obliga a mirar los sistemas OT con los mismos ojos que los IT: con exigencia, con trazabilidad y con responsabilidad. Por eso, el análisis de brechas debe incorporar explícitamente la cobertura de la seguridad industrial, desde el acceso remoto a SCADAs hasta la gestión de firmware en controladores de planta.

En este contexto, resulta especialmente valioso apoyarse en marcos como **la norma IEC 62443**, que permite estructurar el análisis de riesgos de forma específica para entornos industriales. Frente a los modelos más genéricos, esta referencia proporciona criterios técnicos claros para evaluar activos, vulnerabilidades, vectores de amenaza y niveles de protección por capas, incluyendo requisitos de segmentación, autenticación o protección de firmware. Integrar esta norma en el análisis de brechas permite no solo cumplir con NIS2, sino elevar el nivel real de ciberresiliencia en infraestructuras críticas.

Este ejercicio también exige **leer entre líneas**. NIS2 no impone un único modelo de cumplimiento, pero sí establece expectativas claras sobre gobernanza, respuesta a incidentes, supervisión técnica y evaluación de riesgos. La capacidad de interpretar esos principios —y no solo traducirlos a controles— marca la diferencia entre una adecuación formal y una adaptación real. Integrar estándares como ISO 27001 o IEC 62443, no como compartimentos estancos sino como piezas de un mismo marco de gestión, puede generar eficiencias operativas y fortalecer la coherencia del sistema de seguridad.

Además, el alineamiento normativo ofrece una oportunidad para **repensar la arquitectura documental**. Si se gestiona bien, permite evitar duplicidades, reducir carga administrativa y simplificar las auditorías internas y externas. Aprovechar sinergias entre normativas —por ejemplo, entre NIS2 y ENS en entornos públicos o mixtos— no solo es posible, sino recomendable. Algunas ventajas clave de este enfoque son:

- Reutilización de políticas y procedimientos existentes.
- Consolidación de evidencias para auditorías cruzadas.
- Mejora en la trazabilidad y la coherencia documental.
- Reducción del riesgo de contradicciones normativas internas.

Por último, el análisis de brechas debe tener **una dimensión estratégica**. Cumplir con NIS2 no significa lo mismo para todos: no es igual la exigencia que afronta un operador de infraestructura crítica que la de un proveedor de servicios especializados. El grado de exposición, el impacto potencial de un fallo, la complejidad del ecosistema técnico o la dispersión geográfica son factores determinantes a la hora de definir el nivel de madurez deseado. El gap analysis no debe ser un checklist genérico, sino una herramienta de reflexión adaptada al rol, el modelo de negocio y la realidad operacional de cada organización.

Este análisis no solo permite alinear la organización con la normativa, sino también **construir una base sólida para la toma de decisiones futuras**. En sectores con estructuras aún inmaduras, este proceso puede ser la primera oportunidad real de identificar interlocutores, clarificar responsabilidades y sentar las bases de una gobernanza eficaz. En ese sentido, el análisis de brechas no es una simple herramienta de diagnóstico, sino un verdadero catalizador de transformación.

En resumen: NIS2 no obliga a reinventar la seguridad, pero sí a reestructurarla. Aprovechar lo que ya funciona, entender lo que falta, y planificar cómo integrarlo todo bajo una misma lógica. Esa es la verdadera función del análisis de brechas. No como fin en sí mismo, sino como punto de partida inteligente para un cumplimiento sostenible.

4. Riesgos reales, decisiones reales: el análisis como brújula estratégica

Sin comprensión del riesgo, toda estrategia es ciega

En el marco de NIS2, el análisis de riesgos deja de ser una casilla administrativa o un documento auxiliar para convertirse en el **eje central de cualquier estrategia de ciberseguridad eficaz**. No se trata de elaborar un informe para cumplir el expediente, sino de comprender en profundidad cuáles son los activos críticos, qué procesos dependen de ellos, qué vulnerabilidades los afectan y qué consecuencias podría tener un ataque en términos de servicio, seguridad, reputación y responsabilidad legal. Y hacerlo no como un ejercicio estático, sino como un **proceso dinámico**, que evoluciona con el entorno, la tecnología y el negocio.

Este tipo de análisis requiere una **visión transversal del ecosistema operativo**, capaz de conectar lo técnico con lo estratégico. Es imprescindible ir más allá de las aproximaciones genéricas o las plantillas heredadas. Hay que representar la complejidad real: la coexistencia de tecnologías IT y OT, la propagación de fallos entre sistemas interconectados, los riesgos combinados físicos y digitales, y los impactos en cascada que pueden derivarse de una vulnerabilidad aparentemente menor. En sectores como el energético, donde las interdependencias son elevadísimas y el tiempo de respuesta crítico, esta capacidad de modelar escenarios reales no es una sofisticación: es una necesidad operativa.

En este sentido, la **norma IEC 62443** se presenta como una referencia especialmente valiosa. Este conjunto de estándares ha sido diseñado para proteger los sistemas de automatización y control industrial (IACS) y proporciona un enfoque sistemático y escalable para la evaluación de riesgos en entornos OT. Su integración en el análisis permite:

- Identificar claramente los activos industriales y su criticidad en la operación.
- Clasificar zonas y conductos para definir perímetros de seguridad.
- Establecer niveles de seguridad (SL) adecuados para cada segmento.
- Aplicar requisitos específicos de autenticación, autorización, detección y respuesta.
- Alinear el diseño de sistemas con un modelo de defensa en profundidad adaptado al entorno OT.

Componentes esenciales del análisis de riesgos estratégico

Apoyarse en IEC 62443 no solo aporta rigor metodológico, sino que ayuda a **traducir los riesgos OT en términos comprensibles y gestionables** para el negocio, facilitando su integración en los sistemas de gestión globales y en la interlocución con los responsables de continuidad, operaciones o cumplimiento.

Un error común en muchas organizaciones es **aislar el análisis de riesgos del resto del ciclo de vida de la seguridad**. Se hace un informe para justificar una inversión, se revisa en una auditoría o se presenta ante el regulador, pero no se conecta con el diseño de arquitecturas, la gestión del cambio o la contratación de proveedores. En este nuevo contexto, esa desconexión ya no es sostenible. El análisis de riesgos debe integrarse en la toma de decisiones de forma continua, alimentarse de datos operativos y utilizar un lenguaje que sea comprensible para perfiles técnicos, jurídicos y ejecutivos por igual.

Para que este análisis tenga impacto real, debe incorporar ciertos elementos esenciales:

- Inventario actualizado y clasificado de activos.
- Identificación de dependencias críticas entre procesos, servicios y tecnologías.
- Evaluación de amenazas internas y externas, intencionales y accidentales.
- Análisis de vulnerabilidades técnicas y organizativas.
- Estimación del impacto potencial, tanto operativo como reputacional y legal.
- Determinación de la probabilidad y exposición al riesgo.
- Priorización y propuestas de respuesta, mitigación o transferencia del riesgo.

Además, NIS2 no solo exige mirar el presente, sino también **anticipar los riesgos emergentes**. Nuevas tecnologías —como la inteligencia artificial aplicada al edge o la hiperconectividad de los dispositivos— abren nuevos vectores de ataque. Cambios regulatorios, movimientos de fusiones y adquisiciones, tensiones geopolíticas o la evolución de la cadena de suministro pueden introducir amenazas antes inexistentes. Por tanto, el análisis debe tener capacidad prospectiva, detectar señales débiles y alertar con antelación suficiente para evitar respuestas improvisadas.

La incorporación de **modelos cuantitativos de análisis de riesgos**, como el enfoque FAIR (Factor Analysis of Information Risk), puede ayudar a traducir los hallazgos técnicos en métricas útiles para decisiones de negocio. Priorizar riesgos, estimar impactos económicos y justificar inversiones no debe basarse únicamente en la intuición o la experiencia: debe apoyarse en herramientas que permitan comparar alternativas y asignar recursos de forma proporcional a la exposición.

En última instancia, la utilidad real del análisis de riesgos se mide por su **impacto en la toma de decisiones**. No basta con identificar amenazas: hay que traducirlas en cambios concretos, reforzar procesos, justificar presupuestos, redefinir relaciones con terceros o rediseñar arquitecturas de red. Solo así el análisis se convierte en una herramienta de gobierno, y no en un documento decorativo.

