COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

GRADO EN INGENIERÍA EN TECNOLOGÍAS INDUSTRIALES

TRABAJO FIN DE GRADO

IMPACTO ECÓNOMICO Y SOCIAL POR LOS CIBERATAQUES EN EL SECTOR INDUSTRIAL ESPAÑOL

Autor: Blanca Díaz Cirera

Director: Raquel Caro Carretero

Madrid 11 Julio 2024

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

Impacto Económico y Social por los Ciberataques en el Sector Industrial Español

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 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.

Blanca

Fdo.: Blanca Díaz Cirera Fecha: ..11../ …07…/ …2024…

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

CARO CARRETERO RAQUEL - 50182083Q

Digitally signed by CARO CARRETERO RAQUEL - 50182083Q
Date: 2024.07.24 12:45:20 +02'00'

Fdo.: Raquel Caro Carretero Fecha: …11…/ …07…/ …2024…

COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

GRADO EN INGENIERÍA EN TECNOLOGÍAS INDUSTRIALES

TRABAJO FIN DE GRADO

IMPACTO ECÓNOMICO Y SOCIAL POR LOS CIBERATAQUES EN EL SECTOR INDUSTRIAL ESPAÑOL

Autor: Blanca Díaz Cirera

Director: Raquel Caro Carretero

Madrid 11 Julio 2024

IMPACTO ECÓNOMICO Y SOCIAL POR LOS CIBERATAQUES EN EL SECTOR INDUSTRIAL ESPAÑOL

Autor: Díaz Cirera, Blanca.
Director: Caro Carretero, Raquel.
Entidad Colaboradora: ICAI – Universidad Pontificia Comillas

RESUMEN DEL PROYECTO

En este Trabajo de Fin Grado se ha evaluado el parque eólico "El Cortijo de Iruelas" en Tarifa, Cádiz. El objetivo de dicha evaluación es simular la integración de la ciberseguridad de este parque eólico, en función de su situación, y aportar conclusiones para realizar un buen uso de este y protegerlo de las amenazas cibernéticas. Se trata de un parque eólico cuya ubicación y características particulares lo hacen vulnerable a distintos tipos de ataques cibernéticos, por lo que es fundamental implementar estrategias de seguridad robustas.

Palabras clave: Malware, Infraestructura crítica, amenazas cibernéticas, parque eólico, simulación, presupuesto, repotenciación.

1. Introducción

Nos encontramos en la era de la digitalización y la conexión global. El sector industrial español se encuentra sumergido en una constante evolución, caracterizado por la gran dependencia de la tecnología y la información digital.

El avance de la tecnología ha traído consigo numerosos progresos y oportunidades, sin embargo, ha expuesto también a las empresas industriales a una poderosa amenaza: los ciberataques. Podríamos definir estos, como ataques informáticos, tanto a nivel nacional como internacional. Estos representan una seria preocupación desde una perspectiva económica como social. (Zuluaga, 2020)

El propósito de mi trabajo de fin de grado es analizar el impacto socioeconómico de los ciberataques en el sector energético industrial español, centrándome sobre todo en el desarrollo de dichos ataques en el sector de eólico. Considero que es un tema importante en el mundo actual, ya que estos ataques no tienen únicamente consecuencias financieras

significativas para las empresas, sino que también pueden llegar a poner en riesgo la seguridad de todos los trabajadores.

A lo largo de este trabajo, examinaré el creciente panorama de amenazas cibernéticas a la que se enfrenta el sector energético español, evaluaré los costos económicos asociados a los ciberataques y analizaré cómo estos percances pueden impactar en la sociedad, llevando consigo desde la pérdida de empleos hasta la interrupción de servicios esenciales. Asimismo, investigaré las medidas de seguridad y estrategias de prevención que las empresas pueden implementar para reducir estos riesgos y proteger su infraestructura.

Nos encontramos en un momento crítico en que la industria española se esfuerza por mantener su competitividad en un mercado globalizado, comprender y abordar adecuadamente el impacto de los ciberataques, ya que esto se convierte en una tarea imperativa. Solo a través de un estudio detallado se podrá velar por los intereses económicos y sociales del sector industrial energético en España. (Arteaga, 2019)

2. Definición del proyecto

El objeto final del proyecto consiste en simular a nivel socioeconómico el impacto de los ciberataques en el sector energético, centrando dicho análisis en la repotenciación del parque eólico de Tarifa “Cortijo de Iruelas”. Estudiaré su situación actual e integraré la amenaza de los ciberataques de este sector a dicho parque eólico. Se ha llevado a cabo una simulación de las consecuencias que supondrían un ciberataque en el Cortijo de Iruelas al igual que sus medidas para prevenir y protegerse de las amenazas.

3. Descripción de la simulación

Dicha simulación está enfocada al cálculo y desglose de costes tanto a nivel energético como económico para la protección y, en un supuesto caso, ataque cibernético.

