



GRADO EN INGENIERÍA EN TECNOLOGÍAS INDUSTRIALES

TRABAJO FIN DE GRADO

**Impacto de la nueva directiva europea de ciberseguridad  
NIS2 en sectores industriales españoles. Casos de  
aplicación: sector ferroviario y sector eólico.**

Autor: Pablo Pacho Garcia

Director: Daniel Fernández Alonso

Madrid, julio 2024

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título  
Impacto de la nueva directiva europea de ciberseguridad NIS2 en sectores industriales  
españoles, poniendo como caso de aplicación el control de un parque eólico, y si es  
posible, de un tren.

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el  
curso académico 05/2024 es de mi autoría, original e inédito y  
no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido  
tomada de otros documentos está debidamente referenciada.

Fdo.: Pablo Pacho

Fecha: ...31.../ ...07.../ ...2024...

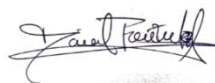


Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Fdo.: Daniel Fernández Alonso

Fecha: ...13.../ ...08.../ ...2024...



# IMPACTO DE LA NUEVA DIRECTIVA EUROPEA DE CIBERSEGURIDAD NIS2 EN SECTORES INDUSTRIALES ESPAÑOLES. CASOS DE APLICACIÓN: SECTOR FERROVIARIO Y SECTOR EÓLICO.

**Autor: Pacho García, Pablo**

Director: Fernández Alonso, Daniel.

Entidad Colaboradora: ICAI – Universidad Pontificia Comillas.

## **RESUMEN DEL PROYECTO**

### **Introducción**

El presente trabajo se centra en el análisis y la evaluación del impacto de la nueva Directiva NIS2 de la Unión Europea en sectores industriales críticos en España, específicamente en el sector ferroviario y eólico. La Directiva NIS2 es una evolución de la Directiva NIS1, con un alcance ampliado y requisitos más estrictos en materia de ciberseguridad para asegurar las infraestructuras críticas. Este proyecto nace de la necesidad imperante de fortalecer las defensas cibernéticas en un entorno cada vez más digitalizado y vulnerable a ciberataques, cuya frecuencia y sofisticación han crecido exponencialmente en los últimos años.

La motivación principal de este trabajo radica en la creciente amenaza que los ciberataques representan para las infraestructuras críticas, como los sistemas de energía y transporte. Estas infraestructuras son vitales para la sostenibilidad y desarrollo económico, y su interrupción puede tener consecuencias desastrosas tanto a nivel económico como para la seguridad nacional y el bienestar social. Con la implementación de la Directiva NIS2, la Unión Europea busca garantizar un nivel común de seguridad en los sistemas de información y redes, imponiendo obligaciones a las entidades responsables de estas infraestructuras para que adopten medidas de ciberseguridad robustas y notificando cualquier incidente significativo a las autoridades competentes.

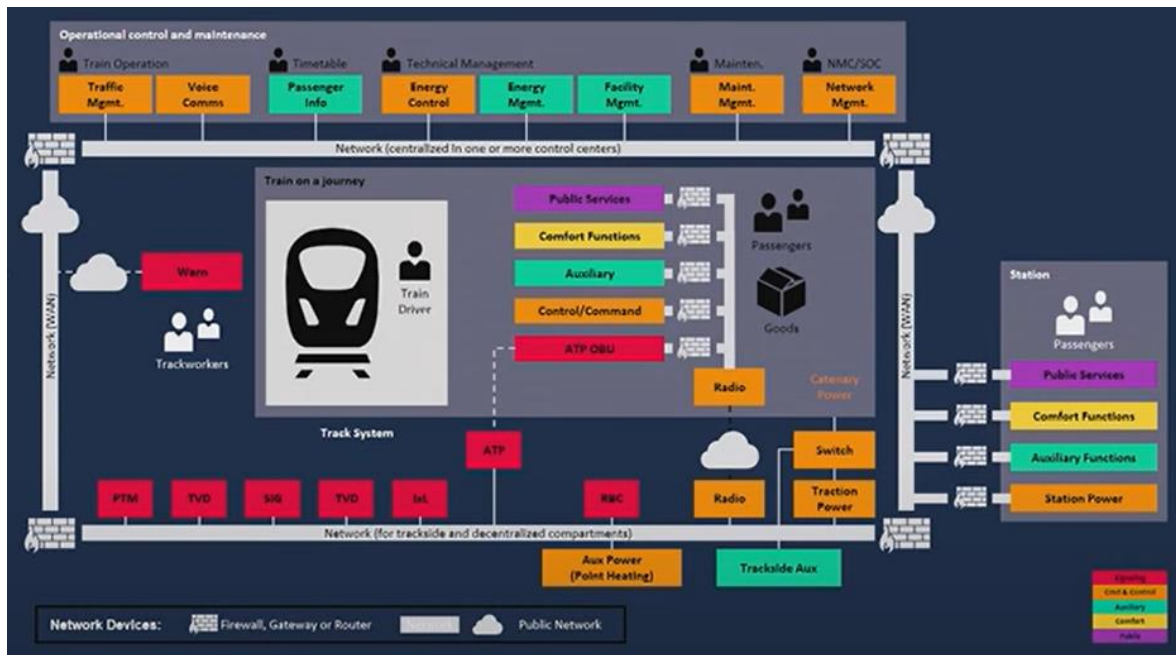
El trabajo también aborda los desafíos que supone la implementación de esta normativa, desde la adaptación de infraestructuras heredadas que no fueron diseñadas con la ciberseguridad en mente, hasta la necesidad de capacitar al personal en nuevas prácticas de seguridad. La digitalización creciente en sectores como el eólico y el ferroviario ha incrementado la superficie de ataque, exponiendo a estos sistemas a riesgos que podrían comprometer su operación y seguridad. Por ello, el proyecto se enfoca en proponer soluciones prácticas y adaptadas que no solo aseguren el cumplimiento de la Directiva NIS2, sino que también fortalezcan la resiliencia de estas infraestructuras frente a ciberamenazas.

En cuanto a la ciberseguridad industrial, se subraya la importancia de integrar tecnologías avanzadas, como la inteligencia artificial y la automatización, que si bien han mejorado la eficiencia y productividad, también han incrementado la exposición a ataques cibernéticos. En este contexto, el proyecto establece un marco claro para la implementación de la Directiva NIS2 en los sectores eólico y ferroviario, evaluando sus vulnerabilidades específicas y desarrollando estrategias de mitigación. Asimismo, se analizan los costos y beneficios asociados a las medidas de ciberseguridad propuestas, promoviendo la colaboración entre empresas y autoridades regulatorias para facilitar el cumplimiento de la normativa.

La contribución de este trabajo se materializa en la creación de una guía detallada para la implementación de la NIS2 en estos sectores críticos, basándose en estudios de casos reales y mejores prácticas. Se espera que las estrategias desarrolladas sirvan como modelo para otras industrias, fortaleciendo la capacidad de las infraestructuras críticas para resistir y recuperarse de ciberataques, asegurando así la continuidad de los servicios esenciales.

### **Sector ferroviario**

El sector ferroviario, al igual que otros sectores críticos, enfrenta desafíos significativos en términos de ciberseguridad, especialmente en un contexto de creciente digitalización y conectividad. A medida que la infraestructura ferroviaria se vuelve más dependiente de sistemas digitales para la operación de trenes, control de señales, gestión de tráfico y servicios a los pasajeros, aumenta la superficie de ataque potencial y el impacto de posibles incidentes de ciberseguridad. Esta situación se ve agravada por la complejidad inherente de los sistemas ferroviarios, que integran múltiples subsistemas interconectados, desde los controles de frenos y velocidad hasta los sistemas de información para pasajeros y los servicios de videovigilancia, mostrados a continuación:



*Ilustración 1: Diagrama del sistema de un tren, en el cual cada una de las cajitas representa un subsistema dentro de un modelo ideal. La parte en rojo muestra los sistemas más críticos, es decir, los sistemas de señalización del tren, que es lo que se encarga de evitar que haya colisiones entre estos. La parte naranja son los sistemas de control (frenos, velocidad, etc.). Por otro lado, tenemos sistemas auxiliares, sistemas de confort, y servicio que se puedan proporcionar a los pasajeros. Fuente: Vídeo de Omar Benjumea, Siemens Mobility.*

Históricamente, el sector ha sido testigo de incidentes que han tenido consecuencias graves, no solo en términos de interrupciones del servicio, sino también en términos de seguridad física para los pasajeros, como lo demuestra el incidente de un tranvía en Polonia en 2008. Estos eventos subrayan la necesidad crítica de implementar medidas robustas de ciberseguridad que cumplan con las normativas vigentes, como la Directiva NIS2.

Para adaptarse a esta directiva, el sector ferroviario debe llevar a cabo una serie de acciones estratégicas. En primer lugar, es esencial realizar una evaluación exhaustiva de los riesgos cibernéticos, identificando vulnerabilidades específicas en los sistemas de control de trenes y en otras infraestructuras críticas, como los centros de control y los sistemas de comunicación. Este proceso implica no solo la identificación de posibles amenazas, sino también la implementación de medidas de mitigación adecuadas, que podrían incluir desde la actualización de sistemas de señalización hasta la integración de tecnologías avanzadas de detección y respuesta.

Un ejemplo destacado en este contexto es Deutsche Bahn, la principal empresa ferroviaria de Alemania, que ha llevado a cabo revisiones exhaustivas de sus sistemas para identificar

y abordar vulnerabilidades. Esto ha incluido la implementación de medidas de autenticación multifactorial para proteger los accesos a sistemas críticos y el desarrollo de un plan de respuesta ante incidentes de ciberseguridad. Además, Deutsche Bahn ha participado activamente en redes de cooperación y compartición de inteligencia cibernética con otros operadores ferroviarios europeos, lo que ha fortalecido significativamente su postura de ciberseguridad.

La adaptación a la Directiva NIS2 también requiere la revisión de los estándares de ciberseguridad actualmente implementados en el sector ferroviario. Estándares como ISO/IEC 27001, IEC 62443, TS 50701, y NIST SP 800-53, aunque ampliamente utilizados, necesitan ser adaptados para cubrir todas las áreas críticas del sistema ferroviario. Por ejemplo, mientras que IEC 62443 ya se aplica en sistemas de control industrial, no todos los subsistemas ferroviarios lo han implementado completamente, lo que requiere una mayor expansión de su alcance.

Otro aspecto crucial es el desarrollo de capacidades internas robustas, lo que implica la formación continua del personal en ciberseguridad y la realización de simulacros regulares para mejorar la respuesta a incidentes. La capacitación no solo debe incluir a los operadores de trenes, sino también al personal de TI y a otros empleados que puedan estar involucrados en la gestión de incidentes.

Finalmente, es fundamental establecer mecanismos de colaboración y compartición de información con otros actores del sector. Participar en redes de cooperación, firmar acuerdos de colaboración y participar en ejercicios conjuntos de ciberseguridad son estrategias clave para fortalecer la resiliencia del sector ferroviario frente a ciberamenazas. Estos esfuerzos, como se ha demostrado en Deutsche Bahn, no solo aseguran el cumplimiento de la Directiva NIS2, sino que también mejoran la seguridad y eficiencia operativa en un entorno cada vez más digitalizado .

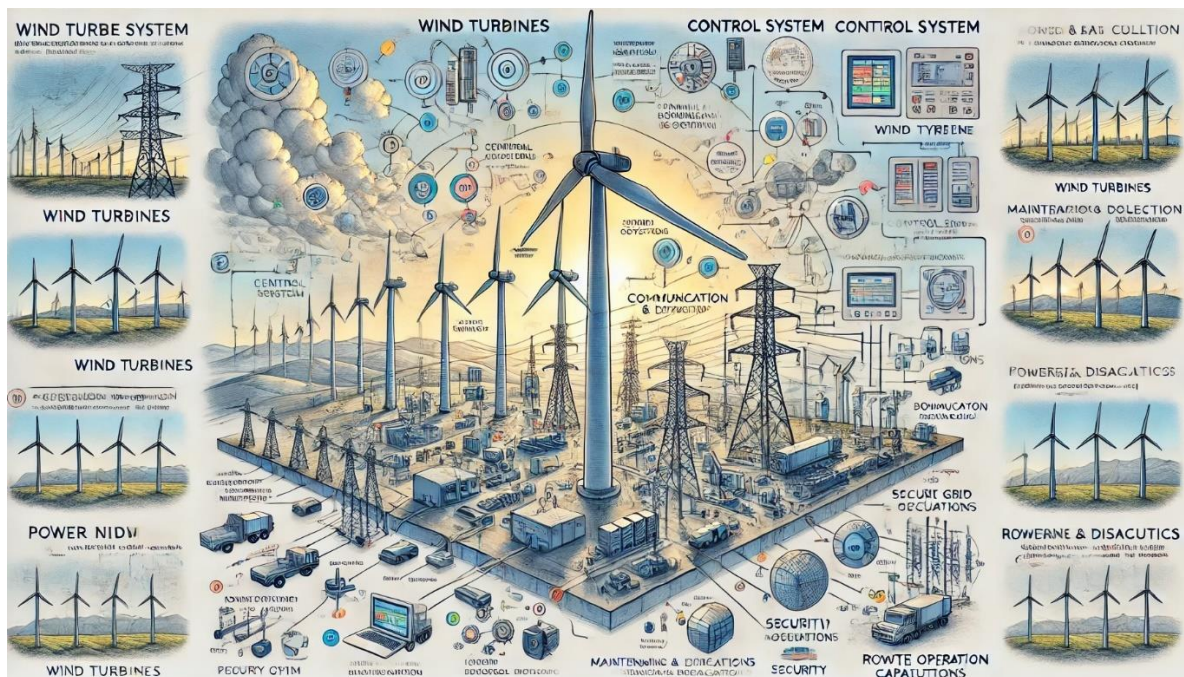
En cuanto a la estimación de costos para la implementación de la Directiva NIS2 en el sector ferroviario, se ha calculado un coste total de aproximadamente 209.000 € para una empresa que fabrica trenes y los comercializa. Este coste incluye:

| <b>Tipo de coste</b>                          | <b>Cantidad (€)</b> |
|-----------------------------------------------|---------------------|
| Evaluación de conformidad y Gap Analysis      | 25.000              |
| Revisión de estándares actuales               | 72.000              |
| Refuerzo de la gestión de incidentes          | 20.000              |
| Mejora de la resiliencia operativa            | 45.000              |
| Capacitación y concienciación                 | 32.000              |
| Establecimiento de mecanismos de colaboración | 15.000              |
| <b>Total</b>                                  | <b>209.000</b>      |

*Tabla 1: Coste desglosado adaptación sector ferroviario a directiva NIS2. Fuente: elaboración propia.*

## Sector eólico

El sector eólico, clave en la transición hacia fuentes de energía renovables, se enfrenta a desafíos cada vez mayores en materia de ciberseguridad debido a la creciente digitalización y conectividad de sus operaciones. La integración de tecnologías avanzadas en la gestión y operación de parques eólicos ha mejorado significativamente la eficiencia y ha permitido un control más preciso de las turbinas. Sin embargo, esta misma digitalización ha incrementado la exposición a ciberamenazas, haciendo que la protección de las infraestructuras críticas sea más urgente que nunca. Esta urgencia se ve alimentada por la complejidad y la interconexión de estos subsistemas que conforman un parque eólico, a continuación, mostrados en este diagrama:



*Ilustración 2: Diagrama de los subsistemas de un parque eólico, que trabajan en conjunto para generar y distribuir energía. Cada uno de estos subsistemas desempeña un papel crucial en la operación del parque.*

*Fuente: Chat GPT.*

La Directiva NIS2, diseñada para reforzar la ciberseguridad en toda la Unión Europea, impone nuevas obligaciones a los operadores de infraestructuras críticas, incluyendo los parques eólicos. A diferencia de su predecesora, la NIS1, esta nueva directiva no solo amplía el alcance de los sectores cubiertos, sino que también establece requisitos más estrictos en cuanto a la gestión de riesgos y la respuesta a incidentes. Los operadores de parques eólicos deben ahora asegurar que sus sistemas de control, como los sistemas SCADA (Supervisory



Control and Data Acquisition), estén adecuadamente protegidos contra ciberataques, ya que estos sistemas son fundamentales para el monitoreo y la operación de las turbinas.

Uno de los primeros pasos en la adaptación a la Directiva NIS2 es la realización de una evaluación exhaustiva de la infraestructura existente en los parques eólicos. Esta evaluación debe identificar todas las vulnerabilidades y áreas de mejora en los sistemas actuales, prestando especial atención a los puntos de acceso que podrían ser explotados por atacantes. Los sistemas SCADA, en particular, requieren un análisis detallado, ya que su naturaleza interconectada los hace especialmente susceptibles a ciberataques. La implementación de medidas de seguridad robustas, como la segmentación de redes, la autenticación multifactorial y el cifrado de datos, es esencial para mitigar estos riesgos.

La protección de los sistemas SCADA no solo implica la implementación de tecnologías de seguridad, sino también la integración de prácticas y procedimientos que aseguren una respuesta rápida y efectiva en caso de un incidente. Esto incluye la creación de planes de contingencia que permitan al operador del parque eólico recuperar la operación normal lo más rápidamente posible, minimizando las interrupciones en el suministro de energía. La resiliencia operativa se convierte así en un aspecto clave para el cumplimiento de la Directiva NIS2, asegurando que incluso en caso de un ataque cibernético, el impacto en la operación del parque sea limitado.

Además de la evaluación y la implementación de medidas de seguridad, la Directiva NIS2 exige una adaptación y expansión de los estándares de ciberseguridad actualmente en uso en el sector eólico. Estándares como ISO/IEC 27001, que cubre la gestión de la seguridad de la información, e IEC 62443, que se enfoca en la protección de los sistemas de control industrial, son esenciales para crear un marco de seguridad robusto. Sin embargo, estos estándares deben ser adaptados para abordar las particularidades de los parques eólicos, que operan en un entorno dinámico y a menudo distribuido geográficamente.

La implementación de estos estándares debe ser acompañada de una revisión continua y de auditorías regulares que aseguren su eficacia a lo largo del tiempo. En este sentido, la Directiva NIS2 promueve una cultura de seguridad proactiva, donde la evaluación de riesgos y la implementación de medidas de seguridad no son acciones puntuales, sino procesos continuos que deben adaptarse a medida que evolucionan las amenazas.

Un aspecto crítico en la adaptación a la NIS2 es la formación del personal. Dado que la ciberseguridad en el sector eólico involucra tanto a técnicos en el campo como a personal de

TI, es esencial que todos los empleados estén capacitados para reconocer y responder a posibles amenazas. Esto incluye no solo la formación técnica sobre cómo operar los sistemas de seguridad, sino también la concienciación sobre las prácticas de seguridad más amplias, como la gestión de contraseñas y la identificación de intentos de phishing.

Además de la capacitación, la participación en redes de ciberseguridad y en ejercicios conjuntos con otras empresas del sector es fundamental para fortalecer la resiliencia ante ciberataques. Estas colaboraciones permiten compartir información sobre amenazas y mejores prácticas, creando una comunidad más robusta frente a las ciberamenazas. Empresas líderes en el sector, como Enercon, han demostrado que la cooperación entre diferentes actores puede ser un factor decisivo en la mejora de la seguridad cibernética.

La adaptación a la Directiva NIS2 también implica una revisión de las políticas internas de seguridad. Esto incluye la actualización de las políticas de acceso y la implementación de controles más estrictos sobre quién puede acceder a los sistemas críticos. En muchos casos, esto requiere una reestructuración completa de los sistemas de gestión de identidades y accesos, asegurando que solo el personal autorizado pueda realizar cambios en los sistemas SCADA y otros sistemas críticos.