Porque en ciberseguridad, como en la navegación, no basta con tener un mapa: hay que saber leerlo, actualizarlo y usarlo para llegar a buen puerto. El análisis de riesgos es esa brújula. Y NIS2 exige que esté siempre encendida.

5. Gobernanza de la ciberseguridad: romper silos y unificar lenguajes

Traducir la estrategia en reglas, estructuras y responsabilidades compartidas

Modelo escalonado de gobernanza de la ciberseguridad

La implementación efectiva de la directiva NIS2 en el sector energético exige, por encima de cualquier otra medida, una transformación estructural en la gobernanza de la ciberseguridad. No se trata únicamente de cumplir nuevos requisitos, sino de replantear cómo se toman las decisiones relacionadas con la seguridad digital, quién las toma, con qué criterios y con qué grado de coordinación entre las distintas partes de la organización. Para muchas empresas, especialmente las de menor tamaño o madurez, esto supone reconfigurar una arquitectura organizativa que ha sido históricamente fragmentada, funcional pero insuficiente en el contexto de riesgo actual.

Uno de los síntomas más evidentes de esta fragmentación es la separación estructural entre los entornos IT y OT. A lo largo de los últimos años, la mayoría de organizaciones han desarrollado estrategias, herramientas y equipos distintos para gestionar la seguridad en cada uno de estos dominios. Esto ha dado lugar a barreras funcionales, terminológicas, técnicas e incluso culturales que dificultan la implementación de una estrategia de ciberseguridad unificada. Mientras los equipos de IT trabajan con normas como ISO/IEC 27001 y herramientas de ciberdefensa perimetral, en los entornos OT se prioriza la disponibilidad y estabilidad de los sistemas, operando a menudo con tecnologías propietarias y sin aplicar criterios de seguridad avanzados.

En este contexto, la gobernanza debe actuar como capa de integración: un marco estructurado que permita alinear objetivos, coordinar recursos y estandarizar procesos en ambos mundos. Esto no significa necesariamente eliminar la especialización, sino garantizar que IT y OT comparten una visión común de los riesgos, de las responsabilidades y de las decisiones clave que afectan a la seguridad de la organización. Esta visión compartida también facilita una mejor interlocución con proveedores, socios estratégicos y administraciones públicas, elementos clave en la aplicación efectiva de NIS2.

Un enfoque escalonado para redefinir la gobernanza

El diseño de este nuevo modelo puede abordarse en tres niveles, que deben evolucionar de forma progresiva:

Nivel estratégico:

La ciberseguridad debe formar parte explícita de la agenda del comité de dirección. Esto implica que haya una persona con responsabilidad ejecutiva sobre la función de seguridad, idealmente con visibilidad sobre IT y OT, que reporte directamente al CEO o al consejo. En organizaciones con alta madurez, esta figura puede adoptar el rol de Chief Security Officer (CSO) o Chief Resilience Officer (CRO); en otras, puede tratarse de una función compartida entre los responsables de tecnología, operaciones y cumplimiento. Lo importante es que exista una línea clara de responsabilidad, autoridad para tomar decisiones e interlocución con el máximo nivel de gobierno corporativo.

Nivel táctico-organizativo:

Aquí es donde se debe romper la lógica de silos. En lugar de mantener equipos de IT y OT aislados, se deben constituir **estructuras híbridas**, como comités de ciberseguridad mixtos, oficinas de convergencia tecnológica o unidades de ciberresiliencia, donde se trabajen de forma conjunta los temas clave:

- Evaluación de riesgos.
- Planes de contingencia.
- Incorporación de nuevos proveedores.
- Adquisición de tecnología.
- Cumplimiento normativo.

Estos equipos deben establecer rutinas compartidas, indicadores comunes y canales de escalado definidos. No se trata solo de intercambiar información, sino de crear un lenguaje común.

Nivel operativo y procedimental:

El último paso consiste en estandarizar las políticas, procesos y herramientas. Esto implica desarrollar un sistema de gestión de la seguridad que funcione como un todo, con una única política de seguridad corporativa que contemple la especificidad de cada entorno, pero que imponga criterios transversales de:

- Control y auditoría.
- Gestión de incidentes.
- Gestión de accesos.
- Procedimientos de cambio y revisión.

También supone definir flujos de trabajo integrados: por ejemplo, un cambio en un entorno OT crítico debe seguir un proceso de análisis de riesgo y aprobación similar al que seguiría en IT, con trazabilidad documental y supervisión independiente.

Ejemplos de aplicación práctica

Una compañía distribuidora de electricidad con múltiples centros de transformación y operación remota puede enfrentarse a problemas de gobernanza si el equipo OT que gestiona el sistema SCADA tiene autonomía total sobre sus dispositivos, sin pasar por los controles definidos por el equipo de seguridad corporativo. Esto puede derivar en configuraciones inseguras, desconocimiento de vulnerabilidades o falta de actualización de firmware. Para evitarlo, puede implantarse una política de cambios conjunta, en la que toda modificación relevante en activos OT pase por un circuito formal de revisión por parte del equipo de ciberseguridad, antes de su implementación en campo.

Otro caso frecuente es el de los proveedores que gestionan componentes críticos en entornos OT (p.ej., sistemas de telegestión, regulación o control de procesos industriales). Si el modelo de gobernanza no incorpora cláusulas específicas en los contratos, protocolos de auditoría o procedimientos para responder ante incidentes relacionados con estos terceros, la organización pierde capacidad de control sobre una parte esencial de su exposición al riesgo. Incluir estos elementos en la gobernanza —como parte de la gestión del ciclo de vida del proveedor— es esencial para cumplir con NIS2.

Consideraciones para distintos niveles de madurez

Es importante adaptar el diseño del marco de gobernanza al nivel de madurez y a la estructura organizativa real. Algunas opciones, en función del punto de partida, pueden ser:

- En compañías pequeñas: establecer un comité de coordinación mensual entre áreas técnicas, operaciones y cumplimiento.
- En organizaciones medianas: crear una unidad formal con responsabilidades claras, procesos estandarizados y reporting periódico a dirección.
- En empresas grandes o con alta complejidad operativa: profesionalizar completamente esta función mediante una oficina de seguridad estructurada, responsables por dominio y un modelo de indicadores integrado.

Sea cual sea el punto de partida, lo fundamental es evitar la parálisis por complejidad. Es preferible comenzar por establecer una mínima estructura de coordinación y hacerla evolucionar gradualmente, que esperar a tener un modelo perfecto para empezar a actuar.

Gobernanza como activo estratégico

En última instancia, el valor de un buen marco de gobernanza no se limita al cumplimiento normativo. Permite a la organización:

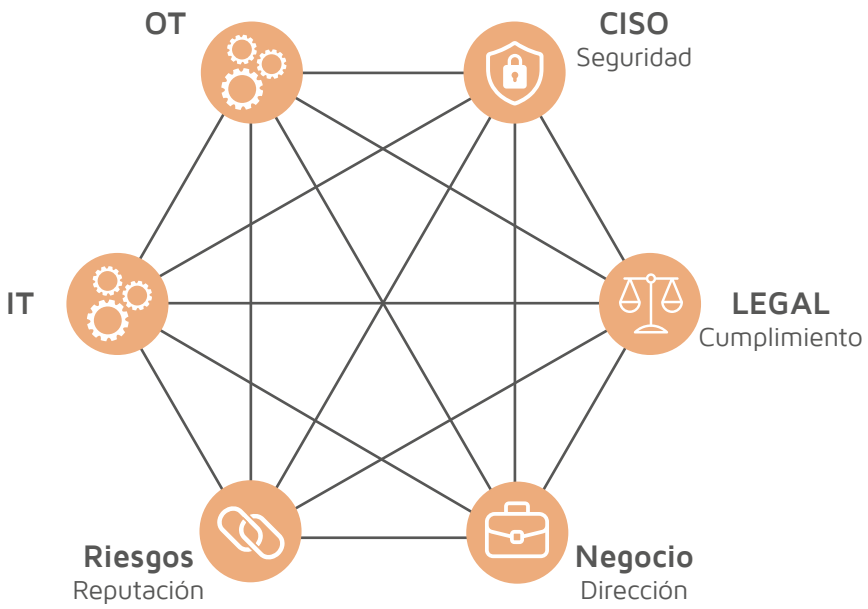
- Ser más eficiente en la asignación de recursos.
- Tomar decisiones con mayor respaldo técnico y estratégico.
- Alinear inversiones tecnológicas con necesidades reales.
- Responder con agilidad ante crisis o incidentes.
- Mejorar la interlocución con el ecosistema: clientes, socios, proveedores y administraciones públicas.