En primer lugar, se ha realizado una investigación exhaustiva de los distintos softwares desarrollados hoy en día para la protección cibernética de las infraestructuras críticas.

Por consiguiente, se ha realizado un estudio del parque eólico escogido, “Cortijo de Iruelas”, analizando su situación, producción para simular con mayor precisión la integración de la ciberseguridad a dicho parque.

Una vez se tienen en cuenta todos los parámetros y variables que afectan de manera directa la seguridad del parque eólico, se realiza un balance/presupuesto aproximado de la repotenciación del Cortijo de Iruelas. Dentro de dicho balance se hace hincapié en los costes y el desglose de estos a favor de la ciberseguridad del parque.

Es importante recordar que todos los resultados obtenidos son fruto de una simulación con datos aproximados y meramente precisos, ya que la ciberseguridad, no solo en el sector energético, si no en cualquier área y, por consiguiente, en cualquier empresa, tiene la mayoría de sus datos restringidos y protegidos.

Por ende, esta simulación se ha realizado con estudios, análisis y documentos oficiales, publicados por empresas dedicadas a dicho sector, consultoras con proyectos asociados al sector energético, en especial, el eólico, y donde cuyos datos ofrecen estimaciones porcentuales y estadísticas globales.

Por ello, adaptando la situación del Cortijo de Iruelas y el profundo análisis realizado, se ha conseguido evaluar dicho parque eólico para favorecer su ciberseguridad.

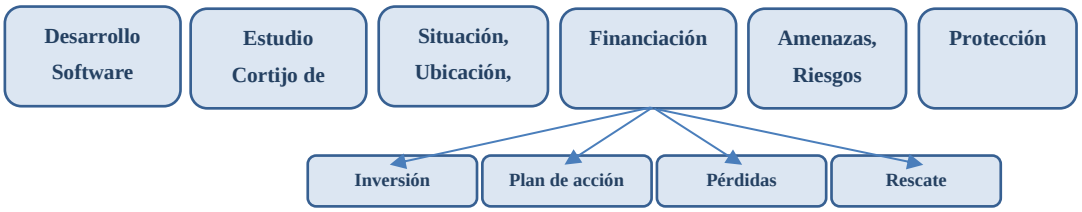

Ilustración 1: Fases Simulación. Elaboración Propia

4. Resultados

Para tener una visión general de la repercusión que está teniendo la amenaza cibernética, no solo a nivel industrial si no global, se ha creado un gráfico de visualización final. Está dividido en 3 series.

La serie roja, corresponde con los sectores dispuestos a financiar el rescate en caso de que su sistema fuese amenazado por un ciberataque. La azul, muestra si las empresas en dicho

sector muestran medidas actuales a favor de la ciberseguridad. Y la naranja, muestra el % de empresas en cada sector que tienen un plan de recuperación en caso de amenaza cibernética.

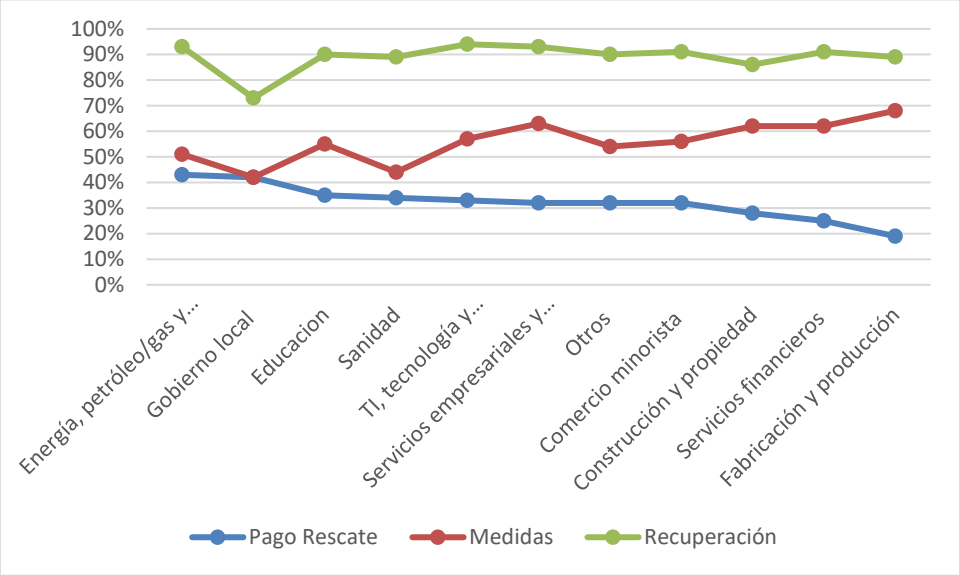

Ilustración 2: Resultado Simulación. Fuente: Elaboración Propia

Se ha obtenido de la simulación el siguiente resultado; el sector energético cuenta con el mayor número de empresas dispuestas a pagar el rescate. Además, es el sector mejor preparado y con mayor número de planes de actuación y medidas impuestas en caso de un ciberataque.