Finalmente, es importante destacar que la implementación de la Directiva NIS2 en el sector eólico no es solo una cuestión de cumplimiento normativo, sino una oportunidad para mejorar la resiliencia y la eficiencia operativa. Al adoptar una postura proactiva en ciberseguridad, los operadores de parques eólicos no solo protegen sus activos, sino que también garantizan la continuidad del suministro de energía, que es vital para la economía y la sociedad en general.

En cuanto a la estimación de costos para la implementación de la Directiva NIS2 en el sector eólico, tomando como ejemplo un parque eólico de 3 MW, con 15 turbinas eólicas, el coste estimado, calculado para cada molino por separado, y multiplicado por el número de molinos que conforman el parque, se ha estimado que es de 294.000 €, desglosado a continuación:

| Tipo de coste                                 | Cantidad (€)          |
|-----------------------------------------------|-----------------------|
| Coste por molino                              |                       |
| Evaluación de conformidad y Gap Analysis      | 2.800                 |
| Revisión de estándares actuales               | 6.100                 |
| Refuerzo de la gestión de incidentes          | 3.000                 |
| Mejora de la resiliencia operativa            | 3.700                 |
| Capacitación y concienciación                 | 2.500                 |
| Establecimiento de mecanismos de colaboración | 1.500                 |
| Total, por molino                             | 19.600                |
| Total 15 molinos                              | 19.600 * 15 = 294.000 |

Tabla 2: Coste desglosado adaptación sector eólico a directiva NIS2. Fuente: elaboración propia.

## Conclusión

La conclusión de este proyecto subraya la importancia crítica de la Directiva NIS2 para mejorar la ciberseguridad en los sectores eólico y ferroviario, sectores que son esenciales para la infraestructura crítica de cualquier país. A lo largo del proyecto, se ha demostrado que, aunque la implementación de esta directiva implica costos iniciales significativos, los beneficios a largo plazo superan con creces estas inversiones.

En primer lugar, la Directiva NIS2 refuerza la seguridad y la resiliencia operativa de las infraestructuras críticas. En un entorno cada vez más digitalizado, donde las amenazas cibernéticas son más frecuentes y sofisticadas, la capacidad de un parque eólico o de una red ferroviaria para resistir y recuperarse rápidamente de un ciberataque es esencial. La implementación de medidas avanzadas de ciberseguridad, como sistemas de detección y respuesta a incidentes, protocolos de recuperación ante desastres y la formación continua del personal, son fundamentales para asegurar que estas infraestructuras puedan mantener su operatividad incluso frente a las amenazas más complejas.

En segundo lugar, cumplir con la Directiva NIS2 es crucial no solo para evitar sanciones, sino también para fortalecer la posición de la empresa en el mercado. La confianza de los inversores, clientes y reguladores depende en gran medida de la capacidad de la empresa para proteger sus sistemas y datos frente a ciberataques. En este sentido, la implementación de la directiva no solo protege a la empresa contra posibles sanciones, sino que también mejora su reputación y competitividad en el mercado.

Además, la Directiva NIS2 fomenta la colaboración y la compartición de información entre las empresas y otros actores del sector. Participar en redes de cooperación y compartir

inteligencia cibernética no solo mejora la capacidad de respuesta ante amenazas emergentes, sino que también permite a las empresas adoptar mejores prácticas y tecnologías. Este enfoque colaborativo es especialmente importante en sectores como el eólico y el ferroviario, donde las operaciones están interconectadas y un ciberataque puede tener un efecto dominó en toda la red.

Finalmente, la mejora continua y la actualización de tecnologías son aspectos cruciales para mantenerse al día con el panorama cambiante de la ciberseguridad. La adopción de nuevas tecnologías y la actualización constante de políticas y procedimientos aseguran que las infraestructuras críticas se mantengan protegidas contra las amenazas emergentes. Este enfoque proactivo es fundamental para asegurar que las empresas no solo cumplan con la Directiva NIS2, sino que también estén preparadas para enfrentar las amenazas del futuro.

En resumen, la implementación de la Directiva NIS2 es una inversión estratégica para cualquier empresa del sector eólico o ferroviario. Aunque requiere un desembolso inicial considerable, los beneficios en términos de seguridad, resiliencia operativa, cumplimiento normativo y mejora continua justifican plenamente estos costos. La Directiva NIS2 no solo fortalece la ciberseguridad de las infraestructuras críticas, sino que también contribuye a la estabilidad y sostenibilidad de estos sectores en un entorno cada vez más digitalizado y amenazado por ciberataques.

# IMPACT OF THE NEW EUROPEAN CYBERSECURITY DIRECTIVE NIS2 ON SPANISH INDUSTRIAL SECTORS. APPLICATION CASES: RAILWAY SECTOR AND WIND SECTOR.

## **Introduction**

This work focuses on the analysis and evaluation of the impact of the new NIS2 Directive of the European Union on critical industrial sectors in Spain, specifically in the railway and wind sector. The NIS2 Directive is an evolution of the NIS1 Directive, with an expanded scope and stricter cybersecurity requirements to secure critical infrastructure. This project was born from the prevailing need to strengthen cyber defenses in an increasingly digitized environment and vulnerable to cyberattacks, whose frequency and sophistication have grown exponentially in recent years.

The main motivation for this work lies in the growing threat that cyberattacks pose to critical infrastructures, such as energy and transport systems. These infrastructures are vital for sustainability and economic development, and their disruption can have disastrous consequences both economically and for national security and social well-being. With the implementation of the NIS2 Directive, the European Union seeks to ensure a common level of security in information systems and networks, imposing obligations on the entities responsible for these infrastructures to adopt robust cybersecurity measures and reporting any significant incidents to the competent authorities.

The work also addresses the challenges involved in the implementation of this regulation, from the adaptation of legacy infrastructures that were not designed with cybersecurity in mind, to the need to train personnel in new security practices. Increasing digitalization in sectors such as wind and rail has increased the attack surface, exposing these systems to risks that could compromise their operation and safety. Therefore, the project focuses on proposing practical and adapted solutions that not only ensure compliance with the NIS2 Directive, but also strengthen the resilience of these infrastructures against cyber threats.

In terms of industrial cybersecurity, the importance of integrating advanced technologies, such as artificial intelligence and automation, is underlined, which, although they have improved efficiency and productivity, have also increased exposure to cyberattacks. In this context, the project establishes a clear framework for the implementation of the NIS2 Directive in the wind and rail sectors, assessing their specific vulnerabilities and developing mitigation strategies. Likewise, the costs and benefits associated with the proposed

cybersecurity measures are analyzed, promoting collaboration between companies and regulatory authorities to facilitate compliance with the regulations.

The contribution of this work is materialized in the creation of a detailed guide for the implementation of NIS2 in these critical sectors, based on real case studies and best practices. The strategies developed are expected to serve as a model for other industries, strengthening the ability of critical infrastructures to withstand and recover from cyberattacks, thus ensuring the continuity of essential services.

### **Railway sector**

The railway sector, like other critical sectors, faces significant challenges in terms of cybersecurity, especially in a context of increasing digitalization and connectivity. As rail infrastructure becomes more reliant on digital systems for train operation, signal control, traffic management and passenger services, the potential attack surface and the impact of potential cybersecurity incidents increases. This situation is compounded by the inherent complexity of rail systems, which integrate multiple interconnected subsystems, from brake and speed controls to passenger information systems and video surveillance services, shown below:

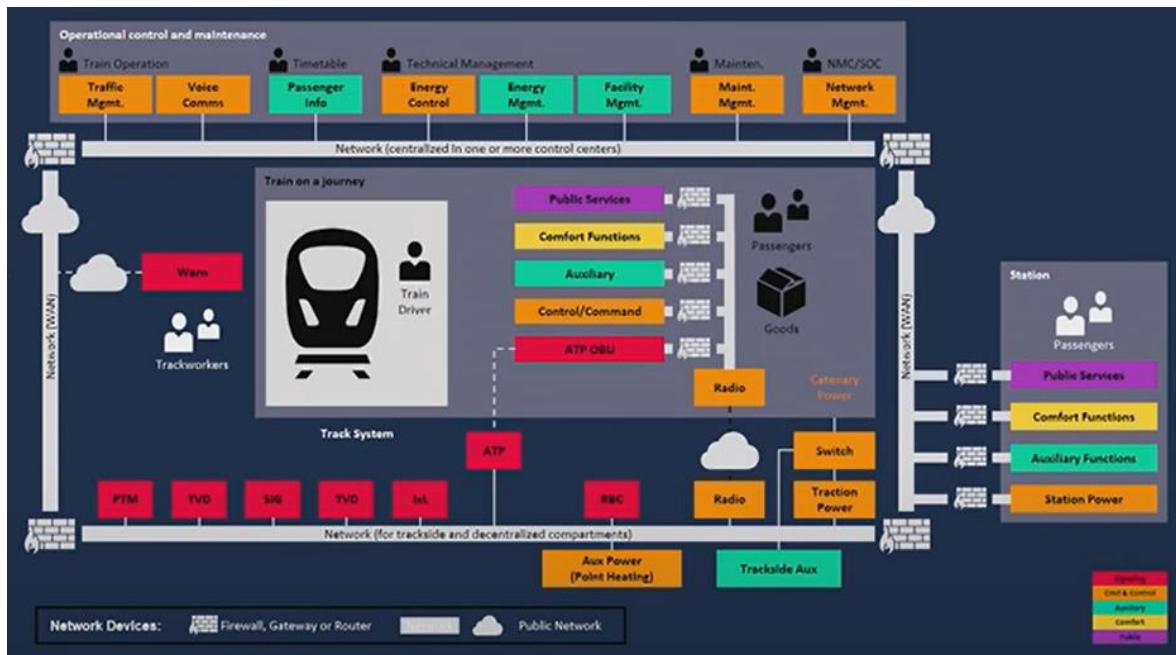


Figure 3: Diagram of the system of a train, in which each of the boxes represents a subsystem within an ideal model. The red part shows the most critical systems, that is, the train's signaling systems, which is what is responsible for preventing collisions between them. The orange part is the control systems (brakes, speed, etc.). On the other hand, we have auxiliary systems, comfort systems, and service that can be provided to passengers. Source: Video by Omar Benjumea, Siemens Mobility.

Historically, the sector has witnessed incidents that have had serious consequences, not only in terms of service disruptions, but also in terms of physical safety for passengers, as evidenced by the tram incident in Poland in 2008. These events underscore the critical need to implement robust cybersecurity measures that comply with current regulations, such as the NIS2 Directive.

To adapt to this directive, the rail sector must carry out a number of strategic actions. First, it is essential to conduct a thorough cyber risk assessment, identifying specific vulnerabilities in train control systems and other critical infrastructure, such as control centers and communication systems. This process involves not only identifying potential threats, but also implementing appropriate mitigation measures, which could include anything from upgrading signaling systems to integrating advanced detection and response technologies.

A prominent example in this context is Deutsche Bahn, Germany's main railway company, which has carried out comprehensive reviews of its systems to identify and address vulnerabilities. This has included implementing multi-factor authentication measures to

protect access to critical systems and developing a cybersecurity incident response plan. In addition, Deutsche Bahn has been actively involved in cyber intelligence sharing and cooperation networks with other European rail operators, which has significantly strengthened its cybersecurity posture.

Adaptation to the NIS2 Directive also requires the revision of cybersecurity standards currently implemented in the rail sector. Standards such as ISO/IEC 27001, IEC 62443, TS 50701, and NIST SP 800-53, although widely used, need to be adapted to cover all critical areas of the railway system. For example, while IEC 62443 is already applied in industrial control systems, not all railway subsystems have fully implemented it, requiring further expansion of its scope.

Another crucial aspect is the development of robust internal capabilities, which involves continuous training of personnel in cybersecurity and conducting regular drills to improve incident response. Training should not only include train operators, but also IT staff and other employees who may be involved in incident management.

Finally, it is essential to establish mechanisms for collaboration and sharing of information with other actors in the sector. Participating in cooperation networks, signing collaboration agreements and participating in joint cybersecurity exercises are key strategies to strengthen the resilience of the railway sector against cyber threats. These efforts, as demonstrated at Deutsche Bahn, not only ensure compliance with the NIS2 Directive, but also improve safety and operational efficiency in an increasingly digitalized environment.

As for the cost estimate for the implementation of the NIS2 Directive in the rail sector, a total cost of approximately €209,000 has been calculated for a company that manufactures trains and markets them. This cost includes:

| <b>Cost Type</b>                          | <b>Quantity (€)</b> |
|-------------------------------------------|---------------------|
| Gap Analysis and Conformity Assessment    | 25.000              |
| Revision of current standards             | 72.000              |
| Revision of current standards             | 20.000              |
| Improving operational resilience          | 45.000              |
| Training and awareness                    | 32.000              |
| Establishment of collaboration mechanisms | 15.000              |
| <b>Total</b>                              | <b>209.000</b>      |

*Table 3: Breakdown cost of adapting the railway sector to the NIS2 directive. Source: own elaboration.*



## Wind sector

The wind sector, key in the transition to renewable energy sources, is facing increasing challenges in terms of cybersecurity due to the increasing digitalization and connectivity of its operations. The integration of advanced technologies in the management and operation of wind farms has significantly improved efficiency and allowed for more precise control of turbines. However, this same digitalization has increased exposure to cyber threats, making the protection of critical infrastructure more urgent than ever. This urgency is fueled by the complexity and interconnectedness of these subsystems that make up a wind farm, shown below in this diagram:



*Illustration 4: Diagram of the subsystems of a wind farm, which work together to generate and distribute energy. Each of these subsystems plays a crucial role in the operation of the park. Source: Chat GPT.*

The NIS2 Directive, designed to strengthen cybersecurity across the European Union, imposes new obligations on operators of critical infrastructure, including wind farms. Unlike its predecessor, NIS1, this new directive not only expands the scope of the sectors covered, but also sets stricter requirements for risk management and incident response. Wind farm operators must now ensure that their control systems, such as SCADA (Supervisory Control and Data Acquisition) systems, are adequately protected against cyberattacks, as these systems are critical for the monitoring and operation of turbines.

One of the first steps in adapting to the NIS2 Directive is to carry out a thorough assessment of the existing infrastructure in wind farms. This assessment should identify all

vulnerabilities and areas for improvement in current systems, paying particular attention to access points that could be exploited by attackers. SCADA systems, in particular, require detailed analysis, as their interconnected nature makes them particularly susceptible to cyberattacks. Implementing robust security measures, such as network segmentation, multi-factor authentication, and data encryption, is essential to mitigate these risks.

The protection of SCADA systems not only involves the implementation of security technologies, but also the integration of practices and procedures that ensure a quick and effective response in the event of an incident. This includes the creation of contingency plans that allow the wind farm operator to return to normal operation as quickly as possible, minimizing interruptions in the energy supply. Operational resilience thus becomes a key aspect for compliance with the NIS2 Directive, ensuring that even in the event of a cyberattack, the impact on the operation of the park is limited.

In addition to the evaluation and implementation of security measures, the NIS2 Directive requires an adaptation and expansion of the cybersecurity standards currently in use in the wind sector. Standards such as ISO/IEC 27001, which covers information security management, and IEC 62443, which focuses on the protection of industrial control systems, are essential for creating a robust security framework. However, these standards need to be adapted to address the particularities of wind farms, which operate in a dynamic and often geographically distributed environment.

The implementation of these standards must be accompanied by continuous review and regular audits to ensure their effectiveness over time. In this sense, the NIS2 Directive promotes a proactive security culture, where risk assessment and the implementation of security measures are not one-off actions, but continuous processes that must be adapted as threats evolve.

A critical aspect in adapting to NIS2 is staff training. Since cybersecurity in the wind sector involves both technicians in the field and IT personnel, it is essential that all employees are trained to recognize and respond to potential threats. This includes not only technical training on how to operate security systems, but also awareness of broader security practices, such as password management and identifying phishing attempts.

In addition to training, participation in cybersecurity networks and joint exercises with other companies in the sector is essential to strengthen resilience to cyberattacks. These collaborations allow for the sharing of threat information and best practices, creating a more

robust community against cyber threats. Leading companies in the sector, such as Enercon, have shown that cooperation between different actors can be a decisive factor in improving cybersecurity.

Adaptation to the NIS2 Directive also involves a review of internal security policies. This includes updating access policies and implementing tighter controls over who can access critical systems. In many cases, this requires a complete restructuring of identity and access management systems, ensuring that only authorized personnel can make changes to SCADA and other critical systems.

Finally, it is important to highlight that the implementation of the NIS2 Directive in the wind sector is not only a matter of regulatory compliance, but an opportunity to improve resilience and operational efficiency. By taking a proactive stance on cybersecurity, wind farm operators not only protect their assets, but also ensure the continuity of energy supply, which is vital for the economy and society at large.

As for the cost estimate for the implementation of the NIS2 Directive in the wind sector, taking as an example a 3 MW wind farm, with 15 wind turbines, the estimated price, calculated for each mill separately, and multiplied by the number of windmills that make up the farm, has been estimated to be € 294,000, broken down below:

| <b>Cost Type</b>                          | <b>Quantity (€)</b>   |
|-------------------------------------------|-----------------------|
| Cost per mill                             |                       |
| Gap Analysis and Conformity Assessment    | 2.800                 |
| Revision of current standards             | 6.100                 |
| Strengthening incident management         | 3.000                 |
| Improving operational resilience          | 3.700                 |
| Training and awareness                    | 2.500                 |
| Establishment of collaboration mechanisms | 1.500                 |
| Total, per mill                           | 19.600                |
| Total 15 mills                            | 19.600 * 15 = 294.000 |

*Table 4: Breakdown cost of adapting the wind sector to the NIS 2 directive. Source: own elaboration.*

## **Conclusion**

The conclusion of this project underlines the critical importance of the NIS2 Directive to improve cybersecurity in the wind and rail sectors, sectors that are essential to any country's critical infrastructure. Throughout the project, it has been shown that although the implementation of this directive involves significant upfront costs, the long-term benefits far outweigh these investments.

First, the NIS2 Directive strengthens the security and operational resilience of critical infrastructures. In an increasingly digitized environment, where cyber threats are more frequent and sophisticated, the ability of a wind farm or railway network to resist and recover quickly from a cyberattack is essential. The implementation of advanced cybersecurity measures, such as incident detection and response systems, disaster recovery protocols, and continuous training of personnel, are essential to ensure that these infrastructures can maintain their operability even in the face of the most complex threats.

Second, complying with the NIS2 Directive is crucial not only to avoid penalties, but also to strengthen the company's position in the market. The confidence of investors, customers, and regulators depends largely on the company's ability to protect its systems and data from cyberattacks. In this sense, the implementation of the directive not only protects the company against possible sanctions, but also improves its reputation and competitiveness in the market.

In addition, the NIS2 Directive encourages collaboration and information sharing between companies and other actors in the sector. Participating in cooperation networks and sharing cyber intelligence not only improves the ability to respond to emerging threats, but also allows companies to adopt best practices and technologies. This collaborative approach is especially important in industries such as wind and rail, where operations are interconnected and a cyberattack can have a ripple effect across the network.

Finally, continuous improvement and updating technologies are crucial aspects of keeping up with the changing cybersecurity landscape. The adoption of new technologies and the constant updating of policies and procedures ensure that critical infrastructures remain protected against emerging threats. This proactive approach is critical to ensure that companies are not only compliant with the NIS2 Directive, but also prepared to face the threats of the future.

In summary, the implementation of the NIS2 Directive is a strategic investment for any company in the wind or rail sector. Although it requires a considerable upfront outlay, the benefits in terms of security, operational resilience, regulatory compliance, and continuous improvement fully justify these costs. The NIS2 Directive not only strengthens the cybersecurity of critical infrastructures, but also contributes to the stability and sustainability of these sectors in an increasingly digitized environment threatened by cyberattacks.