Desde la perspectiva de NIS2, esto se traduce en una mayor capacidad de demostrar cumplimiento, una reducción de la exposición a sanciones, y una mejor reputación ante clientes, socios y administraciones públicas. Pero desde la perspectiva interna, significa algo más profundo: disponer de un sistema de seguridad que forma parte del negocio, no que opera al margen de él.

6. Estructuras transversales para una ciberseguridad coordinada

Conectar personas, procesos y entornos más allá del organigrama

Estructuras transversales para una ciberseguridad coordinada



La adaptación a NIS2 no puede sostenerse sobre estructuras organizativas tradicionales que segmentan responsabilidades y conocimientos en compartimentos estancos. A medida que el perímetro digital de las organizaciones energéticas se difumina —por la convergencia de tecnologías IT y OT, la proliferación de proveedores tecnológicos y la exposición creciente a ciberamenazas—, resulta imprescindible construir equipos con capacidad de trabajar transversalmente, integrar perspectivas distintas y actuar con rapidez ante situaciones complejas. Este enfoque no es únicamente operativo: es una condición para que las decisiones estratégicas de seguridad puedan implementarse eficazmente a todos los niveles.

Romper silos, una necesidad estructural

El modelo clásico —en el que IT se encarga de los sistemas corporativos y OT de los entornos industriales, cada uno con sus propias prioridades, herramientas y estructuras de mando— ha demostrado ser ineficaz frente a ataques que aprovechan precisamente las zonas grises entre ambos mundos. En este modelo, los incidentes se gestionan de forma descoordinada, las decisiones de seguridad se fragmentan y los planes de acción se implementan con criterios divergentes. NIS2 rompe explícitamente esta lógica al exigir una gestión integrada del riesgo y una responsabilidad clara y compartida sobre los activos críticos.

La construcción de **equipos transversales** es la respuesta organizativa a esta exigencia. Implica no solo colaboración, sino codiseño y cogobernanza. En la práctica, esto significa:

- Crear grupos de trabajo formales con funciones permanentes.
- Establecer objetivos comunes que trasciendan las áreas técnicas.
- Integrar perfiles diversos: técnicos IT, especialistas OT, seguridad, cumplimiento, legal, negocio...
- Dotar a estos equipos de autonomía para proponer y ejecutar acciones.

Estos equipos no deben reunirse solo en situaciones de crisis: su trabajo debe formar parte del funcionamiento habitual de la organización, con agendas definidas, roles establecidos y continuidad operativa. La colaboración debe convertirse en rutina, no en excepción.

Construir una cultura técnica compartida

Uno de los primeros pasos para hacer esto posible es desarrollar una **cultura de colaboración técnica real**. Muchas veces, los equipos IT y OT no comparten ni siquiera el mismo vocabulario operativo. Mientras unos hablan de firewalls, hardening, patching o gestión de logs, otros se centran en disponibilidad, redundancia, continuidad de proceso y mantenimiento. La falta de entendimiento mutuo es una barrera real. Por eso, la transversalidad no se construye solo desde la estructura, sino también desde la capacitación:

- Formar a los equipos en los fundamentos del otro dominio.
- Generar espacios de encuentro técnico recurrentes.
- Compartir herramientas, casos de uso y buenas prácticas.
- Diseñar itinerarios de rotación funcional para construir experiencia cruzada.

Ejercicios conjuntos y estructuras avanzadas

A nivel práctico, la creación de **equipos de respuesta a incidentes conjuntos** (CSIRT híbridos) es una de las formas más efectivas de poner en marcha esta transversalidad. Estos equipos permiten coordinar acciones de detección, análisis y mitigación sin que cada parte actúe en solitario. También son clave en los ejercicios de simulación, que deben diseñarse específicamente para:

- Probar la cooperación entre áreas.
- Medir los tiempos de reacción.
- Evaluar la fluidez en la toma de decisiones bajo presión.

En organizaciones más avanzadas, la transversalidad también puede adoptar la forma de **arquitecturas matriciales**, en las que los responsables de seguridad IT y OT no solo dependen jerárquicamente de sus respectivas áreas, sino que participan funcionalmente en estructuras coordinadas de ciberseguridad, con objetivos y rendición de cuentas común. Este enfoque permite:

- Mantener la especialización sin perder alineamiento.
- Escalar decisiones con mayor agilidad.
- Evitar duplicidades o vacíos de cobertura.

Más allá de lo técnico: incorporar otras miradas

Otro elemento crucial en esta construcción es la inclusión de perfiles no técnicos en los equipos transversales. La ciberseguridad no es solo una cuestión de tecnología, y una estrategia eficaz debe incorporar la visión del negocio, del marco legal, de la gestión del cambio o del riesgo reputacional. Cuando estas áreas están presentes en la mesa de decisiones desde el inicio, es más fácil:

- Anticipar obstáculos regulatorios o de gestión.
- Adaptar soluciones técnicas a la operativa real.
- Evitar rigideces que impidan operar con agilidad.

Para las organizaciones de menor tamaño, la creación de equipos transversales no tiene por qué ser compleja. Puede comenzar con una figura de coordinación que conecte áreas, con comités quincenales de seguimiento, o con la designación de responsables funcionales compartidos. Lo importante es romper la lógica de decisiones aisladas y avanzar hacia un modelo en el que la seguridad sea responsabilidad de todos, no una tarea delegada.

En definitiva, construir estructuras transversales es mucho más que un ajuste organizativo. Es un cambio profundo en la forma en que las organizaciones abordan el riesgo, alinean capacidades y construyen resiliencia. Es, en última instancia, una inversión en inteligencia colectiva y agilidad institucional, dos capacidades que serán críticas para sobrevivir en un entorno de amenazas constantes, requisitos normativos crecientes y presión operativa continua.

7. Gestión de activos y Shadow IT: Controlar lo que se tiene, lo que se usa y lo que está fuera del radar.

La protección empieza sabiendo qué hay, dónde está y quién lo maneja

Ciclo de gestión de activos y Shadow IT

En el contexto de la directiva NIS2, la **gestión de activos** ya no puede limitarse a una actividad secundaria de mantenimiento o a un requisito documental de las auditorías. La **identificación, clasificación y supervisión continua** de los activos tecnológicos (tanto IT como OT) constituye una pieza central de cualquier estrategia de ciberseguridad. Esta exigencia cobra especial importancia en sectores como el energético y de utilities, donde la complejidad operativa, la coexistencia de múltiples generaciones tecnológicas y la alta criticidad de los procesos hacen de la **visibilidad** un desafío técnico de primer orden.

Además, el ritmo actual de digitalización ha multiplicado el número y la diversidad de activos conectados a las redes corporativas. Desde sensores en entornos industriales hasta servicios en la nube, pasando por dispositivos móviles, sistemas de telemetría o equipos de usuarios externos, el **perímetro de exposición** se ha expandido de forma exponencial. Cada nuevo nodo es una posible puerta de entrada, y la ausencia de un **control granular** sobre todos ellos incrementa el riesgo de incidentes graves. A esto se suma la creciente sofisticación de las amenazas, que aprovechan precisamente los **puntos ciegos del inventario** para desplegar ataques silenciosos y persistentes.

El problema no es solo saber cuántos equipos hay en la red, sino **entender exactamente qué hacen, quién los gestiona, qué software ejecutan, qué vulnerabilidades pueden tener y qué dependencias crean**. En otras palabras, pasar de un inventario estático a una visión dinámica y contextualizada de la infraestructura. Esto aplica por igual a activos físicos (servidores, estaciones de trabajo, controladores in-

dustriales, routers, sensores IoT) como a activos lógicos (máquinas virtuales, contenedores, aplicaciones, firmware, claves de API, servicios cloud, etc.).

Dentro de este panorama, el **Shadow IT** representa uno de los riesgos más persistentes y difíciles de acotar. Se trata del conjunto de recursos tecnológicos **no autorizados, no inventariados o no supervisados** por los equipos de seguridad o de infraestructura. En muchos casos, su origen es legítimo: un área de operaciones que necesita agilidad, un departamento que despliega una herramienta SaaS sin pasar por IT, un ingeniero que conecta un equipo directamente al entorno OT para una prueba puntual... pero el resultado es una pérdida de control que puede abrir la puerta a brechas críticas.