# Índice

|                                                                                           |           |
|-------------------------------------------------------------------------------------------|-----------|
| <b>Capítulo 1: Introducción</b> .....                                                     | <b>23</b> |
| 1.1 Motivación del proyecto .....                                                         | 26        |
| 1.2 Directiva NIS1 .....                                                                  | 28        |
| 1.3 Directiva NIS2 .....                                                                  | 31        |
| 1.4 Objetivos .....                                                                       | 34        |
| 1.5 Estado de la cuestión.....                                                            | 44        |
| <b>Capítulo 2: Sector ferroviario</b> .....                                               | <b>51</b> |
| 2.1 Retos de ciberseguridad en este sector.....                                           | 51        |
| 2.2 Casos reales: .....                                                                   | 53        |
| 2.3 Estándares de ciberseguridad en el sector ferroviario.....                            | 55        |
| 2.4 Adaptación de los Estándares Actuales del Sector Ferroviario a la Directiva NIS2..... | 57        |
| 2.5 Coste estimado sector ferroviario .....                                               | 65        |
| <b>Capítulo 3: Sector eólico</b> .....                                                    | <b>75</b> |
| 3.1 Retos de ciberseguridad en este sector.....                                           | 75        |
| 3.2 Casos reales: .....                                                                   | 79        |
| 3.3 Estándares de Ciberseguridad en el sector eólico .....                                | 80        |
| 3.4 Adaptación de los Estándares Actuales del Sector Eólico a la Directiva NIS2 .....     | 83        |
| 3.5 Coste estimado sector eólico.....                                                     | 87        |
| <b>Capítulo 4: Conclusión</b> .....                                                       | <b>95</b> |
| 4.1 Viabilidad y Beneficios.....                                                          | 96        |
| 4.2 Comparativa de Costos y Beneficios .....                                              | 97        |
| 4.3 Conclusión Final .....                                                                | 97        |
| <b>Capítulo 5: Referencias</b> .....                                                      | <b>99</b> |

## CAPÍTULO 1: INTRODUCCIÓN

Este proyecto se basa en el estudio de la directiva NIS2 en ciberseguridad para el sector industrial y su aplicación a un parque eólico y al sector ferroviario.

La directiva NIS2 (Directiva sobre Redes y sistemas de Información) es una normativa establecida por la Unión Europea centrada en mejorar la seguridad de las redes y los sistemas de información, aportando normas y expectativas de cumplimiento que toda entidad aplicable debe cumplir.

Es la nueva versión de la directiva NIS1, y tiene como objetivo proporcionar un mayor nivel común de ciberseguridad en la UE.

La directiva NIS1 fue la primera medida legislativa en la UE, y se creó con el objetivo de mejorar la cooperación entre los estados miembros y crear un nivel de armonización en el ámbito de la ciberseguridad.

Con esta investigación, se comprenderá la importancia de proteger la infraestructura clave de posibles ataques cibernéticos y amenazas, y se buscará, por ello, proporcionar un mayor nivel de seguridad en sectores críticos.

La ciberseguridad en el ámbito industrial es cada vez más relevante, dada la mayor digitalización en el campo de la infraestructura. Los parques eólicos, como parte de la industria energética, están expuestos a tales riesgos y, por lo tanto, deben estar preparados para abordar y mitigar los ciber desafíos de seguridad. Por consiguiente, este proyecto no solo se vincula con los esfuerzos por mejorar la resiliencia a los ciberataques, sino que también es importante para definir las posibles adaptaciones de las políticas de la UE al contexto específico. Estos incluyen las fuentes de energía renovable y las disposiciones sobre el transporte ferroviario.

Debe llevarse a cabo la preparación para permitir que la directiva sea nacional o aplicable desde el 17 de octubre de 2024. Este estudio pretende centrarse en los sectores afectados,

sobre todo mediante la implementación en la vida diaria de medidas de ciberseguridad, como la red de un parque eólico y, según la disponibilidad de alcance, la red ferroviaria, para demostrar cómo estas regulaciones y recomendaciones de la directiva NIS2 pueden aplicarse y respetarse en estos ámbitos críticos.

### **Importancia de la ciberseguridad industrial**

La ciberseguridad en el ámbito industrial ha cobrado una importancia crítica en los últimos años debido a la creciente digitalización y la interconexión de los sistemas industriales. La integración de tecnologías avanzadas, como el Internet de las Cosas (IoT), la inteligencia artificial (IA) y la automatización, ha mejorado significativamente la eficiencia y la productividad. Sin embargo, también ha aumentado la superficie de ataque, exponiendo a las infraestructuras críticas a riesgos cibernéticos cada vez más sofisticados. Los ataques cibernéticos pueden tener consecuencias devastadoras, no solo en términos de pérdidas económicas, sino también en la seguridad nacional y el bienestar de la sociedad.

### **Objetivos y alcance del proyecto**

El principal objetivo de este proyecto es proporcionar un marco claro y detallado para la implementación de la directiva NIS2 en los sectores eólico y ferroviario. Esto incluye la identificación de las vulnerabilidades específicas de estos sectores, el desarrollo de estrategias de mitigación y la evaluación de los costes y beneficios de las medidas de ciberseguridad propuestas, que se desarrollarán más adelante. Además, el proyecto busca promover la colaboración y el intercambio de conocimientos entre las empresas y las autoridades regulatorias para facilitar el cumplimiento de la normativa.

### **Contribución del proyecto**

Al proporcionar una guía práctica y basada en la investigación para la implementación de la NIS2, este proyecto contribuye a la seguridad y sostenibilidad de los sectores eólico y ferroviario. Las recomendaciones y estrategias desarrolladas en este estudio pueden servir como modelo para otras industrias que también enfrentan desafíos similares en la implementación de medidas de ciberseguridad. En última instancia, este proyecto no solo



busca cumplir con los requisitos regulatorios, sino también fortalecer la capacidad de las infraestructuras críticas para resistir y recuperarse de los ciberataques, asegurando así la continuidad de los servicios esenciales y la protección de la sociedad.

### Sectores afectados

- Con **carácter general**, la directiva aplica a entidades públicas o privadas, consideradas medianas o grandes empresas, que operen en la Unión, es decir, en lo que respecta a entidades privadas, empresas de más de 50 empleados o con un volumen de negocio mayor de 10 millones de euros, incluidas aquellas que puedan tener inversiones públicas.

Estas empresas son entidades bien consideradas de alta criticidad dentro de los sectores de energía, transporte, banca, infraestructuras de mercados financieros, sector sanitario, agua potable, espacio, infraestructura digital, aguas residuales, gestión de servicios TIC (B2B) o entidades de las AAPP (Administración Pública); o bien consideradas de otros sectores críticos, como las plataformas de redes sociales, entidades dedicadas a servicios postales y de mensajería; gestión de residuos; organismos de investigación, fabricación, producción y distribución de sustancias y mezclas químicas; producción, transformación y distribución de alimentos; y fabricación de material eléctrico, maquinaria y equipo ncop., vehículos de motor, remolques y semirremolques, y otro material de transporte.

- Con **carácter particular**, aplica a entidades pequeñas y microempresas que presentan un papel clave para la sociedad, la economía o para determinados sectores, como las entidades críticas (según la ley PIC), y los OSE (Operadores de Servicios Especiales) de la NIS1.

La ley PIC (Protección de Infraestructuras Críticas) es una ley española que define las infraestructuras críticas y establece medidas para su protección.

Las infraestructuras críticas se refieren a instalaciones físicas o virtuales cuyo correcto funcionamiento es vital para los intereses nacionales. Si estas infraestructuras sufren alteraciones o daños, tendrían un impacto significativo en los servicios esenciales.

## **1.1 Motivación del proyecto**

En primer lugar, la cuestión que plantea este Trabajo de Fin de Grado se basa en la **motivación por el aumento de ciberataques en infraestructuras críticas y la urgencia de reforzar los sistemas de información frente a amenazas en rápida evolución**. Es decir, el sector industrial, como los parques eólicos y de infraestructuras energéticas ferroviarias y de transporte, es fundamental para la sostenibilidad y el desarrollo económico. Dado que estos sectores dependen de tecnologías de la información y comunicación (TIC), son particularmente susceptibles a su interrupción, lo que resultaría en consecuencias extremas, desde apagones hasta riesgos de seguridad para la población.

Este proyecto está motivado por la necesidad intrínseca de implementar y hacer funcionar la Directiva NIS2 en estos sectores, lo que asegurará una mayor protección de seguridad. Se trata de más que seguridad tradicional; es imperativo adoptar una estrategia integral que abarque medidas preventivas, detección, respuesta y recuperación de incidentes de ciberseguridad.

### **Relevancia del contexto global y regional**

El contexto global actual, como ya se ha comentado, muestra un incremento notable en la frecuencia y sofisticación de los ciberataques, que no solo afectan a empresas individuales, sino que también ponen en riesgo la seguridad nacional y la estabilidad económica. Las infraestructuras críticas, como los parques eólicos y las redes ferroviarias, son objetivos atractivos para los atacantes debido a su importancia estratégica. Un ciberataque exitoso en estas infraestructuras podría tener efectos devastadores, no solo a nivel económico, sino también en términos de confianza pública y seguridad nacional. En el ámbito regional, la UE ha reconocido esta amenaza y ha respondido con la directiva NIS2, que busca fortalecer las medidas de ciberseguridad entre sus estados miembros.

### **Impacto económico y social**

La implementación efectiva de la directiva NIS2 tiene un impacto significativo en la economía y la sociedad. Las interrupciones en el suministro de energía o en el transporte

pueden causar grandes pérdidas económicas y afectar la vida diaria de millones de personas. Por ejemplo, un apagón en un parque eólico, como ya se ha comentado antes, puede no solo interrumpir el suministro de energía renovable, sino también afectar a empresas y hogares que dependen de esta fuente de energía. De manera similar, un ciberataque a la red ferroviaria podría causar interrupciones en el transporte de mercancías y pasajeros, afectando la logística y la economía en general. Por lo tanto, la mejora de la ciberseguridad en estos sectores es crucial para garantizar la continuidad de los servicios y proteger el bienestar de la sociedad.

### **Desafíos tecnológicos y operativos**

La transición hacia una infraestructura más segura no está exenta de desafíos. La integración de nuevas tecnologías de ciberseguridad en sistemas industriales existentes puede ser compleja y costosa. Los sistemas heredados, que son comunes en el sector industrial, a menudo no fueron diseñados con la ciberseguridad en mente, lo que los hace vulnerables a los ataques. Además, la formación y capacitación del personal en prácticas de ciberseguridad avanzadas es esencial para asegurar una implementación efectiva de la directiva NIS2. Este proyecto busca abordar estos desafíos proporcionando soluciones prácticas y adaptadas a las necesidades específicas de los sectores eólico y ferroviario.

### **Innovación y desarrollo sostenible**

La mejora de la ciberseguridad también promueve la innovación y el desarrollo sostenible. Al proteger las infraestructuras críticas, se fomenta la confianza en las tecnologías avanzadas y se asegura que los beneficios de la digitalización puedan ser plenamente realizados. Esto es particularmente relevante en el contexto de la transición hacia fuentes de energía renovable, como los parques eólicos, que juegan un papel crucial en la lucha contra el cambio climático. Al asegurar que estas infraestructuras estén protegidas contra ciberataques, se contribuye a un futuro más sostenible y flexible.

## **Colaboración y cooperación internacional**

Finalmente, la implementación de la directiva NIS2 requiere una colaboración estrecha entre las empresas, las autoridades reguladoras y los estados miembros de la UE. La ciberseguridad es un desafío global que no puede ser abordado de manera aislada. Este proyecto destaca la importancia de la cooperación internacional para compartir información, mejores prácticas y recursos. La creación de redes y consorcios de ciberseguridad puede facilitar una respuesta más coordinada y eficaz a las amenazas cibernéticas, mejorando la seguridad global de las infraestructuras críticas.

### **1.2 Directiva NIS1**

La Directiva sobre la Seguridad de las Redes y Sistemas de Información, conocida como NIS1, fue adoptada por la Unión Europea en julio de 2016 y representa uno de los primeros esfuerzos legislativos importantes a nivel europeo para mejorar la ciberseguridad en toda la Unión. Su implementación tenía como objetivo principal establecer un nivel común de seguridad en las redes y sistemas de información en todos los Estados miembros de la UE. La Directiva NIS1 surgió como respuesta a la creciente amenaza de ciberataques y a la necesidad de garantizar la resiliencia y seguridad de las infraestructuras críticas y servicios esenciales que sostienen la economía y el bienestar social de Europa. En este contexto, la NIS1 ha jugado un papel crucial en la armonización de las políticas de ciberseguridad entre los diferentes países europeos, estableciendo una base sólida para la cooperación y respuesta conjunta a los incidentes de ciberseguridad.

### **Objetivos Principales de la NIS1**

#### **1. Mejora de la Ciberseguridad Nacional:**

- Desarrollo de Estrategias Nacionales: Cada Estado miembro debía desarrollar y mantener una estrategia nacional de ciberseguridad. Estas estrategias debían abordar los riesgos de ciberseguridad y delinear las medidas para mitigarlos.

- Autoridades Competentes: Los Estados miembros debían designar una o más autoridades nacionales competentes para supervisar la implementación de la Directiva NIS. Estas

autoridades serían responsables de coordinar la respuesta a incidentes y de colaborar con otras autoridades nacionales e internacionales.

## 2. Cooperación a Nivel de la UE:

- Grupo de Cooperación: Se estableció un Grupo de Cooperación para facilitar la cooperación y el intercambio de información entre los Estados miembros. Este grupo está compuesto por representantes de cada Estado miembro, la Comisión Europea y la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

- Red de CSIRTs: La Directiva NIS1 también creó una red de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRTs) para promover la cooperación en la gestión de incidentes a nivel europeo. Los CSIRTs de cada Estado miembro deben trabajar juntos para prevenir, detectar y responder a los incidentes de ciberseguridad.

## 3. Seguridad de los Servicios Esenciales:

- Operadores de Servicios Esenciales (OES): La Directiva NIS1 identifica ciertos sectores como críticos para la economía y la sociedad, tales como energía, transporte, banca, infraestructuras del mercado financiero, salud, agua potable y digital. Las organizaciones en estos sectores, conocidas como Operadores de Servicios Esenciales (OES), están sujetas a requisitos de seguridad más estrictos.

- Proveedores de Servicios Digitales (DSP): La Directiva también se aplica a ciertos Proveedores de Servicios Digitales, incluyendo mercados en línea, motores de búsqueda y servicios de computación en la nube.

## **Requisitos de Seguridad y Notificación**

### 1. Medidas de Seguridad:

- Evaluación de Riesgos: Los OES y DSP deben adoptar medidas de seguridad adecuadas y proporcionales a los riesgos existentes. Estas medidas deben tener en cuenta tanto la prevención como la respuesta a incidentes de ciberseguridad.

- Gestión de Incidentes: Las organizaciones deben implementar procedimientos para gestionar los incidentes de ciberseguridad de manera efectiva, incluyendo la detección, el análisis, la contención y la recuperación.

## 2. Notificación de Incidentes:

- Obligaciones de Notificación: Los OES y DSP deben notificar a las autoridades competentes o a los CSIRTs sobre los incidentes de ciberseguridad que tengan un impacto significativo en la continuidad de los servicios que prestan. La notificación debe incluir detalles sobre la naturaleza del incidente, su impacto y las medidas de mitigación adoptadas.

## **Implementación y Cumplimiento**

### 1. Supervisión y Sanciones:

- Supervisión: Las autoridades competentes tienen la responsabilidad de supervisar el cumplimiento de la Directiva NIS1 por parte de los OES y DSP. Esto incluye la realización de auditorías y la evaluación de las medidas de seguridad implementadas.

- Sanciones: Los Estados miembros deben establecer un régimen de sanciones efectivo, proporcionado y disuasorio para las infracciones de la Directiva NIS1.

## **Impacto y Evaluación**

### 1. Evaluación de Impacto:

- Revisión y Mejoras: La Comisión Europea debe realizar evaluaciones periódicas sobre la implementación de la Directiva NIS1 y su impacto en la ciberseguridad en la UE. Estas evaluaciones pueden llevar a revisiones y actualizaciones de la legislación para abordar nuevos desafíos y amenazas.

### **1.3 Directiva NIS2**

La Directiva NIS2 fue introducida por la Unión Europea como respuesta a la evolución constante del panorama de amenazas cibernéticas. Esta normativa busca establecer un marco de ciberseguridad coherente y robusto en toda la UE, reforzando y ampliando el alcance de su predecesora, la NIS1. La NIS2 no solo mantiene los objetivos de proteger las redes y sistemas de información esenciales para la sociedad y la economía, sino que también introduce requisitos más estrictos y una cobertura más amplia.

#### **Relevancia de la Directiva NIS2**

La Directiva NIS2 se diseñó para abordar las amenazas emergentes y establecer un marco de ciberseguridad coherente en toda la Unión Europea. A diferencia de su predecesora, la NIS1, la NIS2 amplía su alcance e introduce requisitos más estrictos para la protección de las redes y sistemas de información. La directiva NIS2 obliga a las entidades esenciales y los proveedores de servicios digitales a adoptar medidas de seguridad adecuadas y a reportar incidentes de seguridad significativos a las autoridades competentes. Esta normativa tiene como objetivo mejorar la resiliencia cibernética de las infraestructuras críticas y fomentar la cooperación entre los estados miembros de la UE para enfrentar las amenazas cibernéticas de manera más eficaz.

#### **Principales Objetivos**

Los objetivos principales de la Directiva NIS2 incluyen:

1. Ampliación del Alcance: La NIS2 cubre una gama más amplia de sectores y servicios críticos, incluidos no solo los operadores de servicios esenciales, sino también ciertos proveedores de servicios digitales que no estaban completamente cubiertos bajo la NIS1.
2. Requisitos de Seguridad Más Estrictos: La NIS2 impone requisitos de seguridad más rigurosos, obligando a las organizaciones a implementar medidas técnicas y organizativas adecuadas para gestionar los riesgos cibernéticos y proteger sus sistemas de información.

3. Notificación de Incidentes: Las entidades deben notificar los incidentes de seguridad significativos a las autoridades competentes en un plazo específico. Esto incluye la obligación de proporcionar información detallada sobre el incidente y las medidas correctivas adoptadas.

4. Cooperación y Coordinación: La directiva promueve una mayor cooperación y coordinación entre los estados miembros de la UE, facilitando el intercambio de información y mejores prácticas a través de redes y mecanismos establecidos.

### **Desafíos en la Implementación de la NIS2**

La implementación de la Directiva NIS2 presenta varios desafíos, especialmente en sectores como el eólico y ferroviario:

1. Falta de Estudios Detallados y Guías Específicas: La ausencia de estudios y guías específicas para ciertos sectores dificulta la planificación y ejecución de medidas de ciberseguridad adecuadas.

2. Costos y Complejidad: Adaptar las infraestructuras existentes para cumplir con los requisitos de la NIS2 puede ser costoso y complejo, especialmente para las pequeñas y medianas empresas.

3. Capacitación del Personal: Es crucial asegurar que el personal esté adecuadamente capacitado en ciberseguridad industrial para gestionar y responder a los incidentes de manera efectiva.

4. Integración de Nuevas Tecnologías: La integración de nuevas tecnologías de ciberseguridad con sistemas existentes puede presentar dificultades técnicas y organizativas.

### **Requisitos de la Directiva NIS2**

Los requisitos de la Directiva NIS2 son más amplios y estrictos que los de la NIS1. Estos incluyen:



- Medidas Técnicas y Organizativas: Implementación de medidas adecuadas para gestionar los riesgos cibernéticos.
- Notificación de Incidentes: Obligación de notificar incidentes de seguridad significativos a las autoridades competentes en un plazo determinado.
- Auditorías y Evaluaciones: Realización de auditorías y evaluaciones periódicas para asegurar el cumplimiento continuo.
- Cooperación y Compartición de Información: Participación en redes de cooperación y compartición de inteligencia cibernética.

### **Consecuencias del Incumplimiento**

El incumplimiento de la Directiva NIS2 puede tener graves consecuencias para las empresas. Estas consecuencias incluyen:

- Sanciones Financieras: Las empresas que no cumplan con los requisitos de la NIS2 pueden enfrentarse a multas significativas impuestas por las autoridades competentes.
- Daño a la Reputación: No cumplir con la normativa puede afectar negativamente la reputación de la empresa, especialmente si un incidente de seguridad resulta en una violación de datos o interrupción de servicios.
- Responsabilidad Legal: Las empresas pueden ser responsables legalmente por cualquier daño causado a terceros debido a su incumplimiento de los requisitos de seguridad.
- Intervención Gubernamental: En casos extremos, las autoridades pueden intervenir en las operaciones de la empresa para garantizar la implementación de medidas de ciberseguridad adecuadas.

Implementar y cumplir con la Directiva NIS2 es esencial para que las empresas protejan sus infraestructuras críticas, mantengan la confianza de sus clientes y eviten las severas consecuencias del incumplimiento.

## **1.4 Objetivos**

El objetivo principal es:

- **Evaluar la Directiva NIS2 y su impacto en la ciberseguridad del sector industrial:** abordar la legislación actual que representa la directiva y plantear las expectativas y los requisitos específicos que plantea a las infraestructuras críticas.

El objetivo central de este proyecto es realizar una evaluación exhaustiva de esta normativa y su impacto en la ciberseguridad del sector industrial. Esta evaluación incluye varios aspectos clave que son fundamentales para entender y mejorar la seguridad de las infraestructuras críticas:

### **1. Comprensión de la Directiva NIS2**

Como ya se ha explicado en la primera parte del proyecto, es una actualización de la Directiva NIS1, diseñada para fortalecer la ciberseguridad en la Unión Europea. Esta directiva establece un marco común de medidas de seguridad que deben implementar las infraestructuras críticas para protegerse contra ciberamenazas. La comprensión completa de la directiva implica analizar su descripción antes desarrollada. Esto incluye el análisis de los motivos detrás de su implementación, como el aumento de ciberataques a nivel global y la necesidad de una respuesta coordinada a nivel europeo, que deben ser estudiados por parte de la empresa afectada.

### **2. Análisis del marco legal y regulatorio**

Evaluar la Directiva NIS2 requiere un análisis detallado del marco legal y regulatorio que la respalda. Esto implica estudiar cómo la directiva se integra con las leyes nacionales de los estados miembros de la UE y cómo se armoniza con otras regulaciones de ciberseguridad globales y regionales. Por ejemplo, en España, la Ley de Seguridad de las Redes y Sistemas de Información se actualiza para incorporar los nuevos requisitos de la NIS2, lo que obliga a las empresas de sectores críticos como la energía y el transporte a cumplir con estas actualizaciones para evitar sanciones.

Además, es crucial que la Directiva NIS2 se armonice con otras regulaciones de ciberseguridad tanto globales como regionales para asegurar un enfoque coherente y evitar conflictos normativos. Una empresa multinacional que opera tanto en la UE como en EE. UU., por ejemplo, debe asegurarse de que sus políticas de ciberseguridad cumplan con la NIS2 y con el NIST estadounidense, lo que podría implicar la implementación de un marco de ciberseguridad unificado que cumpla con ambos conjuntos de requisitos.

Las empresas deben revisar y adaptar sus políticas y procedimientos internos para cumplir con la nueva normativa, incluyendo la implementación de nuevas medidas de seguridad, protocolos de respuesta a incidentes y planes de contingencia. Por ejemplo, una empresa de telecomunicaciones debe desarrollar un nuevo protocolo de respuesta a incidentes que incluya la notificación a las autoridades competentes dentro de las 24 horas posteriores a la detección de un ciberataque significativo, tal como lo exige la NIS2.

Finalmente, es crucial entender los mecanismos de supervisión y cumplimiento que las autoridades regulatorias implementarán para asegurar la conformidad con la directiva, así como las posibles sanciones por incumplimiento. La Agencia de Ciberseguridad de la UE (ENISA), por ejemplo, realiza auditorías periódicas a empresas de infraestructura crítica para verificar el cumplimiento de la NIS2. Las empresas que no cumplan con los requisitos pueden enfrentarse a sanciones que incluyen multas significativas y la obligación de implementar medidas correctivas en un plazo determinado.

Estos ejemplos prácticos ilustran cómo las empresas deben abordar la implementación de la Directiva NIS2, asegurando el cumplimiento normativo y fortaleciendo su postura de ciberseguridad.

### **3. Identificación de expectativas y requisitos**

Evaluar la regulación establece claras expectativas y requisitos para las organizaciones que operan infraestructuras críticas. Es crucial identificar y entender estos requisitos para asegurar el cumplimiento y mejorar la capacidad de respuesta de las organizaciones. Además, es necesario evaluar el grado de preparación de las organizaciones para cumplir con estos requisitos e identificar las brechas que deben ser abordadas. Por ejemplo, una empresa de energía podría necesitar implementar sistemas avanzados de monitoreo para detectar y responder a incidentes en tiempo real, mientras que una empresa ferroviaria podría requerir la actualización de sus protocolos de seguridad para alinearse con las nuevas normativas.

### **4. Impacto en el sector industrial**

Evaluar el impacto de la Directiva NIS2 en el sector industrial implica analizar cómo las nuevas obligaciones afectarán las operaciones diarias, la gestión de la seguridad y los costes asociados. Es necesario considerar cómo la implementación de la directiva puede cambiar las prácticas de seguridad existentes, la necesidad de nuevas inversiones en tecnologías de ciberseguridad y la capacitación del personal. También se debe evaluar cómo estas medidas pueden mejorar la protección contra ciberataques y reducir el riesgo de interrupciones en los servicios críticos. Además, se debe considerar el impacto en la cadena de suministro y en las relaciones con los proveedores y socios comerciales, ya que la ciberseguridad es un esfuerzo colaborativo que requiere la cooperación de todas las partes involucradas. Por ejemplo, una empresa operadora de un parque eólico puede necesitar actualizar sus sistemas SCADA (Supervisory Control and Data Acquisition) para cumplir con la normativa y coordinarse con sus proveedores de turbinas para asegurar que toda la cadena de suministro esté protegida contra posibles ciberamenazas.

### **5. Estudio de casos y mejores prácticas**

Para una evaluación completa, es útil estudiar casos de éxito y mejores prácticas de organizaciones que ya han comenzado a implementar la Directiva NIS2. Estos estudios de caso proporcionan información valiosa sobre los desafíos, soluciones y

resultados obtenidos, ayudando a otras organizaciones a evitar errores comunes y adoptar enfoques efectivos. Por ejemplo, Eurostar en el sector ferroviario reevaluó su infraestructura de ciberseguridad, descubrió vulnerabilidades, actualizó sus sistemas, implantó una gestión de acceso estricta y creó un sólido plan de respuesta contra amenazas. Estos cambios aseguraron su conformidad con la Directiva NIS2 y fortalecieron su resiliencia operativa. En el sector eólico, Enercon intensificó sus sistemas de detección de brechas, reforzó su infraestructura informática y formó a su personal en prevención de ciberamenazas, cumpliendo con la normativa y mejorando su protección contra ciberataques. Estudiar estos casos guía a otras organizaciones en su camino hacia el cumplimiento de la Directiva NIS2.

## **6. Recomendaciones y estrategias de implementación**

Para asegurar que las organizaciones industriales cumplan con la Directiva NIS2, es esencial desarrollar recomendaciones y estrategias prácticas. Esto incluye la creación de guías paso a paso para la implementación de medidas de seguridad, como lo hizo Eurostar al actualizar sus sistemas y mejorar la gestión de acceso. También se deben identificar tecnologías clave que deben adoptarse, similar a cómo Enercon implementó tecnologías avanzadas de detección de brechas de datos.

## **7. Evaluación de la eficiencia y eficacia de las medidas de ciberseguridad**

Evaluar la eficiencia y eficacia de las medidas de ciberseguridad implementadas es crucial para medir su impacto. Esto incluye la utilización de métricas y KPIs (Key Performance Indicators) específicos para evaluar el desempeño de las estrategias de ciberseguridad. Por ejemplo, Eurostar podría utilizar KPIs como el tiempo de respuesta a incidentes y la tasa de éxito de recuperación para medir la efectividad de sus nuevas políticas de gestión de accesos. Enercon, por otro lado, podría analizar el número de intentos de ciberataques detectados y mitigados con sus nuevas tecnologías de detección de brechas. La recolección y análisis de datos relacionados con incidentes de seguridad, tiempos de respuesta y recuperación, y el cumplimiento de los requisitos normativos proporcionarán una visión clara del estado de la

ciberseguridad en la organización, permitiendo la identificación de áreas de mejora continua.

## **8. Implicaciones económicas y financieras**

Evaluar el impacto económico y financiero de la implementación de la Directiva NIS2 es otro aspecto crucial. Las organizaciones deben considerar no solo los costes directos de las nuevas medidas de seguridad, sino también los beneficios a largo plazo de evitar incidentes de seguridad que pueden resultar en pérdidas significativas. Por ejemplo, Eurostar podría enfrentar costes relacionados con la inversión en tecnologías avanzadas de gestión de accesos y la capacitación del personal, pero estos gastos se verían compensados por la reducción del riesgo de ciberataques y las posibles sanciones por incumplimiento. De manera similar, Enercon podría invertir en sistemas de detección de brechas y formación continua, lo que podría reducir significativamente los costes asociados a interrupciones en sus servicios críticos y proteger la reputación de la empresa frente a sus clientes y socios comerciales. Estos ahorros potenciales en términos de prevención de ataques y protección de la reputación de la empresa (Goodwill) son factores clave para justificar la inversión en ciberseguridad.

En conclusión, evaluar la Directiva NIS2 y su impacto en la ciberseguridad del sector industrial es un objetivo multifacético que abarca desde la comprensión detallada de la normativa hasta la implementación de estrategias prácticas para mejorar la seguridad, centrándonos en las características propias de este campo. Este objetivo no solo busca asegurar el cumplimiento de la legislación, sino también fortalecer las infraestructuras críticas contra las crecientes amenazas cibernéticas. Al alcanzar este objetivo, se contribuirá a un entorno industrial más seguro, protegiendo tanto a las organizaciones como a la sociedad en general. Además, el enfoque integral de este proyecto permitirá identificar y mitigar riesgos específicos, optimizar el uso de recursos y fomentar una cultura de ciberseguridad proactiva en todo el sector industrial.

y como **objetivos** secundarios de este proyecto se incluyen:

- **Establecer un marco para la implementación de la Directiva NIS2 en un parque eólico:** Establecer y diseñar una metodología que permita establecer la aplicación práctica de la directiva basándose en las instalaciones de parques eólicos. Este objetivo aborda la necesidad de adaptar los principios y requisitos de la directiva a un contexto específico dentro del sector de energías renovables, asegurando que los parques eólicos puedan cumplir con las normativas de ciberseguridad y mejorar su resistencia frente a ciberamenazas.

### **1. Análisis de los requisitos de la Directiva NIS2 aplicables a parques eólicos**

El primer paso para establecer un marco de implementación es realizar un análisis detallado de los requisitos de la Directiva NIS2 y su aplicabilidad específica a los parques eólicos. Esto incluye identificar los aspectos de la directiva que son más relevantes para la operación y seguridad de los parques eólicos, tales como la protección de sistemas SCADA que son críticos para el control y monitoreo de las turbinas eólicas. Estos sistemas son redes de software y hardware que se encargan de supervisar y monitorear máquinas e instalaciones industriales. Por ejemplo, una empresa como Enercon podría llevar a cabo una auditoría exhaustiva de sus sistemas SCADA para identificar vulnerabilidades y asegurarse de que cumplen con los requisitos de la NIS2.

### **2. Diseño de una metodología de implementación**

Basándose en el análisis de los requisitos, se debe diseñar una metodología de implementación que incluya pasos claros y definidos para cumplir con esta normativa. Esta metodología debe considerar las particularidades operativas y tecnológicas de los parques eólicos, proponiendo soluciones específicas para la protección de sus infraestructuras críticas. El diseño de esta metodología incluirá la identificación de tecnologías de seguridad adecuadas, prácticas de gestión de riesgos y protocolos de respuesta a incidentes. Por ejemplo, se podrían implementar tecnologías de inteligencia artificial como IBM Watson for Cyber Security para la

detección de anomalías en los sistemas SCADA. Esta tecnología utiliza algoritmos de aprendizaje automático para analizar grandes volúmenes de datos en tiempo real y detectar patrones inusuales que podrían indicar una amenaza de ciberseguridad. Además, Darktrace es otra solución de inteligencia artificial que puede ser utilizada para predecir y prevenir posibles fallos en las turbinas eólicas mediante el análisis predictivo. Estas herramientas permiten una respuesta rápida y eficiente ante posibles amenazas, asegurando la protección de las infraestructuras críticas del parque eólico.

### **3. Evaluación de la infraestructura actual de los parques eólicos**

Para adaptar la metodología a la realidad operativa, es necesario realizar una evaluación exhaustiva de la infraestructura actual de los parques eólicos. Esto implica revisar los sistemas y tecnologías existentes, identificar vulnerabilidades y evaluar la capacidad de los parques para implementar las medidas de seguridad requeridas. Por ejemplo, al evaluar un parque eólico, se podría descubrir que los sistemas SCADA (Supervisory Control and Data Acquisition) existentes tienen vulnerabilidades que podrían ser explotadas. En respuesta, la evaluación podría recomendar la actualización de los sistemas SCADA a versiones más seguras, la implementación de firewalls específicos para sistemas industriales y la segmentación de redes para limitar el acceso a estos sistemas críticos. Esta evaluación debe incluir tanto componentes de hardware como software, así como las prácticas de gestión y mantenimiento actuales.

- **Analizar la transferibilidad de la Directiva NIS2 al sector del transporte ferroviario:** Abordar y estudiar la manera en que los principios y requisitos implícitos en la directiva pueden ser aplicables al ámbito del transporte por tren, centrándose en la ciberseguridad. Este objetivo se centra en entender las particularidades del transporte ferroviario y en desarrollar estrategias específicas que aseguren la seguridad cibernética dentro de este sector crítico.



### **1. Evaluación de las particularidades del transporte ferroviario**

El primer paso es comprender las particularidades operativas y técnicas del sector ferroviario, al igual que habíamos hecho con el sector eólico, pero aplicadas a este sector. Esto incluye una revisión exhaustiva de los sistemas de señalización, control de trenes, comunicación y gestión del tráfico ferroviario. Es crucial entender cómo estos sistemas difieren de otras infraestructuras críticas y qué requisitos particulares de ciberseguridad necesitan. Por ejemplo, Deutsche Bahn ha llevado a cabo revisiones exhaustivas de sus sistemas de señalización y control para identificar vulnerabilidades específicas y adaptarlas a las normativas actuales de ciberseguridad.

### **2. Identificación de riesgos y amenazas específicas**

A continuación, es esencial identificar los riesgos y amenazas cibernéticas específicas que enfrenta el sector ferroviario. Esto puede incluir amenazas a los sistemas de control de trenes, posibles interrupciones en las comunicaciones ferroviarias y ataques a los datos de gestión del tráfico. Un ejemplo es la identificación de amenazas específicas a los sistemas de control de trenes en Alemania, donde se descubrió que ciertas infraestructuras críticas eran vulnerables a ataques de denegación de servicio (DoS), lo que llevó a la implementación de medidas preventivas más estrictas.

### **3. Adaptación de los requisitos de la Directiva NIS2**

Basado en la comprensión de las particularidades del sector y los riesgos identificados, se debe adaptar los requisitos de la Directiva NIS2 a las necesidades del transporte ferroviario. Esto implica revisar y ajustar las políticas de seguridad existentes para cumplir con las nuevas regulaciones. Por ejemplo, Deutsche Bahn ha adaptado sus políticas de gestión de riesgos y ciberseguridad para alinearlas con los requisitos de la Directiva NIS2, asegurando así una mayor resiliencia ante posibles ciberataques.

#### **4. Desarrollo de capacidades internas**

La implementación exitosa de la Directiva NIS2 en el transporte ferroviario requiere el desarrollo de capacidades internas robustas, al igual que se debe hacer en el parque eólico. Esto incluye la formación especializada del personal en ciberseguridad ferroviaria, la creación de equipos dedicados a la gestión de la seguridad y la implementación de programas continuos de capacitación y concienciación. Un operador regional de servicios de energía de la UE ha demostrado la efectividad de tales programas al formar a su personal en los últimos métodos de prevención de ciberamenazas y mejorar significativamente su respuesta ante incidentes de seguridad.

- **Identificar desafíos y oportunidades en la aplicación de la Directiva NIS2:** Reconocer las barreras y las facilidades para la aplicación exitosa de esta directiva, incluyendo desafíos y oportunidades en torno a tecnologías emergentes, políticas de gobernanza y capacidades de respuesta a incidentes.

##### **1. Análisis de barreras en la implementación**

Identificar y analizar las barreras técnicas, organizativas y económicas que dificultan la implementación de la Directiva NIS2. Ejemplos incluyen la resistencia al cambio, la falta de formación del personal y los altos costos de implementación.

##### **2. Evaluación de tecnologías emergentes**

Evaluar cómo tecnologías emergentes como la inteligencia artificial, el aprendizaje automático y el blockchain pueden integrarse en las estrategias de ciberseguridad para cumplir con los requisitos de la directiva es otro paso importante. Por ejemplo, la implementación de algoritmos de aprendizaje automático como TensorFlow puede mejorar significativamente la detección de anomalías en tiempo real, mientras que la tecnología blockchain puede proporcionar un registro inmutable de las transacciones y eventos de seguridad, mejorando la trazabilidad y la integridad de los datos.

### **3. Evaluación de oportunidades para la mejora continua**

Identificar oportunidades para mejorar las estrategias de ciberseguridad mediante enfoques proactivos y preventivos, optimizando recursos y maximizando beneficios económicos, es esencial para la mejora continua. Implementar programas de gestión de riesgos y mejorar la colaboración e intercambio de información entre organizaciones pueden ser estrategias efectivas. Un ejemplo sería la participación en redes de ciberseguridad, donde las empresas ferroviarias y eólicas pueden compartir información sobre amenazas y mejores prácticas, fortaleciendo colectivamente su postura de seguridad.

En definitiva, identificar desafíos y oportunidades en la aplicación de la Directiva NIS2 es esencial para promover un entorno de seguridad robusto. Este enfoque ayuda a superar barreras, optimizar recursos y mejorar continuamente la ciberseguridad, garantizando que las organizaciones estén preparadas para enfrentar amenazas crecientes y mantener la seguridad de sus infraestructuras críticas.

- **Proponer recomendaciones:** Según el análisis y la evaluación anteriores, desarrollar un conjunto de recomendaciones estratégicas y prácticas que pueden ayudar a guiar a otras infraestructuras en el proceso de cumplimiento de la Directiva NIS2. Estas recomendaciones servirán como guía para otras infraestructuras críticas en su proceso de cumplimiento, optimizando la ciberseguridad y asegurando una mayor capacidad de resistencia frente a ciberamenazas.

Con ello, estos objetivos no solo demuestran un compromiso con la progresión de la ciberseguridad industrial y la defensa de infraestructura crítica, pero, más bien, buscan proporcionar un valor agregado a la industria.