Este tipo de situaciones se ve agravado por varios factores estructurales del sector: redes industriales antiguas con documentación incompleta, activos en ubicaciones remotas con escasa conectividad, múltiples proveedores involucrados en la operación y mantenimiento, y la **falta histórica de una cultura de gestión centralizada de tecnología**. Todo ello dificulta enormemente la capacidad de tener una imagen completa y fiable del ecosistema digital.

Para revertir esta situación, las organizaciones deben adoptar un enfoque basado en múltiples capas:

- **Inventario automatizado y continuo**. Las hojas Excel o CMDBs desactualizadas ya no son suficientes. Es necesario incorporar herramientas de descubrimiento automático y escaneo pasivo (especialmente en OT, donde el escaneo activo puede interrumpir procesos). Soluciones como los sistemas de Asset Inventory Management, apoyadas por sondas de red, agentes de endpoint y tecnologías de análisis de tráfico, permiten generar y mantener un inventario actualizado y contextualizado.
- **Normalización y categorización**. No basta con descubrir activos: hay que poder agruparlos por tipología, función crítica, nivel de exposición, propietario, ubicación, sistema operativo, etc. Este **enriquecimiento semántico del inventario** facilita la priorización de riesgos y la aplicación de políticas diferenciales según la criticidad.
- **Integración con la gestión del ciclo de vida**. La gestión de activos debe formar parte de procesos formales: alta, cambios, y baja de los sistemas. Cada nuevo activo debe ser **evaluado desde el punto de vista de ciberseguridad** antes de su puesta en funcionamiento. Esto implica revisar firmware, versiones de software, configuraciones de red, y vulnerabilidades conocidas (CVE), entre otros.
- **Alerta de desviaciones**. El sistema debe ser capaz de detectar nuevos activos no autorizados, cambios inesperados en la configuración de los equipos existentes, o desapariciones sospechosas de dispositivos que estaban inventariados. Este tipo de eventos debe generar **alertas automáticas** integradas en los sistemas SIEM o de monitorización continua.
- **Responsabilidades definidas**. La gobernanza de la gestión de activos implica que alguien (o varios perfiles) sean **responsables de mantener actualizado el inventario**, validar nuevas incorporaciones y revisar posibles anomalías. Esto cobra especial importancia en entornos OT, donde suele haber una distancia operativa con los equipos IT y de seguridad.
- **Relación con la estrategia de riesgos**. Un activo no es solo una entidad técnica, es un **nodo dentro de la superficie de ataque**. Si no se conoce o no se supervisa, es imposible protegerlo. Por eso, la gestión de activos es una **precondición del análisis de riesgos**, de la segmentación de red, del control de acceso y de la respuesta ante incidentes. La **visibilidad es la base de todo lo demás**.
- **Estándares y marcos de referencia**. NIS2 no define cómo debe hacerse exactamente esta gestión, pero hay múltiples marcos que ofrecen guías técnicas al respecto: desde **ISO/IEC 27001 y 27002**, hasta **NIST CSF**, pasando por **IEC 62443** en el ámbito OT. Todos ellos insisten en la necesidad de contar con **procesos formales para la gestión de activos** como prerrequisito de una postura de seguridad madura.
- **Tecnologías complementarias**. En algunos entornos OT se ha empezado a emplear tecnología de network detection and response (NDR) adaptada a protocolos industriales, que permite identificar dispositivos conectados, mapear relaciones entre ellos y detectar comportamientos anómalos incluso sin tener agentes instalados. En entornos IT, la combinación de **EDR con escáneres de vulnerabilidades y herramientas de discovery en red** puede ofrecer una cobertura muy completa.

En definitiva, abordar el Shadow IT no es una lucha puntual, sino una **disciplina continua**. A medida que se adopten nuevas tecnologías, se integren nuevos proveedores o se desplieguen nuevas arquitecturas (como edge computing o entornos híbridos), el problema volverá a aparecer. Pero establecer ahora un **modelo sólido de gestión de activos** permitirá que la organización crezca sin perder el control.

Una oportunidad estratégica para transformar la cultura tecnológica

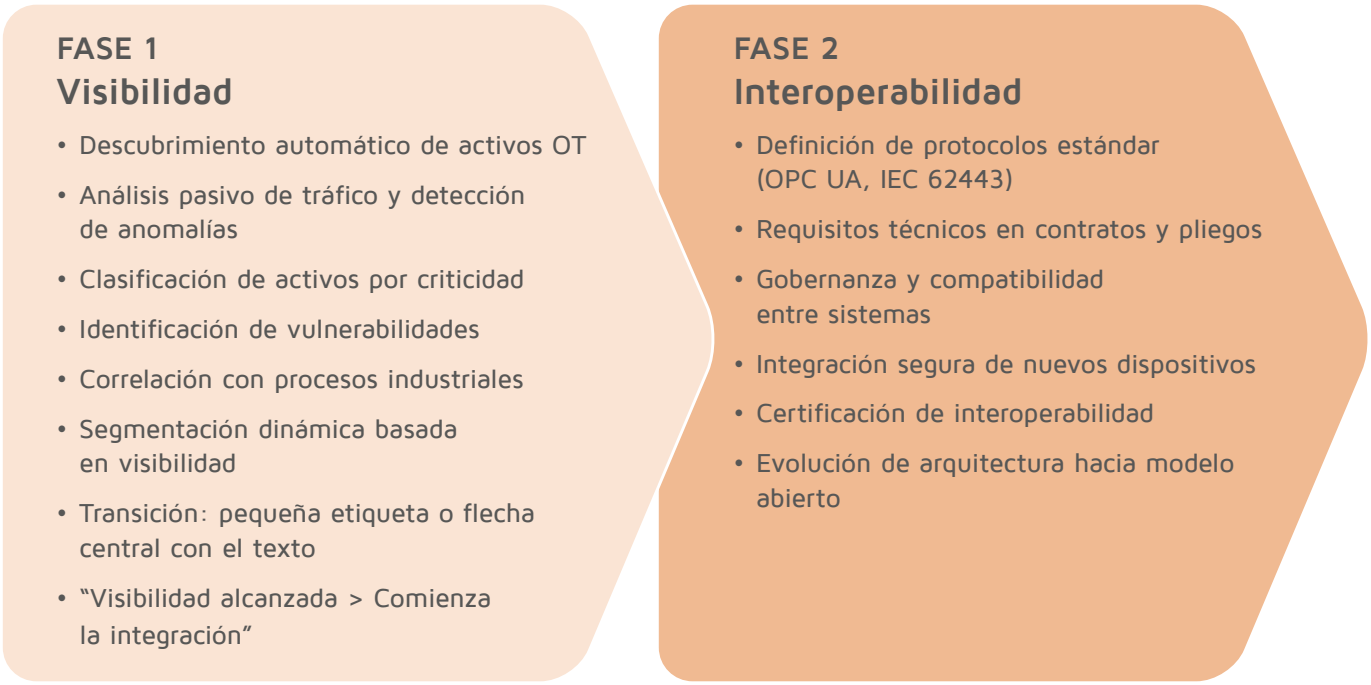
El refuerzo de la gestión de activos, lejos de ser una mera imposición regulatoria, ofrece una oportunidad para **madurar la cultura digital** de la organización. Supone avanzar hacia modelos de **visibilidad total, rendición de cuentas, colaboración interdepartamental y mejora continua**.

Al asumir este reto desde una perspectiva estratégica, las organizaciones no solo **reducen riesgos**, sino que fortalecen sus capacidades para **innovar, integrar nuevas soluciones y responder de forma más ágil** a los cambios tecnológicos o regulatorios. En este sentido, la gestión de activos es una de las grandes **palancas de transformación estructural** que puede dejar NIS2.

8. Interoperabilidad real en entornos OT: superar silos, fabricantes y protocolos cerrados

Lo que no se ve, no se puede proteger; lo que no se integra, no se puede gobernar

De la visibilidad a la interoperabilidad: hoja de ruta hacia la resiliencia OT



Uno de los desafíos más estructurales para la ciberseguridad industrial en el marco de NIS2 es la **falta de visibilidad en entornos OT**. A diferencia de los entornos IT, donde los estándares de conectividad y monitorización están más consolidados, el ecosistema OT —especialmente en el sector energético y de utilities— se caracteriza por una gran fragmentación: dispositivos de diferentes generaciones y fabricantes, protocolos propietarios, arquitecturas heterogéneas y múltiples capas de integración que han ido acumulándose con el tiempo sin una estrategia común.