### **1.5 Estado de la cuestión**

La ciberseguridad industrial se ha destacado con el tiempo como un pilar fundamental para la protección de infraestructuras críticas. Actualmente, el sector industrial no se encuentra en un momento de estabilidad, sino que vienen épocas de grandes transformaciones, lo cual supone un reto para la seguridad de la información. La entrada de tecnología avanzada a la operativa industrial, conocida como la cuarta revolución industrial o Industria 4.0, ha supuesto un salto en eficiencia jamás visto, pero también ha evidenciado focos de riesgos importantes.

Como resumen de las **soluciones** tecnológicas aplicadas hasta la fecha, se pueden apuntar variantes, **desde el enfoque tradicional de la seguridad perimetral hasta las soluciones de inteligencia artificial para la detección proactiva de amenazas**. Sin embargo, la gran parte de ellas **requerirá modificaciones y/o mejoras para cumplir con los requisitos específicos de la directiva NIS2**, diseñado para aumentar el nivel de seguridad de los sistemas de información de la UE.

De las comparaciones con otras industrias que han implementado directrices similares, emerge un modelo de **desafíos** comunes. Entre ellos se encuentran la **falta de claridad de la regulación, la dificultad de aplicación en sistemas ya existentes, y la ausencia de personal calificado en ciberseguridad**. Estas observaciones son fundamentales para lograr que el cuadro no solo cuide de la directiva, sino su funcionamiento práctico y eficiente en la industria.

#### **Situación actual en sectores específicos**

Como se ha comentado anteriormente, **en sectores como el eólico y ferroviario, no hay estudios detallados sobre la implementación del NIS2**. Aunque existen ejemplos de buenas prácticas en sectores como la banca y los servicios de salud, la enseñanza de estos a la industria de las energías renovables y del transporte se encuentra en sus primeras etapas. Por lo tanto, la falta de literatura y el desarrollo de la implementación a nivel industrial elevan la relevancia de este trabajo, ya que no solo debería cerrar el vacío existente, sino que también debería proporcionar la guía necesaria adaptada a estos sectores.

### **Impacto en los sectores industriales**

El impacto afectará a todos los fabricantes, incluidos los que fabrican dispositivos IoT, dispositivos médicos (IoMT) y tecnología operativa (OT). De acuerdo con la directiva NIS2, las instituciones esenciales e importantes deben usar ciertos productos TIC certificados, servicios TIC y procesos TIC u obtener un certificado bajo un esquema europeo de certificación de ciberseguridad. Esto estipula la seguridad de sus productos durante todo el proceso de desarrollo. Esto plantea un desafío importante, especialmente en los casos en que los productos de IoT son particularmente vulnerables a los ataques cibernéticos porque están contruidos con controles de seguridad inadecuados, como contraseñas codificadas, falta de cifrado de los datos transmitidos o vulnerabilidades de software/firmware difíciles de corregir. Las empresas industriales siempre necesitan la ayuda de socios tecnológicos para configurar e implementar una estrategia de seguridad coordinada. Las graves consecuencias de los ciberataques solo pueden mitigarse o prevenirse con un enfoque general.

Las redes digitales en entornos de fabricación y OT se amplían constantemente y, por supuesto, todos los activos utilizados allí son cada vez más el objetivo de los piratas informáticos. Debido a la aguda situación de amenazas, ahora se requieren conceptos integrales de seguridad de TI/TO que tengan en cuenta las necesidades especiales de la producción industrial y protejan los sistemas industriales complejos del acceso no autorizado y los tiempos de inactividad inminentes de la producción debido a los ataques cibernéticos.

Además de realizar capacitación en seguridad y adherirse a la higiene cibernética, el monitoreo continuo de los activos es un factor crítico para permitir el cumplimiento de las pautas NIS2, ya que solo puede proteger los activos que puede identificar claramente. Este tipo de visibilidad completa permite a los equipos de seguridad ver anomalías y cambios de estado en tiempo real, lo que a su vez reduce el tiempo de investigación del SOC (Security Operations Center) y los posibles daños. En particular, la gestión de vulnerabilidades de activos proporciona información detallada sobre cada activo, sin importar el tipo. Al utilizar la gestión inteligente de activos, las empresas obtienen una visión general completa de las últimas vulnerabilidades y compromisos. Esto les permite asumir un papel proactivo en el fortalecimiento de su ciberseguridad y adelantarse a los actores de amenazas.

### **Estrategias de mitigación y prevención**

Para hacer frente a estos desafíos, es esencial que las empresas adopten un enfoque proactivo y multifacético hacia la ciberseguridad, como se ha comentado en los anteriores puntos. Esto incluye la implementación de tecnologías avanzadas para la detección y respuesta a incidentes, la creación de protocolos claros de gestión de crisis y la formación continua del personal en prácticas de seguridad. Además, es fundamental establecer una cultura organizativa que valore la ciberseguridad como una prioridad estratégica, integrando estas prácticas en todos los niveles de la organización. La cooperación entre diferentes sectores y la creación de alianzas estratégicas con proveedores de tecnología y expertos en ciberseguridad también juegan un papel crucial en la mejora de la resistencia frente a las amenazas cibernéticas.

### **Capacitación y desarrollo de competencias**

La falta de personal calificado en ciberseguridad es uno de los desafíos más significativos que enfrentan las industrias. Para abordar esta brecha, es esencial invertir en programas de capacitación y desarrollo de competencias que preparen a la próxima generación de profesionales de ciberseguridad. Las empresas deben colaborar con instituciones educativas y organizaciones de formación para desarrollar perfiles que se alineen con las necesidades del sector industrial. Además, fomentar un entorno de aprendizaje continuo y proporcionar oportunidades de desarrollo profesional para el personal existente puede ayudar a mejorar las capacidades internas y asegurar que las empresas estén bien equipadas para enfrentar las amenazas emergentes.

### **Implementación de buenas prácticas de ciberseguridad**

Las mejores prácticas de ciberseguridad, derivadas de sectores con alta madurez en este ámbito como la banca y los servicios de salud, pueden servir como referencia para otros sectores industriales. Estas prácticas incluyen la segmentación de redes, el uso de autenticación multifactor, la implementación de cifrado robusto y la realización de auditorías regulares de seguridad. Además, es crucial establecer procesos claros para la gestión de incidentes de ciberseguridad, incluyendo la identificación, contención, erradicación y

recuperación de ataques. La documentación y el análisis de incidentes pasados también pueden proporcionar valiosas lecciones aprendidas y mejorar la capacidad de respuesta ante futuras amenazas.

### *Segmentación de redes*

La segmentación de redes consiste en dividir una red de TI en múltiples segmentos más pequeños, cada uno de los cuales actúa como una subred independiente. Este proceso tiene varios beneficios clave:

**1. Mejora de la seguridad:** Al dividir la red en segmentos, se pueden aplicar políticas de seguridad específicas a cada uno de ellos, lo que limita la capacidad de un atacante para moverse lateralmente dentro de la red. Si un segmento es comprometido, los otros segmentos permanecen protegidos.

**2. Control de acceso:** La segmentación permite controlar y restringir el acceso a recursos críticos. Solo los usuarios y dispositivos que necesiten acceso a un segmento específico pueden obtenerlo, reduciendo el riesgo de acceso no autorizado.

**3. Reducción del alcance de los ataques:** En caso de un ataque, la segmentación ayuda a contener el impacto, ya que los atacantes no pueden fácilmente pasar de un segmento a otro. Esto limita el daño y facilita la contención y respuesta al incidente.

**4. Mejora del rendimiento:** La segmentación puede mejorar el rendimiento de la red al reducir la cantidad de tráfico que pasa por cualquier segmento dado. Esto también facilita la gestión de la red y la resolución de problemas.

### *Autenticación multifactor (MFA)*

La autenticación multifactor es un método de control de acceso que requiere que los usuarios proporcionen dos o más factores de autenticación independientes para verificar su identidad. Estos factores pueden incluir algo que el usuario sabe (como una contraseña), algo que el usuario tiene (como un token de seguridad o un dispositivo móvil) y algo que el usuario es (como una huella dactilar o reconocimiento facial).

- 1. Mayor seguridad:** MFA añade una capa adicional de seguridad, ya que incluso si un atacante obtiene una contraseña, aún necesitaría el segundo factor para acceder a la cuenta.
- 2. Reducción del fraude:** MFA reduce significativamente el riesgo de fraude y accesos no autorizados, protegiendo mejor la información sensible y las cuentas de los usuarios.
- 3. Cumplimiento normativo:** Muchas normativas de seguridad requieren el uso de MFA para acceder a sistemas críticos y datos sensibles, lo que ayuda a las organizaciones a cumplir con estos requisitos.

### *Cifrado robusto*

El cifrado robusto implica el uso de algoritmos de cifrado fuertes para proteger los datos en reposo y en tránsito. El cifrado **convierte los datos en un formato codificado que solo puede ser descifrado por personas autorizadas con la clave correcta.**

- 1. Protección de datos:** El cifrado protege los datos sensibles de ser accedidos por personas no autorizadas, incluso si son interceptados durante la transmisión o robados de un dispositivo de almacenamiento.
- 2. Cumplimiento de la normativa:** Muchas leyes y regulaciones de protección de datos, como el GDPR en Europa, requieren el uso de cifrado para proteger la información personal y sensible.
- 3. Confidencialidad:** El cifrado asegura que solo los destinatarios previstos puedan leer y acceder a los datos, manteniendo la confidencialidad de la información.

### *Auditorías regulares de seguridad*

Las auditorías de seguridad son evaluaciones sistemáticas y periódicas de la infraestructura de TI de una organización para identificar vulnerabilidades y asegurar el cumplimiento de las políticas de seguridad.

- 1. Identificación de vulnerabilidades:** Las auditorías ayudan a identificar puntos débiles y vulnerabilidades en los sistemas antes de que puedan ser explotados por atacantes.



**2. Cumplimiento normativo:** Las auditorías garantizan que la organización cumpla con las regulaciones y normativas de seguridad pertinentes, evitando sanciones y multas.

**3. Mejora continua:** Las auditorías proporcionan información valiosa que puede ser utilizada para mejorar continuamente las políticas y prácticas de seguridad de la organización.

### *Gestión de incidentes de ciberseguridad*

La gestión de incidentes de ciberseguridad implica la identificación, contención, erradicación y recuperación de ataques cibernéticos. Tener procesos claros para la gestión de incidentes es crucial para minimizar el impacto de un ataque y recuperar rápidamente las operaciones normales.

**1. Identificación:** Detectar y reconocer rápidamente un incidente de seguridad es fundamental para iniciar una respuesta eficaz.

**2. Contención:** Limitar el alcance y el impacto del incidente para evitar que se propague a otros sistemas o datos.

**3. Erradicación:** Eliminar la causa raíz del incidente y asegurar que el sistema esté limpio y seguro antes de restaurar las operaciones.

**4. Recuperación:** Restaurar y validar los sistemas afectados para volver a las operaciones normales de manera segura y controlada.

**5. Lecciones aprendidas:** Analizar el incidente y la respuesta para identificar áreas de mejora y fortalecer las defensas futuras.

### *Documentación y análisis de incidentes*

La documentación y el análisis de incidentes pasados son esenciales para aprender de los errores y mejorar la respuesta a futuros ataques.

- 1. Registro detallado:** Mantener registros detallados de todos los incidentes, incluyendo cómo fueron detectados, la respuesta implementada y los resultados obtenidos.
- 2. Análisis post-incidente:** Realizar análisis exhaustivos de cada incidente para entender las causas raíz y los puntos de falla en la seguridad.
- 3. Mejora continua:** Utilizar la información obtenida del análisis para mejorar las políticas, procedimientos y tecnologías de seguridad, fortaleciendo así la postura de seguridad de la organización.

## CAPÍTULO 2: SECTOR FERROVIARIO

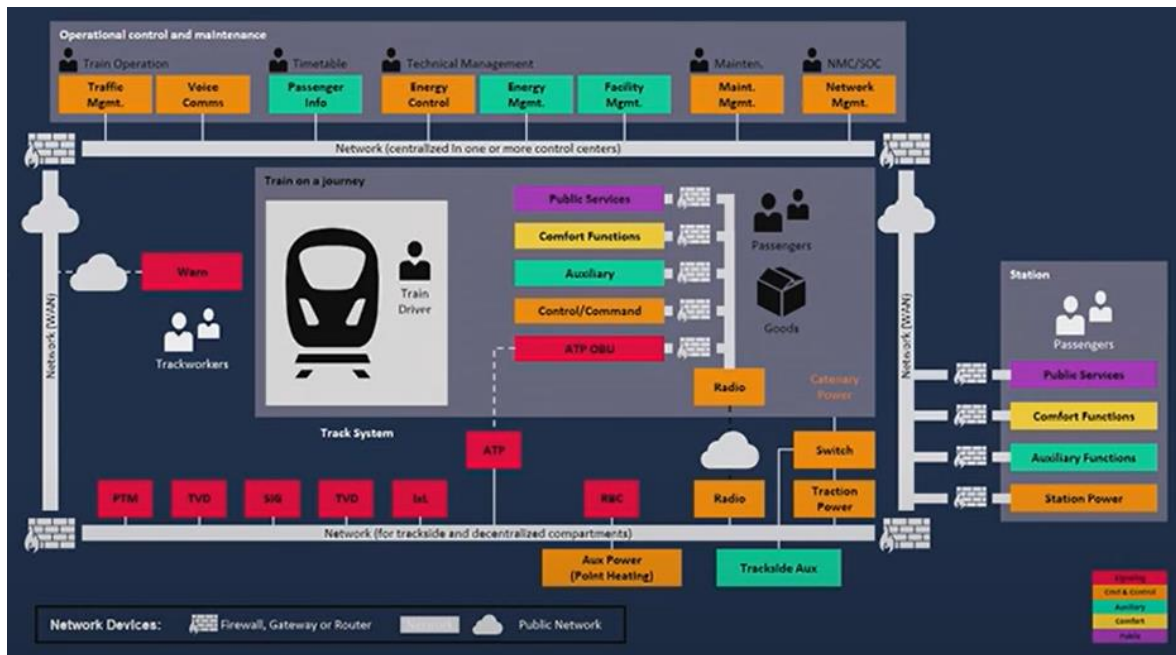
### 2.1 Retos de ciberseguridad en este sector

En un sector con un claro aumento de la digitalización, las oportunidades se incrementan, desde un mejor aprovechamiento de las infraestructuras, es decir, con las mismas infraestructuras ahora es posible tener una frecuencia mucho mayor de trenes, hasta una reducción de costes, ya que en cuanto automatizas determinadas funciones, se pueden abaratar los costes mantenimiento.

Estas oportunidades no vienen sin un coste, ya que un aumento de digitalización supone un aumento de interconectividad, por un lado, y por otro, un aumento de la dependencia de esas funciones digitales. Esto deriva en un aumento de la superficie de ataque, por un lado, y por otro, un impacto potencial mucho mayor en caso de incidente de ciberseguridad.

Un tren es un sistema muy complejo, ya que al fin y al cabo es un centro de datos sobre raíles, que se compone a su vez de subsistemas complicados. Por un lado, tenemos la zona de control, con los sistemas que controlan los frenos, la velocidad del tren, etc. Por otro lado, tenemos la zona de la red del operador del tren, donde se pueden encontrar servicios de videovigilancia, el sistema de megafonía, etc. Por otro lado, tenemos la zona de pasajeros, donde se encuentran el sistema de información de los pasajeros, internet a bordo, etc. Y por último, tenemos la zona de tierra, donde se hace el control de flotas, control de capacidad, etc.

Con esto, se puede observar que el tren no es un producto, sino que es un sistema realmente complejo. En este diagrama se puede apreciar lo complejo que es:



*Ilustración 5: Diagrama del sistema de un tren, en el cual cada una de las cajitas representa un subsistema dentro de un modelo ideal. La parte en rojo muestra los sistemas más críticos, es decir, los sistemas de señalización del tren, que es lo que se encarga de evitar que haya colisiones entre estos. La parte naranja son los sistemas de control (frenos, velocidad, etc.). Por otro lado, tenemos sistemas auxiliares, sistemas de confort, y servicio que se puedan proporcionar a los pasajeros. Fuente: Vídeo de Omar Benjumea, Siemens Mobility.*

Estos subsistemas se encuentran interconectados entre sí, formando un gran sistema, que depende de cada uno de estos subsistemas. Al estar interconectados, se pueden extraer conclusiones obvias de lo que puede pasar si tan solo uno de ellos recibe un ciberataque y es perpetrado por este.

Habiendo podido observar que este sector es considerablemente vulnerable a estos ciberataques, su historial, que a continuación se muestra, no demuestra lo contrario.

Estos son unos de los principales incidentes en el sector, llegando al daño físico a personas, como en 2008, en un tranvía en Polonia, donde hubo un descarrilamiento.

## Recent railway sector incidents

2015 Ukraine: DoS attack as part of the large-scale coordinated attack

2015-16 United Kingdom: Intrusion (reconnaissance phase)

2017 Germany: Ransomware (Wannacry)

2018 Denmark: DDoS impacting ticketing systems. 15k customers affected

2020 United Kingdom: Data breach. 10k passenger who used WiFi

2020 Switzerland: Malware. Manufacturer hit and steal sensitive data

2020 Spain: ADIF hit by ransomware exposing gigabytes of data

*Ilustración 6: Historial de los principales incidentes en el sector ferroviario recientemente, habiendo llegado al daño físico de personas. Fuente: Vídeo de Omar Benjumea, Siemens Mobility.*

Todos estos incidentes provocan una limitación por parte de los reguladores, como la directiva NIS 2, ya que como se ha podido observar, de lo contrario no se puede alcanzar un nivel mínimo de ciberseguridad.

### 2.2 Casos reales:

- **Caso de Estudio 1: Eurostar, empresa de transporte**

En virtud de la directiva NIS2, Eurostar, la empresa de transporte transeuropea que opera los servicios de trenes de alta velocidad que conectan Londres con París y Bruselas a través del Eurotúnel, tuvo que reevaluar su infraestructura de ciberseguridad. Gracias a una evaluación detallada de los riesgos, la empresa descubrió varias vulnerabilidades en sus sistemas heredados. Actualizaron su sistema, implantaron una gestión de acceso más estricta y crearon un sólido plan de respuesta contra las posibles amenazas a la ciberseguridad. Con

estos cambios, aseguraron su conformidad con la Directiva NIS2, fortificando su resiliencia operativa.

- **Caso de Estudio 2: Deutsche Bahn, empresa ferroviaria alemana**

En virtud de la directiva NIS2, Deutsche Bahn, la principal empresa ferroviaria de Alemania, tuvo que reevaluar su infraestructura de ciberseguridad. A través de una evaluación exhaustiva de los riesgos, Deutsche Bahn identificó múltiples vulnerabilidades en sus sistemas de señalización y control de trenes. Decidieron actualizar sus sistemas, implementaron medidas de autenticación multifactorial para el acceso a los sistemas críticos y desarrollaron un plan de respuesta ante incidentes de ciberseguridad.

Además, la empresa participó activamente en redes de cooperación y compartición de inteligencia cibernética con otros operadores ferroviarios europeos. Estos cambios no solo aseguraron su conformidad con la Directiva NIS2, sino que también fortalecieron significativamente su postura de ciberseguridad, garantizando operaciones más seguras y eficientes en un entorno cada vez más digitalizado y complejo. Como resultado, Deutsche Bahn pudo continuar sus operaciones de manera beneficiosa y mantener la confianza de sus pasajeros y socios comerciales.

Estos casos subrayan cómo los proveedores y las empresas afectadas por la Directiva NIS2 se están adaptando de forma proactiva al cambio en el panorama normativo, asegurando su continuidad empresarial y preservando la confianza de sus partes interesadas en el proceso.

Teniendo en cuenta estos casos de mercado, mi objetivo es seguir sus pasos en función de los errores cometidos, e implementarlos en el parque eólico y en la red ferroviaria.

En cuanto al primer caso de estudio, como conclusión extraigo implantar directamente una gestión de acceso estricta y crear un sólido plan de respuesta contra posibles amenazas a la ciberseguridad.

En cuanto al segundo caso de estudio, como conclusión, extraje la necesidad de actualizar los sistemas de señalización y control de trenes, implementar medidas de autenticación multifactorial y desarrollar un plan de respuesta ante incidentes de ciberseguridad. Además,

fomentar la participación activa en redes de cooperación y compartición de inteligencia cibernética ha demostrado ser esencial para fortalecer la postura de ciberseguridad y asegurar operaciones más seguras y eficientes en Deutsche Bahn.

### **2.3 Estándares de ciberseguridad en el sector ferroviario**

El sector ferroviario se enfrenta a desafíos únicos en términos de ciberseguridad debido a la complejidad y la criticidad de sus operaciones. Los estándares de ciberseguridad son fundamentales para garantizar que los sistemas ferroviarios funcionen de manera segura y eficiente. A continuación, se presenta una descripción más detallada de algunos de los principales estándares de ciberseguridad aplicables al sector ferroviario:

#### **1. ISO/IEC 27001:**

Este estándar internacional proporciona un marco para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). Incluye requisitos para la evaluación de riesgos, la implementación de controles de seguridad y la gestión de incidentes.

##### Aplicación en el sector ferroviario:

- ✓ Gestión de riesgos: Identifica y evalúa riesgos específicos relacionados con la información y los sistemas de control en el sector ferroviario.
- ✓ Controles de seguridad: Implementa controles de seguridad técnicos y organizativos para proteger la confidencialidad, integridad y disponibilidad de la información.
- ✓ Gestión de incidentes: Establece procedimientos para la identificación, notificación y gestión de incidentes de seguridad de la información.

#### **2. IEC 62443:**

Este estándar se centra en la ciberseguridad para los sistemas de control industrial (ICS). Proporciona un marco para proteger los sistemas de automatización y control industrial contra ciberamenazas.

#### Aplicación en el sector ferroviario:

- ✓ Protección de sistemas de control: Implementa medidas de seguridad específicas para los sistemas de señalización y control de trenes, que son críticos para la operación segura del sistema ferroviario.
- ✓ Segmentación de redes: Segmenta las redes de control industrial para limitar la propagación de ataques y proteger los sistemas más críticos.
- ✓ Acceso seguro: Controla y monitorea el acceso a los sistemas de control industrial para prevenir accesos no autorizados y detectar actividades sospechosas.

### **3. TS 50701:**

Este es un estándar específico para la ciberseguridad en el sector ferroviario desarrollado por el Comité Técnico 9X de CEN/CENELEC. Proporciona directrices para la gestión de riesgos de ciberseguridad en sistemas ferroviarios.

#### Aplicación en el sector ferroviario:

- ✓ Evaluación de riesgos: Realiza evaluaciones de riesgos de ciberseguridad para identificar vulnerabilidades en los sistemas ferroviarios y determinar las medidas de mitigación adecuadas.
- ✓ Protección de infraestructuras críticas: Implementa medidas de protección para las infraestructuras críticas del sistema ferroviario, como los centros de control y los sistemas de comunicación.
- ✓ Respuesta a incidentes: Establece procedimientos para la respuesta a incidentes de ciberseguridad, incluyendo la detección, contención, erradicación y recuperación de incidentes.

### **4. NIST SP 800-53:**

Proporciona un catálogo de controles de seguridad y privacidad para los sistemas de información federales de los Estados Unidos. Aunque es un estándar estadounidense, es ampliamente reconocido y utilizado globalmente.



### Aplicación en el sector ferroviario:

- ✓ Controles de seguridad: Implementa una amplia gama de controles de seguridad para proteger los sistemas de información ferroviarios, incluyendo la gestión de identidad y acceso, la protección de datos y la continuidad del negocio.
- ✓ Monitoreo continuo: Establece programas de monitoreo continuo para detectar y responder a amenazas de ciberseguridad en tiempo real.
- ✓ Capacitación y concienciación: Desarrolla programas de capacitación en ciberseguridad para el personal del sector ferroviario para asegurar que todos estén al tanto de las mejores prácticas y las políticas de seguridad.

## **2.4 Adaptación de los Estándares Actuales del Sector Ferroviario a la Directiva NIS2**

### **Evaluación de Conformidad y Gap Analysis**

(gap Analysis es el proceso utilizado para comparar la situación actual de la organización con un estándar deseado, y la evaluación de conformidad trata de verificar esto)

### **Informe de Conformidad y Brechas**

#### **Revisión de Estándares Actuales:**

- ISO/IEC 27001 Implementado parcialmente. Falta de controles específicos para el sector ferroviario.
- IEC 62443 Implementado en sistemas de control industrial, pero no en todos los subsistemas ferroviarios.
- TS 50701: No implementado completamente. Necesidad de evaluación específica.
- NIST SP 800-53: Implementado parcialmente, principalmente en áreas de TI, pero no en sistemas de control de trenes.

### **Requisitos de la Directiva NIS2:**

- Notificación de Incidentes: Debe realizarse en un plazo de 24 horas.
- Gestión de Riesgos: Evaluación de riesgos cibernéticos y físicos.
- Seguridad de Redes y Sistemas de Información: Medidas técnicas y organizativas para gestionar riesgos.
- Colaboración y Compartición de Información: Participación en redes de cooperación y compartición de inteligencia.

### **Brechas Identificadas:**

1. Falta de Cobertura Completa: Algunos estándares no se aplican en todos los subsistemas ferroviarios.
2. Notificación de Incidentes: Procedimientos actuales no cumplen con los plazos de la NIS2.
3. Gestión de Riesgos: Evaluaciones de riesgos no integran ciberseguridad y riesgos físicos.
4. Colaboración: Falta de participación activa en redes de cooperación y compartición de información.

### **Acciones Correctivas:**

1. ISO/IEC 27001: Expandir la implementación para cubrir todos los subsistemas ferroviarios.
2. IEC 62443: Completar la implementación en todos los sistemas de control industrial.
3. TS 50701: Realizar una evaluación completa y adaptar los procedimientos existentes.
4. NIST SP 800-53: Ampliar la implementación para incluir todos los sistemas críticos.
5. Notificación de Incidentes: Establecer procedimientos que cumplan con los plazos de 24 horas.

6. Gestión de Riesgos: Integrar ciberseguridad y riesgos físicos en las evaluaciones de riesgos.

7. Colaboración: Participar activamente en redes de cooperación y compartición de inteligencia.

### **Refuerzo de la Gestión de Incidentes**

### **Mejora de Procedimientos de Gestión de Incidentes**

#### **Revisión de Procedimientos Actuales:**

- Detección: Implementar SIEM (Security Information and Event Management), que recopila y analiza eventos de seguridad en tiempo real de múltiples fuentes dentro de una organización para detectar y responder a amenazas; y EDR (Endpoint Detection and Response), que monitorea, detecta, investiga y responde a actividades sospechosas en dispositivos individuales como computadoras y servidores., ambas para mejorar la detección de amenazas.

- Notificación: Establecer un protocolo que cumpla con la Directiva NIS2.

- Respuesta: Crear un equipo de respuesta a incidentes (CSIRT) dedicado.

- Recuperación: Desarrollar planes de recuperación detallados para cada tipo de incidente.

#### **Nuevos Procedimientos Implementados:**

1. Detección Mejorada: Implementación de sistemas SIEM y EDR en toda la red ferroviaria.

2. Notificación Rápida: Protocolo de notificación que asegura el reporte de incidentes dentro de 24 horas.

3. Respuesta Coordinada: Creación de un equipo CSIRT con roles y responsabilidades definidos.

4. Recuperación Eficiente: Desarrollo de planes de recuperación detallados y específicos para cada tipo de incidente.

**Ejemplo de esto:**

1. Detección Inicial:

- Sistema SIEM: El sistema de SIEM detecta una actividad anómala y genera una alerta inmediata.

2. Confirmación de Incidente:

- Equipo de Respuesta a Incidentes (CSIRT): El CSIRT recibe la alerta y, en un plazo de 30 minutos, revisa y confirma si se trata de un incidente de seguridad.

3. Clasificación del Incidente:

- Nivel de Severidad: El CSIRT clasifica el incidente según su severidad (Crítico, Alto, Medio, Bajo).

4. Notificación Interna:

- Comunicación Inmediata: Dentro de la primera hora, el CSIRT notifica a los responsables de seguridad y a la alta dirección mediante correo electrónico y sistema de mensajería interna.

5. Preparación de Informe Preliminar:

- Detalles del Incidente: En un plazo de 2 horas, el CSIRT prepara un informe preliminar que incluye:

- Descripción del incidente.
- Hora de detección.

- Sistemas afectados.
- Medidas inmediatas tomadas.

#### 6. Notificación a Autoridades Competentes:

- Informe a Autoridades: Dentro de las 4 horas siguientes, se envía un informe preliminar a la autoridad competente (como el CSIRT nacional o la Agencia de Ciberseguridad) a través de un canal de comunicación seguro.

#### 7. Actualización Continua:

- Informes Intermedios: Cada 4 horas, se envían actualizaciones intermedias sobre el progreso en la mitigación y análisis del incidente.

- Informe Final: En un plazo máximo de 24 horas, se elabora y envía un informe final con:

- Resumen del incidente.
- Impacto detallado.
- Acciones correctivas implementadas.
- Plan de prevención para futuros incidentes.

#### **Ejemplo de Notificación Interna Inicial:**

Asunto: Notificación de Incidente de Seguridad - Nivel Crítico

Fecha y Hora: [Fecha y Hora de la Detección]

Equipo Afectado: [Descripción del Equipo/Sistema Afectado]

Descripción: Se ha detectado una actividad anómala que indica una posible brecha de seguridad en el sistema [Nombre del Sistema].

Acciones Inmediatas: El CSIRT está investigando y ha aislado el sistema afectado para evitar una mayor propagación.

Se proporcionará una actualización en las próximas 4 horas.

Atentamente,

Equipo CSIRT

**Ejemplo de Notificación a Autoridades Competentes:**

Asunto: Informe Preliminar de Incidente de Seguridad - [ID del Incidente]

Fecha y Hora: [Fecha y Hora de la Detección]

Clasificación: Crítico

Descripción del Incidente: El sistema [Nombre del Sistema] ha detectado una actividad anómala que indica una posible brecha de seguridad.

Acciones Inmediatas: Aislamiento del sistema afectado, inicio de investigación detallada.

Impacto Inicial: [Descripción del Impacto Inicial]

Próximos Pasos: Continuación de la investigación, implementación de medidas correctivas.

Se proporcionarán actualizaciones intermedias cada 4 horas.

Atentamente,

[Nombre del responsable de notificación]

Equipo CSIRT

Este protocolo asegura que los incidentes de seguridad se reporten dentro de las 24 horas exigidas, manteniendo una comunicación clara y efectiva tanto internamente como con las autoridades competentes.

## **Mejora de la Resiliencia Operativa**

### **Fortalecimiento de la Resiliencia de los Sistemas Ferroviarios**

#### **Implementación de Redundancias y Planes de Recuperación:**

- Redundancias: Duplicación de sistemas críticos de señalización y control para asegurar que, si uno falla, el otro puede tomar su lugar sin interrupciones.
- Planes de Recuperación: Realización de pruebas regulares de planes de recuperación y continuidad del negocio.
- Virtualización y Respaldo: Uso de tecnologías de virtualización y respaldo para mantener operaciones continuas.

#### **Resultados Obtenidos:**

1. Sistemas Redundantes: Implementación de redundancias en todos los sistemas críticos.
2. Planes Probados: Realización de simulacros trimestrales de recuperación ante desastres para verificar que todos los procedimientos y protocolos funcionan correctamente en situaciones de crisis.
3. Disponibilidad Asegurada: Implementación de tecnologías de virtualización, como VMware vSphere, que es una plataforma de virtualización que permite la creación y gestión de máquinas virtuales en servidores físicos, optimizando el uso de recursos y asegurando la alta disponibilidad de los servicios; y respaldos automáticos, como Veeam Backup & Replication, que es una solución de respaldo que realiza copias de seguridad automáticas de las máquinas virtuales, permitiendo la restauración rápida y eficiente de datos y sistemas en caso de fallos, para garantizar que todos los datos y servicios críticos estén siempre disponibles, incluso en caso de fallos del sistema.

## **Capacitación y Concienciación**

### **Desarrollo de Programas de Capacitación Continua**

### **Programas de Capacitación Implementados:**

- Plan de Capacitación: Módulos específicos sobre la Directiva NIS2 y ciberseguridad ferroviaria.
- Sesiones Periódicas: Formación regular para todo el personal, incluyendo operadores de trenes y personal de TI.
- Simulaciones de Ciberataques: Ejercicios de simulación para entrenar al personal en la respuesta a incidentes.

### **Resultados Obtenidos:**

1. Personal Capacitado: Todo el personal ha recibido formación específica sobre la Directiva NIS2.
2. Simulaciones Realizadas: Realización de simulaciones regulares para mejorar la respuesta a incidentes.
3. Concienciación Aumentada: Mayor concienciación y comprensión de las mejores prácticas de ciberseguridad.

### **Colaboración y Compartición de Información**

#### **Establecimiento de Mecanismos de Colaboración**

#### **Participación en Redes de Cooperación:**

- Redes de Ciberseguridad: Participación activa en redes de ciberseguridad y grupos de trabajo de la UE.
- Acuerdos de Colaboración: Establecimiento de acuerdos con otros operadores ferroviarios y entidades del sector.
- Ejercicios Conjuntos: Participación en ejercicios de ciberseguridad organizados por la UE.



### **Resultados Obtenidos:**

1. Colaboración Activa: Participación en la red europea de ciberseguridad ferroviaria, contribuyendo a discusiones y desarrollos de nuevas estrategias de seguridad.
2. Acuerdos Establecidos: Firma de un acuerdo de colaboración con operadores ferroviarios de Francia y Alemania para compartir información sobre amenazas y buenas prácticas de ciberseguridad.
3. Ejercicios Realizados: Participación en un ejercicio de ciberseguridad organizado por la UE, simulando un ataque cibernético a la infraestructura ferroviaria y evaluando la respuesta coordinada entre diferentes países.

### **Conclusión**

La adaptación de los estándares actuales del sector ferroviario a la Directiva NIS2 ha resultado en una transformación integral que abarca desde la revisión de estándares y procedimientos hasta la implementación de nuevos mecanismos de cooperación y resiliencia operativa. La incorporación de tecnologías avanzadas de detección y respuesta, la mejora de protocolos de notificación de incidentes y la realización de pruebas regulares de recuperación han fortalecido la capacidad del sector para enfrentar ciberamenazas. Además, la colaboración activa en redes de ciberseguridad y la capacitación continua del personal han aumentado la conciencia y la preparación ante incidentes. Estos cambios no solo aseguran el cumplimiento con la Directiva NIS2, sino que también han mejorado significativamente la postura de ciberseguridad del sector ferroviario, garantizando operaciones seguras y eficientes en un entorno cada vez más digitalizado y complejo.

### **2.5 Coste estimado sector ferroviario**

Ejemplo de precio estimado para una empresa que fabrica trenes, y a su vez los comercializa.

### **Evaluación de Conformidad y Gap Analysis**

- Consultoría y análisis de brechas: Este coste incluye la contratación de consultores especializados en ciberseguridad para llevar a cabo un análisis detallado de las brechas

actuales en el cumplimiento de los estándares. Se estima un equipo de consultores trabajando durante aproximadamente 2-3 semanas, a un precio de 2.500 € por consultor, y de 8 consultores, que serían **20.000€**.

- Generación de informes detallados: La generación de informes detallados incluye aproximadamente 40 horas de análisis y redacción a unos 75 €/hora (3000 €), unas 20 horas de revisión a 50 €/hora (1000 €), licencias de software (500 €) y ediciones finales (500 €), asegurando precisión y cumplimiento normativo. Coste estimado: **5.000€**.

Coste total: **25.000 €**

### **Revisión de Estándares Actuales**

- ISO/IEC 27001:

- Expansión de la implementación: La consultoría especializada, con una tarifa de unos 100 €/hora y 80 horas estimadas, totaliza 8,000 €. La capacitación del personal, con una tarifa de 50 €/hora y 80 horas, suma 4,000 €. La integración de sistemas y políticas, con una tarifa de 75 €/hora y 40 horas, asciende a 3,000 €. Coste total estimado: **15.000€**

- Auditorías periódicas: La tarifa para auditores certificados es de unos 125 €/hora, y se estima que cada auditoría requiere 40 horas de trabajo, lo que suma 5,000 € por auditoría. Se realizan dos auditorías al año, lo que totaliza **10,000 €**. Estas auditorías aseguran el cumplimiento continuo de ISO/IEC 27001 mediante revisiones regulares.

- IEC 62443:

- Expansión de la implementación: **11,000 €**

- Consultoría especializada: Se encargan de la revisión e implementación de estándares de control industrial.

- Tarifa: 100 €/hora

- Horas: 60 horas (6,000 €)

- Capacitación del personal: Formación del personal en nuevas políticas y controles específicos para sistemas de control industrial.

- Tarifa: 50 €/hora

- Horas: 60 horas (3,000 €)

- Integración de sistemas y políticas: Integración de los nuevos controles de seguridad en los sistemas de control industrial.

- Tarifa: 100 €/hora

- Horas: 20 horas (2,000 €)

- Auditorías periódicas: **6,000 €**

- Auditorías semestrales: Realización de auditorías semestrales en sistemas de control industrial.

- Tarifa: 100 €/hora

- Horas: 20 horas/auditoría x 2 auditorías = 40 horas (4,000 €)

- Informes y recomendaciones: Preparación de informes y recomendaciones basadas en auditorías.

- Tarifa: 80 €/hora

- Horas: 15 horas (1,200 €)

- Actualización de procedimientos: Actualización de procedimientos para cumplir con los resultados de las auditorías.

- Tarifa: 50 €/hora

- Horas: 16 horas (800 €)

TS 50701:

- Expansión de la implementación: 10,000 €

- Consultoría especializada: Consultoría para la implementación de TS 50701.

- Tarifa: 100 €/hora

- Horas: 40 horas (4,000 €)

- Capacitación del personal: Formación del personal en los nuevos procedimientos y políticas.

- Tarifa: 50 €/hora

- Horas: 60 horas (3,000 €)

- Integración de sistemas y políticas: Adaptación de los sistemas y políticas a los nuevos estándares.

- Tarifa: 100 €/hora

- Horas: 30 horas (3,000 €)

Auditorías periódicas: 6,000 €

- Auditorías semestrales: Auditorías periódicas para asegurar el cumplimiento con TS 50701.

- Tarifa: 100 €/hora

- Horas: 15 horas/auditoría x 2 auditorías = 30 horas (3,000 €)

- Informes y recomendaciones: Preparación de informes detallados.

- Tarifa: 80 €/hora

- Horas: 20 horas (1,600 €)

- Actualización de procedimientos: Mejora y ajuste de procedimientos basados en las auditorías.

- Tarifa: 50 €/hora

- Horas: 28 horas (1,400 €)

#### NIST SP 800-53:

- Expansión de la implementación: 8,000 €

- Consultoría especializada: Revisión y adaptación de políticas de seguridad para incluir todos los sistemas críticos.

- Tarifa: 100 €/hora

- Horas: 40 horas (4,000 €)

- Capacitación del personal: Formación en los nuevos estándares de seguridad.

- Tarifa: 50 €/hora

- Horas: 40 horas (2,000 €)

- Integración de sistemas y políticas: Integración y adaptación de las nuevas políticas de seguridad en los sistemas existentes.