Este tipo de infraestructuras operativas suelen crecer "por necesidad" y no "por diseño", lo que genera una situación de **silos técnicos**: redes que no hablan entre sí, sistemas legados sin soporte que no permiten

actualizaciones seguras, y equipamiento crítico que escapa a la supervisión de los responsables de ciberseguridad. A esto se suma la coexistencia de múltiples entornos operativos con distintas prioridades, como subestaciones eléctricas, plantas de tratamiento o redes de distribución, cada una con configuraciones específicas, proveedores distintos y requerimientos de disponibilidad elevados.

En este contexto, la **visibilidad a nivel de dispositivo** se convierte en el primer paso imprescindible para cualquier estrategia de ciberseguridad. No se puede supervisar lo que no se ve, ni proteger lo que no se puede identificar como parte de un sistema común. Y esta premisa es aún más crítica cuando recordamos que muchos de los activos OT —especialmente los que operan con protocolos cerrados o infraestructuras antiguas— ya han sido identificados como potenciales focos de Shadow IT, dificultando la aplicación de controles sistemáticos.

Tecnologías clave para lograr visibilidad OT

Lograr esa visibilidad exige la implantación de herramientas avanzadas de descubrimiento automático y análisis pasivo de tráfico, que permitan **mapear los dispositivos conectados**, interpretar su comportamiento, identificar relaciones funcionales y detectar vectores de ataque ocultos. Algunas soluciones reconocidas en este ámbito incluyen plataformas como Claroty, Nozomi Networks o Tenable.ot.

Estas herramientas no solo ayudan a descubrir dispositivos, sino que también permiten:

- Detectar cambios no autorizados en los activos OT.
- Identificar vulnerabilidades conocidas en el software de los dispositivos.
- Observar comportamientos atípicos que puedan indicar una intrusión.
- Clasificar cada activo en función de su rol dentro del proceso industrial.
- Correlacionar eventos de red con estados operativos de planta.
- Establecer patrones de tráfico legítimo frente a desviaciones peligrosas.

Este conocimiento operativo es clave para establecer **zonas de seguridad lógicas**, aplicar segmentación dinámica, e implementar barreras adaptadas al riesgo real. En otras palabras, la visibilidad no es un lujo: es la base técnica sobre la que se construyen todas las demás capacidades de ciberdefensa OT.

Interoperabilidad como evolución natural de la visibilidad

Una vez que se ha logrado visibilidad a nivel de dispositivo, el siguiente paso lógico es avanzar hacia la **interoperabilidad a nivel de sistemas**. Aquí es donde entran en juego los estándares abiertos, las arquitecturas de control unificadas y la necesidad de superar el vendor lock-in que todavía afecta a muchas instalaciones industriales.

La interoperabilidad OT debe entenderse como la capacidad de integrar, monitorizar y gobernar un ecosistema industrial de forma estructurada y segura, incluso cuando incluye dispositivos heterogéneos. Esta capacidad es esencial no solo para reducir complejidad operativa, sino para poder escalar políticas de seguridad, automatizar tareas de respuesta ante incidentes y cumplir con los principios de gobernanza exigidos por NIS2.

Gobernanza de la interoperabilidad: reglas, exigencias y contratos

Superar la fragmentación técnica también exige voluntad organizativa. Es imprescindible que las empresas establezcan políticas internas que definan con claridad:

- Qué protocolos son aceptables en su ecosistema OT.
- Qué estándares deben cumplir los nuevos dispositivos.
- Qué condiciones deben exigirse a proveedores y subcontratistas.

- Cómo asegurar la compatibilidad de nuevas soluciones con el entorno existente.
- Cuáles son los procedimientos para certificar interoperabilidad antes del despliegue.

Una palanca clave es el **poder de compra**: incluir en los pliegos y contratos exigencias como compatibilidad con IEC 62443, uso de OPC UA o entrega de documentación técnica es fundamental para construir entornos interoperables desde el diseño.

Planificación progresiva y realismo operativo

Modificar de golpe un entorno OT legado es inviable. Por eso, se recomienda establecer **hojas de ruta específicas** para avanzar hacia la interoperabilidad de forma gradual, priorizando:

- Los activos más expuestos.
- Los entornos de mayor criticidad.
- Las zonas fronterizas entre OT e IT.
- Las plataformas más antiguas o con menor capacidad de actualización.
- Los puntos donde la visibilidad previa ya esté consolidada.

En algunos casos, el uso de **gateways de seguridad**, proxies de protocolo o soluciones de encapsulamiento puede ofrecer una vía intermedia para controlar dispositivos que no pueden modificarse directamente.

Esta planificación debe estar acompañada de una evaluación continua de madurez. Aquí, marcos como **IEC 62443** no solo sirven como referencia técnica, sino también como guía organizativa para evolucionar con solidez y coherencia.

Visibilidad e interoperabilidad: binomio indispensable para la resiliencia

Más allá del cumplimiento normativo, una arquitectura OT visible e interoperable tiene un valor estratégico tangible. Permite:

- Automatizar procesos de supervisión y respuesta.
- Reducir costes operativos al simplificar la gestión.
- Acelerar la adopción de tecnologías como edge computing o IA.
- Centralizar la monitorización y aplicar inteligencia de amenazas de forma coherente.
- Mejorar la capacidad de recuperación ante incidentes mediante acciones coordinadas.
- Fortalecer la colaboración entre equipos IT, OT y de seguridad.

En definitiva, avanzar hacia una visibilidad completa y una interoperabilidad real —especialmente en entornos OT complejos— no es solo una mejora técnica. Es una **decisión estratégica que determina la capacidad de la organización para defenderse, evolucionar y cumplir** con los nuevos marcos regulatorios como NIS2. El primer paso es ver; el siguiente, integrar. Sin ambos, no hay resiliencia posible.

9. De socio a vector de ataque: redefinir la confianza en la cadena

El eslabón débil ya no está dentro: está en manos de terceros

La directiva NIS2 introduce una novedad fundamental respecto a su predecesora: reconoce explícitamente que la seguridad de una organización no puede evaluarse de forma aislada, sino que **depende críticamente del ecosistema de terceros con el que interactúa**. En sectores como el energético y de utilities, esta dependencia se intensifica debido a la complejidad de las infraestructuras y a la necesidad constante de recurrir a fabricantes, integradores, operadores logísticos y proveedores de servicios especializados para mantener la operativa diaria.

Esta realidad ha convertido a la **cadena de suministro en una de las superficies de ataque más relevantes —y más explotadas—** por parte de actores maliciosos. A través de un proveedor comprometido, los atacantes pueden introducirse en redes internas, distribuir malware mediante actualizaciones, alterar procesos de mantenimiento remoto o exfiltrar datos sensibles. Algunos de los ciberincidentes más notorios de los últimos años (como el ataque a SolarWinds o los casos de ransomware distribuidos a través de software de gestión) se produjeron precisamente por este tipo de brechas.

La dificultad principal reside en que las organizaciones **no siempre tienen visibilidad ni capacidad de control sobre los sistemas de sus proveedores**. Muchos entornos OT aún permiten conexiones remotas sin segmentación específica, acceso directo a equipos de campo sin autenticación fuerte, o intercambios de datos sin cifrado. A ello se suma la frecuente rotación de proveedores, la falta de procesos estandarizados para su evaluación en términos de ciberseguridad, y una cultura de confianza implícita ("lleva años trabajando con nosotros") que choca de lleno con las exigencias de diligencia debida que impone NIS2.

Esta heterogeneidad, especialmente grave en ecosistemas industriales con decenas o centenares de terceros implicados, plantea retos específicos:

- Proveedores con niveles muy dispares de madurez digital y ciberseguridad.
- Sistemas operativos de dispositivos IoT sin garantías de actualización ni soporte.
- Pliegos técnicos de adquisición que no incorporan requisitos alineados con NIS2.
- Falta de estandarización mínima en medidas de protección, cifrado o control de accesos.

Para afrontar este reto de forma estructurada, las organizaciones deben adoptar una **estrategia de seguridad de la cadena de suministro** basada en cinco ejes fundamentales:

Clasificación de proveedores según criticidad

No todos los terceros representan el mismo nivel de riesgo. Es necesario segmentar a los proveedores según el tipo de acceso que tienen (lógico, físico, remoto), la criticidad de los activos que gestionan, la frecuencia de su interacción y el grado de integración en los procesos operativos. Esta clasificación permite priorizar recursos de supervisión y definir requisitos diferenciados según el perfil de riesgo.

Evaluación de ciberseguridad como parte del proceso de homologación

Antes de incorporar un nuevo proveedor, debe exigirse información sobre su postura de seguridad: políticas internas, certificaciones (como **ISO 27001**, **IEC 62443** o **TISAX**), histórico de incidentes, procedimientos de gestión de vulnerabilidades, etc. Esta evaluación puede incluir cuestionarios, auditorías, simulacros de ataque controlado (red teaming) o el uso de plataformas de risk scoring basadas en OSINT.

Cláusulas contractuales específicas de ciberseguridad

Los contratos con terceros deben incorporar obligaciones claras en materia de seguridad, incluyendo la obligación de notificar incidentes, permitir auditorías, mantener actualizaciones de software, cifrar las comunicaciones, establecer controles de acceso y definir quién es responsable de qué en caso de incidente. Es esencial definir consecuencias ante el incumplimiento, y prever mecanismos de respuesta conjunta.

Supervisión continua y detección temprana

La relación con los proveedores no termina tras la firma del contrato. Debe existir una **monitorización** constante de su actividad cuando interactúan con el entorno interno, especialmente en conexiones remotas o servicios críticos. Soluciones como los jump servers con control de sesión, la tokenización de accesos, o la supervisión del tráfico de red procedente de terceros, ayudan a detectar comportamientos anómalos y minimizar el impacto de accesos no autorizados.

Integración de los proveedores en la estrategia de resiliencia

Los terceros deben ser considerados parte del sistema, no una externalidad. Esto implica incluirlos en los planes de continuidad de negocio, en los escenarios de **respuesta ante incidentes**, en los **ejercicios de simulacro** y en las **políticas de formación y concienciación**. El objetivo no es únicamente reducir su riesgo, sino asegurar que pueden colaborar de forma efectiva si se produce un incidente.

Adicionalmente, debe asumirse que el problema no es únicamente técnico, sino de **gobernanza**. La gestión segura de la cadena de suministro exige **coordinación entre departamentos de compras, legal, IT, OT y ciberseguridad**, y requiere establecer un marco común que supere los enfoques aislados. Del mismo modo, en casos en los que se utilicen plataformas de terceros en la nube o soluciones SaaS, es fundamental revisar los SLA, la arquitectura de compartición de datos, y la jurisdicción en la que operan los servicios.

Por último, debe evitarse caer en la trampa de **"controlar lo que no se puede controlar"**. Hay proveedores que no aceptarán auditorías, equipos que no pueden modificarse, o situaciones en las que el riesgo debe ser asumido por necesidad operativa. En esos casos, lo esencial es reconocer el riesgo, documentarlo y definir medidas compensatorias: segmentación adicional, monitorización reforzada, planes de contingencia o límites contractuales.

En resumen, la cadena de suministro no puede seguir siendo el eslabón débil de la ciberseguridad. NIS2 obliga a mirarla con nuevos ojos: como parte integrante del sistema, como fuente potencial de vulnerabilidades, y como espacio prioritario de acción para reducir la exposición real de las organizaciones del sector energético y de utilities.

10. Formación más allá de la alta dirección: extender cultura, competencias y compromiso

Si no llega a todos los niveles, la seguridad se queda en el papel

Extender la cultura de ciberseguridad a todos los niveles

Uno de los aspectos más relevantes —y a menudo menos desarrollados— de cualquier estrategia de ciberseguridad es la **formación continua**. Aunque la directiva NIS2 establece explícitamente la responsabilidad de la alta dirección en la supervisión de las políticas de seguridad y la necesidad de que reciba formación adecuada, limitar el esfuerzo formativo a los niveles ejecutivos es, en el mejor de los casos, insuficiente. La eficacia real se alcanza solo cuando la **cultura de ciberseguridad** permea toda la organización, desde la presidencia hasta el operario en planta, pasando por los mandos intermedios, las áreas técnicas, el personal administrativo y los proveedores clave.

El desafío es estructural: muchas organizaciones abordan la formación como una obligación puntual, una casilla que hay que marcar una vez al año. Pero en un entorno donde las amenazas evolucionan semanalmente, los entornos digitales cambian constantemente y las decisiones individuales pueden tener un impacto directo en la continuidad del negocio, se impone un **modelo de capacitación continua, segmentada, actualizada y adaptada al rol** de cada persona en la organización.

Este enfoque requiere abandonar la lógica de las formaciones genéricas. Un técnico de mantenimiento en un entorno OT no necesita el mismo contenido que un administrativo que gestiona licitaciones públicas, ni que un ingeniero de telecomunicaciones, ni que un directivo del comité de riesgos. Cada uno de ellos se enfrenta a vectores distintos de exposición, toma decisiones con impactos diferentes y requiere competencias específicas. Por tanto, los programas de formación deben diseñarse a medida, teniendo en cuenta:

- El análisis funcional de cada puesto
- El nivel de exposición a riesgos
- Las competencias actuales del perfil
- El tipo de decisiones que toma
- El impacto que pueden tener sus errores

Y deben utilizar diferentes formatos (cursos presenciales, contenidos online, simulaciones, píldoras formativas, pruebas prácticas o ejercicios de red teaming) con un enfoque orientado a la aplicación real.

En el caso de los entornos industriales, por ejemplo, se han identificado brechas significativas en la comprensión de los riesgos asociados al uso de dispositivos externos (como USB o portátiles no autorizados), en la validación de actualizaciones de firmware, o en la gestión de accesos temporales de contratistas. En muchos incidentes reales, el vector de entrada ha estado en decisiones aparentemente inofensivas tomadas por personal no especializado. Por eso es fundamental que la formación en OT no se limite a lo técnico, sino que incorpore **protocolos operativos seguros**, gestión de anomalías, concienciación sobre ingeniería social y pautas claras para la comunicación de incidencias.

En el otro extremo, la alta dirección no puede delegar la seguridad en los responsables técnicos. NIS2 establece que los máximos responsables de la organización pueden ser **legalmente responsables del incumplimiento** de las obligaciones de gestión del riesgo. Por ello, su formación debe ir más allá de las generalidades y centrarse en tres áreas clave:

- Comprensión del marco regulatorio y consecuencias jurídicas
- Gobernanza estratégica del riesgo, como parte de la toma de decisiones del negocio
- Evaluación e impulso de inversiones en ciberseguridad, con perspectiva de retorno y sostenibilidad

Además, existe una capa intermedia —los mandos, jefes de proyecto, coordinadores de área— que habitualmente no son objeto de programas formativos específicos, pero que actúan como bisagra organizativa. Son quienes ejecutan presupuestos, aprueban proveedores, definen requerimientos técnicos o gestionan personas. Sin una cultura de seguridad sólida en estos niveles, el despliegue de cualquier estrategia transversal se debilita. Invertir en su capacitación es uno de los movimientos más rentables en términos de impacto organizativo.

Otra línea estratégica clave es la inclusión de los proveedores críticos en los programas de formación y sensibilización. NIS2 exige a las organizaciones garantizar no solo su propia seguridad, sino también la de su cadena de suministro. En este contexto, **extender la cultura de seguridad más allá del perímetro organizativo** no es una opción, sino una obligación. Algunas empresas del sector ya han comenzado a diseñar programas formativos específicos para proveedores estratégicos, incluyéndolos en simulacros, ofreciéndoles recursos compartidos o estableciendo requisitos formativos en los contratos marco.

Por último, toda estrategia formativa debería ir acompañada de mecanismos de **evaluación y mejora continua**. Algunos mecanismos eficaces de seguimiento incluyen:

- Encuestas de autoevaluación y test periódicos
- Simulacros y ejercicios de red teaming
- Métricas como la tasa de clic en campañas de phishing simuladas
- Monitorización de incidentes atribuidos a error humano
- Evolución de indicadores de concienciación

No se trata solo de formar, sino de generar una cultura viva de aprendizaje permanente en torno a la seguridad.

Formar es, en última instancia, empoderar. Y una organización segura no es la que tiene más herramientas técnicas, sino la que cuenta con personas que saben cómo prevenir, detectar, reaccionar y aprender. Extender ese conocimiento de forma estructurada, continua y alineada con los riesgos reales es una de las formas más eficaces de cumplir con NIS2... y de construir resiliencia operativa a largo plazo.