- Tarifa: 100 €/hora

- Horas: 20 horas (2,000 €)

- Auditorías periódicas: **6,000 €**

- Auditorías semestrales: Auditorías periódicas en sistemas críticos.

- Tarifa: 100 €/hora

- Horas: 15 horas/auditoría x 2 auditorías = 30 horas (3,000 €)

- Informes y recomendaciones: Preparación de informes de auditoría.

- Tarifa: 80 €/hora

- Horas: 15 horas (1,200 €)

- Actualización de procedimientos: Actualización de procedimientos de seguridad.

- Tarifa: 50 €/hora

- Horas: 16 horas (800 €)

Coste total: **72,000 €**

**Refuerzo de la Gestión de Incidentes**

Implementación de SIEM: Incluye la instalación, configuración y pruebas del sistema SIEM para monitorear y analizar incidentes de seguridad en tiempo real:

- Tarifa: 150 €/hora
- Horas: 60 horas (9,000 €)

Implementación de EDR: Configuración y despliegue del sistema EDR para la detección y respuesta a amenazas en dispositivos finales:

- Tarifa: 150 €/hora
- Horas: 40 horas (6,000 €)

Entrenamiento del equipo CSIRT: Formación especializada para el equipo CSIRT en el uso de nuevas herramientas y procedimientos de gestión de incidentes:

- Tarifa: 100 €/hora
- Horas: 50 horas (5,000 €)

Coste total: **20,000 €**

### **Mejora de la Resiliencia Operativa**

Sistemas Redundantes: Implementación de redundancias en todos los sistemas críticos (20,000 €)

- Tarifa: 100 €/hora (Consultoría y trabajo técnico especializado en sistemas críticos)

- Horas: 200 horas

Planes Probados: Realización de simulacros trimestrales de recuperación ante desastres (10,000 €)

- Tarifa: 100 €/hora (Desarrollo y simulación de planes por expertos en recuperación de desastres)

- Horas: 100 horas

Disponibilidad Asegurada: Implementación de tecnologías de virtualización y respaldo para mantener operaciones continuas (15,000 €)

- Tarifa: 150 €/hora (Implementación de tecnologías avanzadas como VMware o Veeam)

- Horas: 100 horas

Coste total: **45,000 €**

### **Capacitación y Concienciación**

Personal Capacitado: Todo el personal ha recibido formación específica sobre la Directiva NIS2 (10,000 €)

- Tarifa: 80 €/hora (Desarrollo de programas de formación por expertos en ciberseguridad y cumplimiento normativo)

- Horas: 125 horas



Simulaciones Realizadas: Realización de simulaciones regulares para mejorar la respuesta a incidentes (12,000 €)

- Tarifa: 100 €/hora (Entrenamiento práctico y simulaciones dirigidas por especialistas en ciberseguridad)

- Horas: 120 horas

Concienciación Aumentada: Mayor concienciación y comprensión de las mejores prácticas de ciberseguridad (10,000 €)

- Tarifa: 80 €/hora (Desarrollo de programas de formación por expertos en ciberseguridad y cumplimiento normativo)

- Horas: 125 horas

Coste total: **32,000 €**

### **Establecimiento de Mecanismos de Colaboración**

Colaboración Activa: Participación en redes de ciberseguridad y grupos de trabajo (5,000 €)

- Tarifa: 100 €/hora (Asistencia y contribución en reuniones y actividades de redes de ciberseguridad)

- Horas: 50 horas

Acuerdos Establecidos: Negociación y firma de acuerdos de colaboración (3,000 €)

- Tarifa: 100 €/hora (Negociación y formalización de acuerdos de colaboración)

- Horas: 30 horas

Ejercicios Realizados: Participación en ejercicios conjuntos para mejorar la respuesta coordinada (7,000 €)

- Tarifa: 100 €/hora (Preparación y participación en ejercicios de ciberseguridad)

- Horas: 70 horas

Coste total: **15,000 €**

### Resumen y Total General

Sumando todos los costes desglosados:

➔ **Total General: 209.000€**

| Tipo de coste                                 | Cantidad (€)   |
|-----------------------------------------------|----------------|
| Evaluación de conformidad y Gap Analysis      | 25.000         |
| Revisión de estándares actuales               | 72.000         |
| Refuerzo de la gestión de incidentes          | 20.000         |
| Mejora de la resiliencia operativa            | 45.000         |
| Capacitación y concienciación                 | 32.000         |
| Establecimiento de mecanismos de colaboración | 15.000         |
| <b>Total</b>                                  | <b>209.000</b> |

Tabla 5: Coste desglosado adaptación sector ferroviario a directiva NIS2. Fuente: elaboración propia.

## CAPÍTULO 3: SECTOR EÓLICO

### 3.1 Retos de ciberseguridad en este sector

En el sector eólico, la digitalización ha traído consigo una serie de oportunidades y desafíos significativos. La integración de tecnologías avanzadas en los sistemas de control y monitoreo de los aerogeneradores permite una optimización continua de la producción de energía y una reducción considerable de los costes operativos. Sin embargo, esta creciente digitalización también aumenta la superficie de ataque, exponiendo los sistemas a diversas ciberamenazas.

Un aerogenerador moderno es un sistema altamente complejo que incluye varios subsistemas interconectados: desde los sistemas de control del rotor y las palas hasta los sistemas de comunicación y monitoreo en tiempo real. La interconectividad de estos subsistemas, tanto a nivel local como remoto, implica un incremento en las posibles vulnerabilidades de seguridad. Cualquier brecha en la seguridad puede tener un impacto significativo no solo en la producción de energía, sino también en la seguridad física del equipo y del personal que opera y mantiene estos sistemas.

Además, la dependencia de redes de comunicación para la operación y el mantenimiento remoto de los parques eólicos añade una capa adicional de riesgo. Los ciberataques dirigidos a estas redes pueden interrumpir las operaciones y causar pérdidas económicas significativas. Por lo tanto, es crucial establecer protocolos robustos de ciberseguridad para proteger estos sistemas y asegurar la continuidad de la producción de energía.

Los principales retos de ciberseguridad en el sector eólico incluyen:

1. Interconectividad y Supervisión Remota: La interconectividad entre los aerogeneradores y los sistemas de control centralizado es fundamental para el funcionamiento eficiente de un parque eólico. Sin embargo, esta interconectividad también crea múltiples puntos de entrada potenciales para los ciberatacantes. La supervisión remota, aunque esencial para la gestión eficiente, también abre nuevas vías para posibles intrusiones.

2. Dependencia de Sistemas de TI y Comunicaciones: La operación de parques eólicos depende en gran medida de sistemas de TI y redes de comunicaciones para la transmisión de datos y el control operativo. Las interrupciones en estas redes pueden afectar gravemente la capacidad de monitorizar y controlar los aerogeneradores, impactando la producción de energía y la seguridad del sistema.

3. Complejidad de los Sistemas de Control: Los sistemas de control de los aerogeneradores son cada vez más sofisticados, integrando tecnologías de automatización avanzada. Esta complejidad añade desafíos adicionales en términos de seguridad, ya que los sistemas más avanzados pueden tener más vulnerabilidades que deben ser gestionadas.

4. Protección de Datos Sensibles: Los parques eólicos generan y procesan grandes cantidades de datos, incluidos datos operativos y de rendimiento, que son esenciales para la optimización y el mantenimiento. Proteger estos datos contra el acceso no autorizado y garantizar su integridad es vital para la operación segura y eficiente.

Un parque eólico se compone de varios subsistemas interconectados que trabajan en conjunto para generar y distribuir energía. Cada uno de estos subsistemas desempeña un papel crucial en la operación del parque. A continuación, se presenta un diagrama que ilustra la complejidad y la interconexión de estos subsistemas:

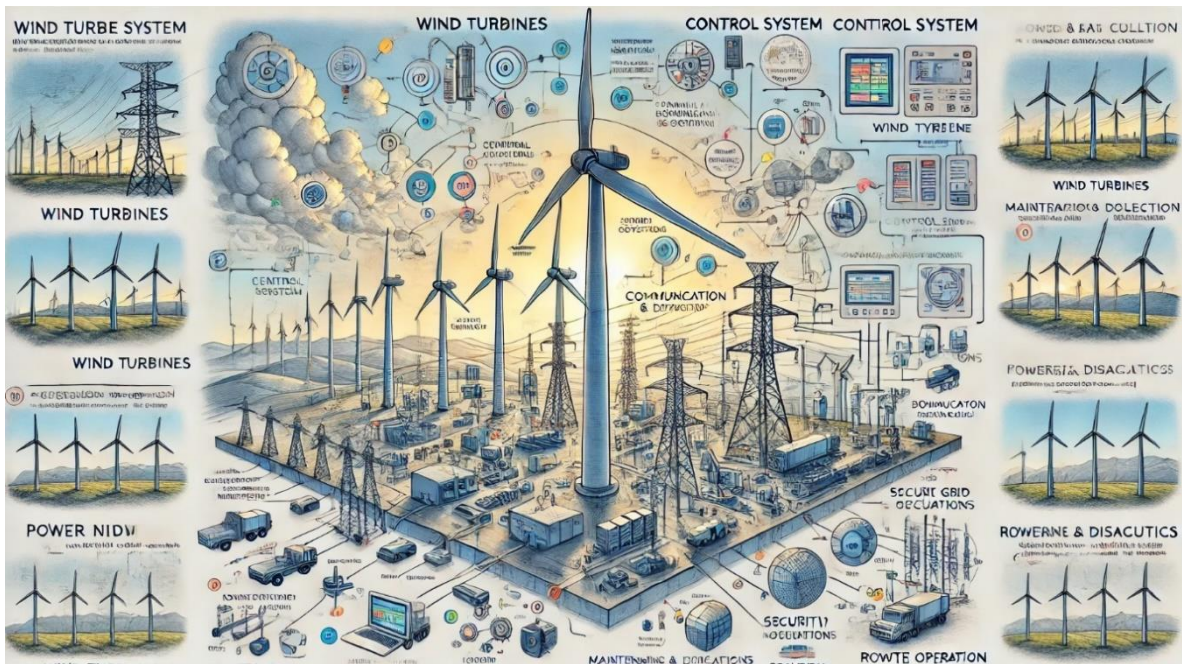


Ilustración 7: Diagrama de los subsistemas de un parque eólico, que trabajan en conjunto para generar y distribuir energía. Cada uno de estos subsistemas desempeña un papel crucial en la operación del parque.

Fuente: Chat GPT.

### Descripción de los subsistemas de la ilustración:

1. Turbinas Eólicas: Las turbinas son los componentes principales del parque eólico. Cada turbina genera electricidad a partir de la energía del viento. Las turbinas están equipadas con sistemas de control que optimizan su rendimiento y aseguran su funcionamiento seguro.
2. Sistema de Control de Energía: Este sistema gestiona la distribución de la electricidad generada por las turbinas, asegurando que se envíe a la red eléctrica de manera eficiente y segura. Incluye sistemas de monitoreo y control en tiempo real.
3. Sistema de Comunicaciones: Es fundamental para la coordinación y operación del parque. Permite la comunicación entre las turbinas y el centro de control, así como la transmisión de datos de rendimiento y estado de las turbinas.

4. Centro de Control: Es el cerebro del parque eólico. Aquí se supervisan y controlan todas las operaciones del parque, desde el funcionamiento de las turbinas hasta la distribución de energía y la gestión de emergencias.

5. Sistemas de Seguridad y Monitoreo: Incluyen cámaras de vigilancia, sensores de seguridad y sistemas de monitoreo ambiental. Aseguran la protección física del parque y el cumplimiento de las normativas medioambientales.

### **Complejidad y Vulnerabilidades:**

Los subsistemas están interconectados, formando un sistema integral que depende de la operación coordinada de cada componente. Esta interconexión implica que un fallo o un ataque cibernético en un subsistema puede tener un efecto dominó en todo el parque. Por ejemplo, un ataque al sistema de comunicaciones podría interrumpir la coordinación entre las turbinas y el centro de control, afectando la eficiencia y la seguridad del parque.

El historial de incidentes en el sector eólico, mostrado más adelante en esta sección, aunque menos conocido que en otros sectores, muestra que es vulnerable a ciberataques. La implementación de la Directiva NIS2 es crucial para establecer medidas de ciberseguridad robustas que mitiguen estos riesgos y aseguren el funcionamiento seguro y eficiente de los parques eólicos.

Cada subsistema, desde los sistemas de control del generador hasta las redes de comunicación y los sistemas de monitoreo, debe ser protegido contra ciberataques. La implementación de medidas de seguridad como la segmentación de redes, el cifrado de comunicaciones y la autenticación multifactor son esenciales para mitigar estos riesgos.

### **Incidentes recientes en el sector eólico**

A continuación, se presentan algunos incidentes recientes en el sector eólico que destacan la importancia de una robusta ciberseguridad:

- 2018: Alemania: Ataque de ransomware a una empresa operadora de parques eólicos que afectó la producción y los sistemas de control, causando interrupciones significativas y pérdidas económicas.

- 2019: Estados Unidos: Intrusión en los sistemas de monitoreo remoto de un parque eólico, resultando en la pérdida de datos críticos y comprometiendo la integridad de la operación.

- 2020: España: Ciberataque a la red de comunicación de un parque eólico que interrumpió la operación de varios aerogeneradores, evidenciando la vulnerabilidad de los sistemas de control.

l- 2021: Dinamarca: Incidente de DDoS que impactó los sistemas de gestión de un parque eólico, afectando la monitorización en tiempo real y la capacidad de respuesta ante emergencias.

Estos incidentes subrayan la necesidad de implementar y mantener medidas de ciberseguridad robustas y actualizadas en el sector eólico, alineadas con normativas como la Directiva NIS2, para asegurar la continuidad operativa y la protección de las infraestructuras críticas.

### 3.2 Casos reales:

- **Caso de Estudio 1: Interrupción de los aerogeneradores de Enercon**

A finales de febrero de 2022, Enercon, la mayor empresa alemana de construcción de aerogeneradores, denunció una **interrupción de 5.800 aerogeneradores producto de una falla en las conexiones satelitales**, eliminando el monitoreo y control remoto de las turbinas eólicas, con una capacidad total de 11 GW.

Este fue uno de los casos más alarmantes para la industria de la generación eólica y las compañías como Phoenix Contact aprovecharon para difundir y concientizar sobre ciberseguridad.

Según explican desde la firma, en todo el mundo, alrededor del 66 % de las pequeñas y medianas empresas industriales ya han sido objeto de ciberataques.

La opción más buscada para lograr una seguridad global es un sistema modular que permite personalizar distintas soluciones según los requisitos para extender la vida útil de un aerogenerador. Mediante estos dispositivos integrados se puede evaluar el estado de las palas y utilizar el mantenimiento predictivo de manera real, programando las actuaciones solamente cuando sean necesarias.

Este control de palas de rotor se denomina Blade Intelligence. Puede reaccionar prematuramente ante eventos y combina la detección de hielo, el control de carga, la medición de las corrientes de rayos y la monitorización estructural.

- **Caso de Estudio 2: Operador de servicios de Energía**

Un operador regional de servicios de Energía de la UE fue identificado como OES en virtud de la directiva NIS2, que hace referencia a las empresas que proporcionan servicios críticos que son esenciales para el funcionamiento de la sociedad y la economía, y que, en el contexto de esta normativa, son identificados y están sujetos a requisitos de ciberseguridad más estrictos debido a la importancia de los servicios que proporcionan. Empezaron un análisis de deficiencias para averiguar en qué aspectos sus operaciones no cumplían la normativa. En consecuencia, intensificaron sus sistemas de detección de brechas de datos, reforzaron su infraestructura informática y formaron regularmente a su personal en los últimos métodos de prevención de ciberamenazas. Sus acciones proactivas les permitieron no sólo cumplir la directiva, sino también estar mejor equipados contra las posibles ciberamenazas.

### **3.3 Estándares de Ciberseguridad en el sector eólico**

La ciberseguridad en el sector eólico es crucial para garantizar la integridad y disponibilidad de la infraestructura de generación de energía. A continuación, se detallan algunos de los principales estándares de ciberseguridad que se aplican específicamente al sector eólico y su implementación:



### **IEC 61400-25**

- Gestión de Comunicaciones y Datos: Este estándar se enfoca en la comunicación para la monitorización y control de parques eólicos. Incluye protocolos para la transmisión segura de datos entre turbinas, sistemas SCADA y centros de control.
- Auditorías de Comunicación: Se realizan auditorías anuales para garantizar la seguridad y la integridad de los canales de comunicación utilizados en el parque eólico.

### **ISO/IEC 27019**

- Seguridad de la Información en el Sector de Energía: Este estándar se adapta específicamente a las necesidades de las empresas de energía. En el sector eólico, implica la implementación de políticas de seguridad que cubran desde la generación hasta la distribución de la energía.
- Revisiones de Políticas: Revisión semestral de las políticas de seguridad para asegurar su relevancia y efectividad en un entorno de amenazas en constante evolución.

### **IEC 62443**

- Seguridad para Sistemas de Automatización Industrial: Este estándar aborda la ciberseguridad en sistemas de control industrial. En el sector eólico, se aplica a los sistemas de control de las turbinas y a la infraestructura de comunicación.
- Pruebas de Vulnerabilidad: Realización de pruebas de vulnerabilidad trimestrales para identificar y mitigar riesgos en los sistemas de control de las turbinas.

### **NERC CIP** (North American Electric Reliability Corporation Critical Infrastructure Protection)

- Protección de Infraestructuras Críticas: Este conjunto de estándares es crucial para la protección de la infraestructura crítica de generación y distribución de energía. Incluye requisitos específicos para la seguridad física y cibernética de los activos críticos en parques eólicos.

- Evaluaciones de Seguridad: Evaluaciones de seguridad anuales para asegurar el cumplimiento con los estándares NERC CIP y la protección de los activos críticos.

### **ISO/IEC 27001**

- Sistema de Gestión de Seguridad de la Información (SGSI): Este estándar proporciona un marco para la gestión de la seguridad de la información. En el sector eólico, incluye la implementación de políticas de seguridad, la gestión de riesgos y la realización de auditorías internas.
- Capacitación Continua: Programas de capacitación y concienciación sobre seguridad de la información para todo el personal del parque eólico, actualizados anualmente para reflejar las últimas amenazas y mejores prácticas.

### **Medidas Específicas de Cumplimiento y Mejora Continua**

- Monitoreo Continuo: Implementación de sistemas avanzados de monitoreo para detectar y responder a incidentes de seguridad en tiempo real.
- Simulaciones de Incidentes: Realización de simulaciones periódicas de ciberataques específicos al sector eólico para evaluar y mejorar la capacidad de respuesta.
- Colaboración Internacional: Participación en redes y foros internacionales de ciberseguridad para compartir información sobre amenazas emergentes y mejores prácticas.
- Actualización de Tecnologías: Evaluación y actualización continua de tecnologías de seguridad utilizadas en la infraestructura del parque eólico, asegurando que se utilicen las soluciones más avanzadas y efectivas disponibles en el mercado.

### **Conclusión**

La implementación de estos estándares de ciberseguridad en el sector eólico asegura una operación segura y eficiente de la infraestructura de generación de energía. Adaptar estos estándares a las necesidades específicas del sector eólico no solo mejora la postura de

ciberseguridad, sino que también garantiza la resiliencia operativa y la continuidad del servicio en un entorno cada vez más digitalizado y complejo.

### **3.4 Adaptación de los Estándares Actuales del Sector Eólico a la Directiva NIS2**

#### **Evaluación de Conformidad y Gap Analysis**

#### **Informe de Conformidad y Brechas**

Se llevará a cabo una evaluación exhaustiva como ya se ha hecho en el anterior sector, aplicada ahora al sector eólico.