Resultados esperados

La aplicación sistemática del decálogo planteado en este informe permite a las organizaciones del sector energético y de utilities abordar la adaptación a la directiva NIS2 de forma proactiva, estructurada y con una visión de conjunto. No se trata únicamente de cumplir con una nueva obligación normativa, sino de aprovechar el marco que impone NIS2 como una oportunidad para elevar el nivel de madurez organizativa en materia de ciberseguridad. Los beneficios esperados pueden agruparse en cinco grandes dimensiones:

Cumplimiento normativo y reducción del riesgo jurídico

El primer resultado, y quizá el más inmediato, es la capacidad de demostrar un cumplimiento diligente ante la entrada en vigor de NIS2. Aplicar las recomendaciones del decálogo permite generar evidencia documental y operativa que acredita el alineamiento con los requisitos de la directiva, especialmente en lo relativo a gobernanza, gestión de riesgos, seguridad de la cadena de suministro, respuesta ante incidentes y formación. Esto reduce significativamente el riesgo de sanciones, responsabilidades personales en la alta dirección o pérdida de licencias en el caso de operadores de servicios esenciales.

Fortalecimiento de la resiliencia técnica y operativa

Desde el punto de vista técnico, el decálogo promueve una mejora sustancial en la visibilidad, control y protección de activos críticos, con especial foco en entornos OT. La interoperabilidad a nivel de dispositivo, la gestión activa del Shadow IT, la segmentación de redes, la detección temprana de anomalías y la adopción de políticas de seguridad integradas entre IT y OT se traducen en una reducción efectiva de la superficie de ataque, una mayor capacidad de contención y una mejora en los tiempos de recuperación ante incidentes.

Evolución del modelo organizativo y ruptura de silos

A nivel interno, la aplicación del decálogo conlleva un cambio profundo en la forma de organizar la seguridad. La ciberseguridad deja de ser una función aislada del área de IT para convertirse en una responsabilidad compartida que conecta operaciones, negocio, tecnología y gobierno corporativo. Esto se refleja en la creación de estructuras más transversales, en la aparición de nuevos roles intermedios y en la formalización de políticas comunes que superan las tradicionales divisiones

Transformación cultural y compromiso colectivo

Uno de los elementos menos tangibles, pero más transformadores, es la evolución del mindset organizativo. Integrar la seguridad en la cultura empresarial —desde el comité de dirección hasta el personal de campo— permite generar un entorno de corresponsabilidad, donde los riesgos se comprenden, se gestionan y se comunican con naturalidad. Esta transformación no solo facilita la implementación de medidas técnicas, sino que refuerza la confianza interna y el sentido de propósito común frente a un reto complejo y compartido.

Mejora de la posición competitiva y reputacional

Finalmente, las organizaciones que lideran la adaptación a NIS2 no solo ganan en cumplimiento o eficiencia, sino también en reputación. La capacidad de garantizar la continuidad del servicio, proteger infraestructuras críticas y colaborar de forma segura con terceros se convierte en un activo estratégico en un contexto marcado por la interdependencia, la supervisión creciente y la presión de la opinión pública. Esto puede traducirse en ventajas competitivas en licitaciones, alianzas o proyectos estratégicos que requieran altos niveles de fiabilidad y gobernanza.

En conjunto, el decálogo no debe entenderse como una lista de tareas técnicas, sino como un plan de transformación estructural que permite pasar de una ciberseguridad reactiva y fragmentada a un modelo integrado, anticipativo y alineado con los objetivos de sostenibilidad, innovación y continuidad que hoy definen el futuro del sector.

Conclusiones

La entrada en vigor de la directiva NIS2 representa un punto de inflexión en la forma en que las organizaciones, y especialmente las del sector energético y de utilities, deben concebir su estrategia de seguridad. No se trata únicamente de adaptarse a una nueva norma europea ni de evitar sanciones mediante el cumplimiento formal de unos requisitos. Se trata de redefinir el papel de la ciberseguridad en la estructura, la cultura y el modelo de operación de las organizaciones que prestan servicios esenciales.

En este nuevo escenario, la seguridad deja de ser un componente técnico subordinado para convertirse en un eje estratégico de primer orden. NIS2 no solo plantea qué debe hacerse, sino también quién debe implicarse, cómo debe gobernarse, y con qué grado de responsabilidad y trazabilidad deben tomarse las decisiones que afectan a la resiliencia digital. Las direcciones generales, los consejos de administración y los órganos reguladores adquieren un rol más activo, con responsabilidades legales explícitas y un mandato claro de transformación.

El decálogo de recomendaciones recogido en este informe ha sido diseñado precisamente desde esa visión: no como una guía puramente técnica, sino como un marco orientado a la madurez, la coherencia y la anticipación. Se abordan aspectos estructurales —como la gobernanza, la integración de IT/OT o la relación con la cadena de suministro— que requieren una revisión profunda de los modelos actuales, y se apuesta por una visión proactiva que entiende la ciberseguridad como un proceso continuo y transversal, no como un ejercicio puntual de cumplimiento.

Esta transformación no es homogénea ni instantánea. Dependerá del punto de partida de cada organización, de su cultura, su grado de exposición y su capacidad de liderazgo interno. Pero sí hay una constante: quienes entiendan la directiva como una oportunidad y no como una imposición estarán mejor posicionados para ganar legitimidad ante los reguladores, generar confianza en sus stakeholders y consolidar su papel como referentes en un ecosistema energético cada vez más digital, interconectado y expuesto.

En este sentido, NIS2 debe entenderse como un catalizador de cambio estructural. Un impulso normativo que obliga a tomar decisiones estratégicas, pero que también habilita nuevos niveles de eficiencia, control y colaboración. Cumplir con la directiva es imprescindible, pero aprovechar su marco para evolucionar hacia modelos de ciberresiliencia más integrados, inteligentes y sostenibles es, sin duda, el verdadero valor añadido que está en juego.

La ciberseguridad, en este contexto, no es un coste ni una carga: es una capacidad crítica para la continuidad del servicio, la protección de infraestructuras clave y la confianza social en un sector que es esencial para todo lo demás.

ANEXO:
Marcos normativos, certificaciones y frameworks de referencia

A lo largo del presente informe se han mencionado diversos marcos legales, normativos y de buenas prácticas que constituyen el entorno regulador y técnico de referencia para las organizaciones del sector energético y de utilities en el contexto de la ciberseguridad. Este anexo tiene como objetivo recopilar y contextualizar dichos elementos para facilitar su consulta e interpretación:

Normativas europeas y nacionales

Directiva NIS (UE) 2016/1148

Primera normativa europea en materia de ciberseguridad, dirigida a mejorar el nivel global de seguridad de las redes y sistemas de información en la UE. Su enfoque estaba centrado en operadores de servicios esenciales y proveedores de servicios digitales.

Directiva NIS2 (UE) 2022/2555

Sustituye a la directiva NIS original, ampliando su ámbito de aplicación, reforzando las obligaciones de gobernanza, gestión de riesgos y supervisión, y endureciendo el régimen sancionador. Exige una implicación explícita de los órganos de dirección en materia de ciberseguridad. Su transposición al ordenamiento jurídico español está en proceso.

Esquema Nacional de Seguridad (ENS)

Marco normativo español que establece los principios y requisitos mínimos de seguridad para el uso de medios electrónicos en el sector público. Es de aplicación también a entidades del sector privado que colaboran con la Administración o gestionan servicios públicos.

Normas y estándares internacionales

ISO/IEC 27001

Norma internacional para sistemas de gestión de seguridad de la información (SGSI). Establece un enfoque basado en riesgos para la protección de datos y activos informáticos. Muy extendida en el ámbito corporativo y en procesos de certificación.

IEC 62443

Conjunto de estándares internacionales desarrollados específicamente para la ciberseguridad de sistemas de automatización y control industrial (IACS). Incluye requisitos tanto técnicos como organizativos, con un enfoque estructurado por roles (operadores, integradores, fabricantes).

NIST SP 800-82

Guía del Instituto Nacional de Estándares y Tecnología de EE. UU. sobre la gestión segura de sistemas de control industrial (ICS), incluyendo recomendaciones técnicas y de buenas prácticas específicas para entornos OT.

FAIR (Factor Analysis of Information Risk)

Marco metodológico para cuantificar y modelar el riesgo de seguridad de la información en términos económicos. Permite priorizar inversiones y decisiones estratégicas sobre una base analítica y comparable.

Contenido relacionado

El Plan de Actividades de la Plataforma enerTIC volverá a abordar temáticas relacionadas con las planteadas en este coloquio en estas actividades y acciones de comunicación.

11 SEP

MADRID

Reunión de Grupos de Trabajo

8-9 OCT

MADRID

Smart Energy Congress 2025

6 NOV

BILBAO

Desayuno – Coloquio: Energéticas e industria: inteligencia artificial para reinventar la eficiencia y la sostenibilidad

20 NOV

MADRID

Foro Tendencias 2025 Regulaciones, competitividad y sostenibilidad: digitalización para las necesidades presentes y futuras

9 DIC

MADRID

Desayuno – Coloquio: Redes e infraestructuras en la transformación de energéticas y utilities: de regulación a sostenibilidad

11 DIC

MADRID

XIII edición enerTIC Awards

Contenido relacionado

Las empresas asociadas a la Plataforma enerTIC.org se caracterizan, entre otros aspectos, por la aportación de soluciones tecnológicamente avanzadas, en diferentes ámbitos/sectores.

A continuación, se presentan Casos de Uso innovadores, ejemplos de cómo la tecnología y la digitalización contribuyen a mejorar la competitividad y la sostenibilidad en el sector objeto de este Desayuno – Coloquio.

Inteligencia Artificial Generativa que revoluciona el mantenimiento industrial

31/3/25

ayesa

La IA Generativa está revolucionando el mantenimiento industrial al optimizar diagnósticos y reducir tiempos de inactividad. A través de asistentes inteligentes, los técnicos acceden rápidamente a información relevante, mejorando la eficiencia y reduciendo costes.

Grupo Holcim apuesta por la tecnología de Nutanix para impulsar su compromiso con la sostenibilidad en el sector de la construcción

11/4/25

NUTANIX

El Grupo Holcim ha modernizado su infraestructura TI en la región EMEA con una plataforma de hiperconvergencia basada en Nutanix, mejorando la eficiencia, seguridad y sostenibilidad. La solución permite escalar servicios de forma flexible, automatizar operaciones críticas y reducir significativamente la huella de carbono.

Optimización de rutas para mejorar la eficiencia energética

29/4/25

berocam

Una empresa industrial se enfrentaba al reto de optimizar sus rutas de distribución con un enfoque claro en el ahorro energético. Desarrollamos un modelo que combinaba algoritmos heurísticos con seguimiento en tiempo real y recálculo dinámico de rutas. Esta solución no solo ha permitido reducir el consumo energético y las emisiones de CO , también mejorar la productividad y ofrecer una mejor experiencia de cliente.

Gemmo impulsa su transformación digital con una solución EMS basada en N3uron

20/5/25

N3uron

Gemmo ha transformado su gestión energética al implementar N3uron, reduciendo la latencia de datos a menos de 15 minutos y permitiendo análisis en tiempo real para una toma de decisiones más ágil y eficiente.

Los beneficios de los Gemelos Digitales Industriales

21/3/25

HEXAGON

En 2025, la industria afronta desafíos clave, y el 72% de los ejecutivos apuesta por los gemelos digitales para mejorar eficiencia y reducir costos.

¿Puede la digitalización industrial impulsar la transición hacia la descarbonización y la competitividad?

25/2/25

sener

La digitalización industrial se posiciona como el pilar para transformar procesos y potenciar la competitividad, permitiendo optimizar desde el consumo energético hasta la gestión de recursos productivos.

El Futuro de la Industria: Cómo la digitalización hace crecer la eficiencia y el negocio

25/2/25

ECOMT

Mejor gestión de riesgos, ahorro de costes y sostenibilidad con tecnología digital.

La eficiencia energética y la digitalización, claves en el sector industrial

25/2/25

getronics

La electrificación y digitalización industrial ya no son tendencias futuras, sino una realidad en marcha. Las empresas que lideren esta transformación no solo estarán mejor preparadas para cumplir con las regulaciones ambientales, sino que serán más eficientes, rentables y competitivas.

Transformando la Industria: Retos y Oportunidades en la Descarbonización

24/2/25

kyndryl

La descarbonización de la industria europea, y en especial la española, requiere un enfoque dual: reducir progresivamente las emisiones de CO_2 y acelerar la adopción de materias primas y energías no fósiles.

La importancia del Sistema HVAC en la climatización industrial, ¿cómo funciona?

24/2/25

ENGIE

La transición hacia sistemas HVAC más sostenibles responde a los objetivos de eficiencia energética y responsabilidad ambiental que las empresas buscan alcanzar hoy en día.

Acerca de enerTIC

La Plataforma enerTIC.org tiene por misión contribuir al desarrollo y ejecución de la transformación energética y digital en España, en favor de una economía más competitiva y sostenible. Para ello, cuenta con el apoyo de sus empresas asociadas y una extensa red de colaboradores institucionales.

Desde su creación en 2011, la Plataforma trabaja para impulsar el conocimiento y la divulgación de soluciones tecnológicas e innovadoras, apostando fuertemente por la digitalización para la mejora significativa de la competitividad energética y, con ello, la competitividad de sectores clave como el Energético, la Industria, el Transporte o los Servicios Públicos. En los tiempos actuales, afrontamos un nuevo Paradigma de la Sostenibilidad, en el que las compañías energéticas, las industrias y la administración pública deben abordar grandes retos para alcanzar los objetivos de descarbonización, sostenibilidad y competitividad energética, marcados para 2030. Para ello, deben apoyarse en las soluciones aportadas por el propio sector energético, las tecnológicas y bajo el paraguas de la innovación abierta. Consiguiendo, de este modo, adaptarse a las nuevas exigencias de clientes e inversores por la sostenibilidad, la reducción de costes de la energía y el cumplimiento de las nuevas regulaciones.

Para afrontar estos grandes desafíos, enerTIC.org trabaja intensamente junto a sus empresas asociadas, siendo dinamizadores y facilitadoras, fomentando tres aspectos clave: la concienciación, la promoción y difusión de tecnologías, y el fomento de la colaboración entre los diferentes stakeholders.

Otros Informes:

Retos y oportunidades en la Industria logística Gran Consumo y Distribución: Innovación, eficiencia energética y nuevas tecnologías

ABR 2022

Retos y oportunidades en el Sector Energético: Transición hacia un nuevo modelo descarbonizado, eficiente y sostenible

MAY 2022

Retos y oportunidades en la Transición hacia un nuevo modelo de Centro de Datos: Hiperescala, sostenibilidad y eficiencia energética

JUN 2022

Retos y oportunidades en la Transición hacia un nuevo modelo de industria: Sector manufacturero

JUL 2022

Retos y oportunidades en la Transición hacia un nuevo modelo de ciudad: Transporte Inteligente y movilidad del futuro

OCT 2022

Retos y oportunidades en la Transición hacia un nuevo modelo de industria: Sectores Automoción, Aeronáutico, Marítimo y Ferroviario

DIC 2022

Innovación y digitalización de las redes de distribución eléctricas ante el nuevo reto energético: Retos y oportunidades

MAR 2023

Nuevos retos y oportunidades en el avance de la transformación de las ciudades hacia ecosistemas inteligentes y bajos en carbono

MAR 2024

Nuevos retos y oportunidades en el avance de la transformación del sector energético: distribución y comercialización de la energía

ABR 2024

La Plataforma tiene un amplio programa de actividades anuales para fomentar la dinamización del mercado, la divulgación de las tecnologías, relaciones entre directivos, etc.

Consulte aquí el álbum fotográfico de algunas actividades realizadas

Asociados enerTIC

Asociados destacados

Asociados

INTELIGENCIA ARTIFICIAL:
REIMAGINANDO LA SOSTENIBILIDAD

Smart Energy Congress.eu

8 y 9 OCTUBRE 2025 | IFEMA

Prepárate para ser parte del cambio: el Smart Energy Congress 2025 es mucho más que un evento, es el escenario donde la inteligencia artificial y las tecnologías habilitadoras se encuentran con los líderes del futuro para transformar desafíos en oportunidades. Descubre cómo optimizar recursos, impulsar alianzas estratégicas y ser protagonista de la revolución de la eficiencia energética y la sostenibilidad. Únete al congreso que marca el camino hacia un futuro más eficiente, conectado y resiliente. ¡El momento de reimaginar la sostenibilidad es ahora!

#SEC2025Madrid

ORGANIZA

enerTIC

Agenda e Inscripción gratuita en www.SmartEnergyCongress.eu

MÁS INFORMACIÓN > SEC2025@enerTIC.org - Tel. 912 794 825