#### **Brechas Identificadas y Acciones Correctivas**

##### **Falta de Cobertura Completa:**

- Acción Correctiva: Asegurar que todos los subsistemas del parque eólico cumplan con los estándares de seguridad aplicables. Por ejemplo, extender la cobertura de ISO/IEC 27001 y IEC 62443 para incluir sistemas de soporte y auxiliares, como los sistemas de comunicación interna y los sistemas de monitoreo ambiental.

##### Ejemplo de Acción Correctiva:

Para extender la cobertura de ISO/IEC 27001 e IEC 62443, se deben realizar auditorías internas en todos los subsistemas, incluyendo las áreas de comunicación interna y monitoreo ambiental. Esto implica:

- Auditorías Internas: Realizar auditorías internas trimestrales para evaluar el cumplimiento de los estándares.

- Capacitación del Personal: Capacitar al personal encargado de estos subsistemas en los requisitos específicos de ISO/IEC 27001 e IEC 62443.

- Actualización de Políticas: Revisar y actualizar las políticas de seguridad para incluir controles específicos para los sistemas de comunicación interna y monitoreo ambiental.

### **Notificación de Incidentes:**

- Acción Correctiva: Mejorar los procedimientos de notificación de incidentes para cumplir con los plazos establecidos por la Directiva NIS2. Un ejemplo sería la creación de un equipo de respuesta a incidentes (CSIRT) dedicado, con procedimientos claros para la notificación rápida y eficiente de incidentes.

#### Ejemplo de Acción Correctiva:

Para mejorar la notificación de incidentes, se puede establecer un protocolo detallado que asegure una respuesta rápida y eficiente:

- Establecimiento de un CSIRT: Crear un equipo CSIRT con miembros capacitados en la gestión de incidentes.
- Procedimiento de Notificación: Definir un procedimiento que incluya la detección, clasificación y notificación de incidentes dentro de las primeras 24 horas.
- Herramientas de Notificación: Implementar herramientas automatizadas para la notificación de incidentes a las autoridades competentes y a los stakeholders internos.

### **Gestión de Riesgos:**

- Acción Correctiva: Integrar la gestión de riesgos cibernéticos y físicos en todos los niveles de la organización. Esto podría incluir la implementación de herramientas de análisis de riesgos en tiempo real y la capacitación del personal en la identificación y mitigación de riesgos.

#### Ejemplo de Acción Correctiva:

Para integrar la gestión de riesgos, se pueden implementar las siguientes acciones:

- Herramientas de Análisis de Riesgos: Utilizar software avanzado de análisis de riesgos que permita la identificación en tiempo real de amenazas cibernéticas y físicas.

- Capacitación Continua: Ofrecer programas de capacitación continua al personal para que puedan identificar y mitigar riesgos de manera efectiva.
- Evaluaciones Periódicas: Realizar evaluaciones de riesgos trimestrales para identificar nuevas amenazas y ajustar las estrategias de mitigación.

### **Colaboración:**

- Acción Correctiva: Fomentar la participación en redes de cooperación e intercambio de inteligencia. Un ejemplo sería la firma de acuerdos de colaboración con otros operadores de parques eólicos para compartir información sobre amenazas y coordinar la respuesta a incidentes.

#### Ejemplo de Acción Correctiva:

Para fomentar la colaboración, se pueden realizar las siguientes acciones:

- Redes de Cooperación: Unirse a redes de cooperación de ciberseguridad a nivel europeo y global.
- Acuerdos de Colaboración: Firmar acuerdos con otros operadores de parques eólicos para compartir información y mejores prácticas.
- Ejercicios Conjuntos: Participar en ejercicios de simulación de ciberseguridad organizados por entidades externas para mejorar la coordinación y respuesta conjunta ante incidentes.

### **Nuevos Procedimientos Implementados**

#### **Detección y Respuesta a Incidentes:**

- Implementación: Implementar sistemas avanzados de monitoreo y respuesta (SIEM y EDR) para detectar y responder a incidentes en tiempo real. Por ejemplo, utilizar plataformas SIEM para centralizar la recopilación y análisis de datos de seguridad, y EDR para la detección y respuesta rápida a actividades sospechosas en los sistemas de control de los aerogeneradores.

### Ejemplo de Implementación:

- SIEM: Implementar un sistema SIEM para centralizar la recopilación y análisis de logs de seguridad de todos los sistemas del parque eólico. Este sistema permitirá la detección de patrones anómalos y la generación de alertas en tiempo real.
- EDR: Utilizar soluciones EDR en los sistemas de control de los aerogeneradores para detectar actividades sospechosas y responder rápidamente a posibles amenazas. Esto incluye el monitoreo continuo y la capacidad de aislar dispositivos comprometidos para evitar la propagación del ataque.

### **Notificación y Respuesta Coordinada:**

- Implementación: Crear equipos de respuesta a incidentes (CSIRT) con roles y responsabilidades claramente definidos. Un ejemplo sería establecer un protocolo de respuesta a incidentes que incluya la identificación, clasificación, contención y recuperación de incidentes, con una comunicación clara y efectiva tanto interna como externamente.

### Ejemplo de Implementación:

- Equipo CSIRT: Formar un equipo CSIRT con miembros de diferentes áreas de la organización, incluyendo TI, operaciones y seguridad.
- Protocolo de Respuesta: Definir un protocolo de respuesta que cubra todas las etapas de gestión de incidentes, desde la detección hasta la recuperación. Este protocolo debe incluir la comunicación inmediata con los stakeholders internos y las autoridades competentes.
- Simulacros Regulares: Realizar simulacros regulares para asegurarse de que todos los miembros del equipo CSIRT estén familiarizados con el protocolo y puedan actuar de manera coordinada en caso de un incidente real.

### **Planes de Recuperación Detallados:**

- Implementación: Desarrollar planes de recuperación específicos para cada tipo de incidente. Esto podría incluir la creación de escenarios de simulación para pruebas de

recuperación y la actualización de los planes de contingencia basados en los resultados de estas pruebas.

#### Ejemplo de Implementación:

- Escenarios de Simulación: Crear escenarios de simulación que cubran diferentes tipos de incidentes, como ciberataques, fallos de sistemas y desastres naturales. Estos escenarios deben probar la capacidad de recuperación de los sistemas y la efectividad de los planes de contingencia.
- Actualización de Planes: Basado en los resultados de las simulaciones, actualizar los planes de contingencia para abordar cualquier deficiencia identificada y mejorar la capacidad de respuesta y recuperación ante incidentes futuros.

### **3.5 Coste estimado sector eólico**

Tomando como ejemplo un parque eólico de 3 MW, con 15 turbinas eólicas, el precio estimado, calculado para cada molino por separado, y multiplicado por el número de molinos que conforman el parque, de adaptar todo el funcionamiento a la directiva NIS2 se estima que sea el siguiente:

#### **Evaluación de Conformidad y Gap Analysis por molino**

- Consultoría y análisis de brechas (2.000€): Este coste incluye la contratación de consultores especializados en ciberseguridad para llevar a cabo un análisis detallado de las brechas actuales en el cumplimiento de los estándares.
- Tarifa: 125 €/hora
- Horas: 16 horas

- Generación de informes detallados (800€):

- Tarifa: 100 €/hora

- Horas: 8 horas

Coste total por molino: **2.800 €**

### **Revisión de Estándares Actuales por molino**

- ISO/IEC 27001:

- Expansión de la implementación (1.500€):

- Tarifa: 100 €/hora

- Horas: 15 horas

- Auditorías periódicas (800€): La tarifa para auditores certificados es de unos 125 €/hora, y se estima que cada auditoría requiere 10 horas de trabajo. Asumiendo 4 auditorías:

- Tarifa: 20 €/hora

- Horas: 40 horas

- IEC 62443:

- Expansión de la implementación (1.600€): Consultoría especializada. Se encargan de la revisión e implementación de estándares de control industrial.



- Tarifa: 100 €/hora

- Horas: 16 horas

- Capacitación del personal (900€): Formación del personal en nuevas políticas y controles específicos para sistemas de control industrial.

- Tarifa: 50 €/hora

- Horas: 18 horas

- Integración de sistemas y políticas (600€): Integración de los nuevos controles de seguridad en los sistemas de control industrial.

- Tarifa: 75 €/hora

- Horas: 8 horas

- Auditorías periódicas (700€): Auditorías semestrales en sistemas de control industrial.

- Tarifa: 100 €/hora

- Horas: 7 horas

Coste total por molino: **6.100 €**

### **Refuerzo de la Gestión de Incidentes por molino**

- Implementación de SIEM (1.200€): Incluye la instalación, configuración y pruebas del sistema SIEM para monitorear y analizar incidentes de seguridad en tiempo real.

- Tarifa: 150 €/hora

- Horas: 8 horas

- Implementación de EDR (1.000€): Configuración y despliegue del sistema EDR para la detección y respuesta a amenazas en dispositivos finales.

- Tarifa: 143 €/hora

- Horas: 7 horas

- Entrenamiento del equipo CSIRT (800€): Formación especializada para el equipo CSIRT en el uso de nuevas herramientas y procedimientos de gestión de incidentes.

- Tarifa: 100 €/hora

- Horas: 8 horas

Coste total por molino: **3.000 €**

### **Mejora de la Resiliencia Operativa por molino**

- Sistemas Redundantes (1.500€): Implementación de redundancias en todos los sistemas críticos.

- Tarifa: 100 €/hora

- Horas: 15 horas

- Planes Probados (1.000€): Realización de simulacros trimestrales de recuperación ante desastres.

- Tarifa: 100 €/hora

- Horas: 10 horas

- Disponibilidad Asegurada (1.200€): Implementación de tecnologías de virtualización y respaldo para mantener operaciones continuas.

- Tarifa: 150 €/hora

- Horas: 8 horas

Coste total por molino: **3.700 €**

### **Capacitación y Concienciación por molino**

- Personal Capacitado (800€): Todo el personal ha recibido formación específica sobre la Directiva NIS2.

- Tarifa: 80 €/hora

- Horas: 10 horas

- Simulaciones Realizadas (900€): Realización de simulaciones regulares para mejorar la respuesta a incidentes.

- Tarifa: 100 €/hora

- Horas: 9 horas

- Concienciación Aumentada (800€): Mayor concienciación y comprensión de las mejores prácticas de ciberseguridad.

- Tarifa: 80 €/hora

- Horas: 10 horas

Coste total por molino: **2.500 €**

### **Establecimiento de Mecanismos de Colaboración por molino**

- Colaboración Activa (500€): Participación en redes de ciberseguridad y grupos de trabajo.

- Tarifa: 100 €/hora

- Horas: 5 horas

- Acuerdos Establecidos (300€): Negociación y firma de acuerdos de colaboración.

- Tarifa: 100 €/hora

- Horas: 3 horas

- Ejercicios Realizados (700€): Participación en ejercicios conjuntos para mejorar la respuesta coordinada.

- Tarifa: 100 €/hora

- Horas: 7 horas

Coste total por molino: **1.500 €**

### **Resumen por molino**

Sumando todos los costes desglosados por molino:

- Total por molino: 19.600 €

### **Coste total para 15 molinos**

Multiplicando el coste estimado por molino por el número total de molinos:

- Total General:  $19.600 \times 15 = \mathbf{294.000 \text{ €}}$

Esta nueva estimación proporciona un coste diferenciado del anterior totalizando 294.000 €, abordando todas las áreas críticas de ciberseguridad para un parque eólico de 3 MW con 15 molinos y asegurando el cumplimiento normativo de la Directiva NIS2.

A continuación, una tabla con los costes desglosados:

| <b>Tipo de coste</b>                          | <b>Cantidad (€)</b>          |
|-----------------------------------------------|------------------------------|
| Coste por molino                              |                              |
| Evaluación de conformidad y Gap Analysis      | 2.800                        |
| Revisión de estándares actuales               | 6.100                        |
| Refuerzo de la gestión de incidentes          | 3.000                        |
| Mejora de la resiliencia operativa            | 3.700                        |
| Capacitación y concienciación                 | 2.500                        |
| Establecimiento de mecanismos de colaboración | 1.500                        |
| <b>Total, por molino</b>                      | <b>19.600</b>                |
| <b>Total 15 molinos</b>                       | <b>19.600 * 15 = 294.000</b> |

*Tabla 6: Coste desglosado adaptación sector eólico a directiva NIS2. Fuente: elaboración propia.*

## CAPÍTULO 4: CONCLUSIÓN

Este proyecto ha evaluado en profundidad la viabilidad y los beneficios de implementar la Directiva NIS2 en los sectores eólico y ferroviario, con un enfoque particular en la ciberseguridad de infraestructuras críticas. A través de un análisis detallado de los costos, las necesidades de actualización de estándares y la implementación de nuevas tecnologías y procedimientos, se ha determinado que, a pesar de los costos iniciales significativos, los beneficios a largo plazo justifican esta inversión para las empresas.

Recapitulando, la directiva NIS2 busca establecer un marco de ciberseguridad coherente y robusto en toda la UE, reforzando y ampliando el alcance de su predecesora, la NIS1. La NIS2 no solo mantiene los objetivos de proteger las redes y sistemas de información esenciales para la sociedad y la economía, sino que también introduce requisitos más estrictos y una cobertura más amplia.

Se diseñó para abordar las amenazas emergentes y establecer un marco de ciberseguridad coherente en toda la Unión Europea. A diferencia de su predecesora, la NIS1, la NIS2 amplía su alcance e introduce requisitos más estrictos para la protección de las redes y sistemas de información. La directiva NIS2 obliga a las entidades esenciales y los proveedores de servicios digitales a adoptar medidas de seguridad adecuadas y a reportar incidentes de seguridad significativos a las autoridades competentes. Esta normativa tiene como objetivo mejorar la resiliencia cibernética de las infraestructuras críticas y fomentar la cooperación entre los estados miembros de la UE para enfrentar las amenazas cibernéticas de manera más eficaz.

Los objetivos principales de la Directiva NIS2 incluyen:

1. Ampliación del Alcance: La NIS2 cubre una gama más amplia de sectores y servicios críticos, incluidos no solo los operadores de servicios esenciales, sino también ciertos proveedores de servicios digitales que no estaban completamente cubiertos bajo la NIS1.

2. Requisitos de Seguridad Más Estrictos: La NIS2 impone requisitos de seguridad más rigurosos, obligando a las organizaciones a implementar medidas técnicas y organizativas adecuadas para gestionar los riesgos cibernéticos y proteger sus sistemas de información.
3. Notificación de Incidentes: Las entidades deben notificar los incidentes de seguridad significativos a las autoridades competentes en un plazo específico. Esto incluye la obligación de proporcionar información detallada sobre el incidente y las medidas correctivas adoptadas.
4. Cooperación y Coordinación: La directiva promueve una mayor cooperación y coordinación entre los estados miembros de la UE, facilitando el intercambio de información y mejores prácticas a través de redes y mecanismos establecidos.

#### **4.1 Viabilidad y Beneficios**

A pesar de los costos iniciales, los beneficios derivados de la implementación de la Directiva NIS2 son significativos y justificados para ambos sectores:

1. Mejora de la Seguridad y Resiliencia Operativa: La implementación de medidas avanzadas de ciberseguridad y la mejora de los protocolos de respuesta a incidentes aumentan la capacidad de los parques eólicos y las infraestructuras ferroviarias para resistir y recuperarse de ciberataques, asegurando la continuidad operativa.
2. Cumplimiento Normativo: Cumplir con la Directiva NIS2 evita sanciones y fortalece la posición de la empresa en el mercado, mejorando la confianza de los inversores, clientes y reguladores. Este cumplimiento es crucial para mantener la operatividad y evitar sanciones que pueden surgir de la no conformidad.
3. Reducción de Riesgos: La identificación y mitigación de vulnerabilidades reduce el riesgo de interrupciones significativas que podrían causar pérdidas económicas y daños a la reputación. Esto también abarca la protección contra amenazas internas y externas, esenciales para ambos sectores.



4. Colaboración y Compartición de Información: Participar en redes de cooperación y compartir inteligencia cibernética mejora la capacidad de respuesta a amenazas emergentes y fortalece la postura de ciberseguridad a nivel sectorial. La colaboración con otros operadores también puede conducir a la adopción de mejores prácticas y tecnologías.

5. Mejora Continua y Actualización de Tecnologías: La adopción de nuevas tecnologías y la actualización continua de políticas y procedimientos aseguran que las infraestructuras críticas se mantengan protegidas contra las amenazas emergentes y que se adapten a los cambios en el panorama de la ciberseguridad.

#### **4.2 Comparativa de Costos y Beneficios**

Para el sector eólico, se estimaron costos totales de aproximadamente 294,000 € para cumplir con los requisitos de la Directiva NIS2. Para el sector ferroviario, los costos fueron menos elevados (209.000 €) pero necesarios para asegurar la conformidad y mejorar la resiliencia operativa. En ambos casos, los costos incluyen consultoría, capacitación, implementación de tecnologías avanzadas, auditorías y mejoras continuas.

A pesar de estos costes, los beneficios a largo plazo, como la mejora de la seguridad, la reducción de riesgos, el cumplimiento normativo y la colaboración intersectorial, justifican la inversión inicial. Estas inversiones no solo fortalecen la seguridad cibernética de las infraestructuras críticas, sino que también mejoran la resiliencia operativa y la competitividad de las empresas en un entorno cada vez más digitalizado.

#### **4.3 Conclusión Final**

La adaptación y cumplimiento de la Directiva NIS2 es viable y beneficiosa para las empresas de los sectores eólico y ferroviario. Aunque requiere una inversión inicial considerable, los beneficios a largo plazo en términos de seguridad, cumplimiento normativo, reducción de riesgos y mejora continua justifican plenamente estos costes. La implementación de la NIS2 no solo fortalece la ciberseguridad de las infraestructuras críticas, sino que también contribuye a la estabilidad y sostenibilidad de estos sectores en un entorno cada vez más digitalizado y amenazado por ciberataques.

Las acciones proactivas y colaborativas aseguradas por la NIS2 permiten que las empresas estén mejor preparadas para enfrentar las crecientes amenazas en el entorno digital, garantizando operaciones seguras y eficientes. En última instancia, la implementación de la Directiva NIS2 es una inversión estratégica que refuerza la resiliencia y competitividad de las empresas en el mercado global.

## CAPÍTULO 5: REFERENCIAS

- [SOSA24] SoSafe, “[Artículo sobre tendencias en ciberdelincuencia en 2024](#)”, 2024.
- [ENES22] Energía Estratégica España, “[Artículo sobre claves para mejorar la ciberseguridad de parques eólicos y mejorar su vida útil](#)”, septiembre de 2022.
- [RENF24] Renfe, “[El reto de Renfe para aplicar la tecnología cuántica en la transformación del futuro de la movilidad, y los requisitos de ciberseguridad que esto implica](#)”, Marzo de 2024.
- [RENF23] Renfe, “[La ingente cantidad invertida por parte de Renfe en ciberseguridad entre 2018 y 2023 denota la importancia de esta](#)”, junio de 2023.
- [CIBE24] CyberSeguridad Latam, “[Ataque Eurostar](#)”, julio de 2024.
- [VANG17] La Vanguardia, “[Ataque trenes alemanes](#)”, mayo de 2017.
- [REVE22] Reve, “[Interrupción aerogeneradores Enercon](#)”, marzo de 2022.
- [OMBE22] Omar Benjumea, “[Retos de ciberseguridad en el entorno ferroviario](#)”, enero de 2022.
- [TFMM24] Manuel Benavente, “[TRABAJO FIN DE MASTER: Seguridad de la Información en Europa: Una Comparación entre el Esquema Nacional de Seguridad \(RD 311/2022\) y la Directiva NIS2](#)”, julio de 2024.
- [TFGB24] Blanca Díaz Círrera, “[TRABAJO FIN DE GRADO: Impacto económico y social por los ciberataques en el sector industrial español](#)”, julio de 2024.