5. Conclusiones

Mediante la elaboración de dicha simulación, se han podido observar una serie de variables clave que hace que la ciberseguridad en nuestro país pueda fortalecerse y combatir mejor las amenazas.

En primer lugar, es necesario elegir bien el software que protegerá toda la infraestructura crítica. La implementación de dicho software va acompañada de un considerable desembolso inicial por parte de la empresa energética.

Es de gran importancia tener en cuenta que, aunque el coste en ciberseguridad sea grande, no garantiza la seguridad de la infraestructura crítica al 100%. Actualmente, el desarrollo de las nuevas tecnologías es cada vez más rápido y abarca amenazas mucho más fuertes y de mayor calibre que antes. Por ello se ha concluido que, no es más importante su protección inicial, que su capacidad de reacción y su resolución al recibir un ataque. (Chen, 2010)

Aquí las empresas en el sector energético se muestran más vulnerables, puesto como a diferencia del resto de sectores, una inhabilitación del sistema operativo del parque eólico tiene una complicada puesta en marcha en comparación con un robo de información del sector financiero, ya que esta podría solucionarse con continuas copias de seguridad. (Centeno, 2015)

6. Referencias

- Arteaga, F. (2019). Ciberseguridad y seguridad integral en el sector energético. Real Instituto Elcano, 9(7).

- Chen, Thomas. Stuxnet, the real start of cyber warfare? [Editor's Note].Network, IEEE 24.6 (2010): 2-3.

- Centeno, F. J. U. (2015). CIBERATAQUES, la mayor amenaza actual. Prebie3, (1), 42.

- Zuluaga, D. (2020). Ciberseguridad para la operación centralizada y distribuida de generación de energía eléctrica en ISAGEN. Ingeniería y Ciencia, 16(32), 171-194. https://publicaciones.eafit.edu.co/index.php/ingciencia/article/download/6282/5066/2260

ECONOMIC AND SOCIAL IMPACT OF CYBERATTACKS ON THE SPANISH INDUSTRIAL SECTOR

Author: Díaz Cirera, Blanca
Supervisor: Caro Carretero, Raquel.
Collaborating Entity: ICAI – Universidad Pontificia Comillas

ABSTRACT

In this Final Degree Project, the wind farm "El Cortijo de Iruelas" in Tarifa, Cádiz, has been evaluated. The objective of this evaluation is to simulate the integration of cybersecurity for this wind farm, based on its situation, and to provide conclusions for its proper use and protection against cyber threats.

Keywords: Malware, Critical infrastructure, Cyber threats, Wind farm, Simulation, Budget, Repowering.

1. Introduction

We are in the era of digitization and global connectivity. The Spanish industrial sector is immersed in constant evolution, characterized by a great dependence on technology and digital information.

The advancement of technology has brought numerous progress and opportunities; however, it has also exposed industrial companies to a powerful threat: cyberattacks. These could be defined as cyber-attacks at both national and international levels. They represent a serious concern from both an economic and social perspective. (Zuluaga, 2020)

The purpose of my final degree project is to analyze the socioeconomic impact of cyberattacks on the Spanish industrial energy sector, focusing primarily on the development of such attacks in the wind energy sector. I consider this to be an important issue in today's world, as these attacks not only have significant financial consequences for companies but can also endanger the safety of all workers.

Throughout this work, I will examine the growing landscape of cyber threats faced by the Spanish energy sector, evaluate the economic costs associated with cyberattacks, and analyze how these incidents can impact society, leading to job losses and disruptions of

essential services. I will also investigate the security measures and prevention strategies that companies can implement to reduce these risks and protect their infrastructure.

We are at a critical moment when the Spanish industry strives to maintain its competitiveness in a globalized market. Understanding and adequately addressing the impact of cyberattacks is becoming an imperative task. Only through detailed study can the economic and social interests of the industrial energy sector in Spain be safeguarded. (Arteaga, 2019)

2. Project Definition

The final objective of the project is to simulate the socioeconomic impact of cyberattacks on the energy sector, focusing this analysis on the repowering of the Tarifa Wind Farm "Cortijo de Iruelas." I will study its current situation and integrate the threat of cyberattacks in this sector to this wind farm. What follows is a brief simulation of the consequences that a cyberattack on the Cortijo de Iruelas would entail, as well as measures to prevent and protect against these threats.

3. Description of the model/system/tool

This simulation focuses on the calculation and breakdown of costs both in terms of energy and economics for protection and, in a hypothetical case, a cyberattack.

Firstly, an exhaustive investigation of the various software developed today for the cybersecurity of critical infrastructures has been carried out. Consequently, a study of the selected wind farm, "Cortijo de Iruelas," was conducted, analyzing its situation and production to simulate more accurately the integration of cybersecurity into this wind farm.

Once all the parameters and variables that directly affect the security of the wind farm are considered, an approximate budget is created for the repowering of Cortijo de Iruelas. This budget emphasizes the costs and their breakdown in favor of the wind farm's cybersecurity.

It is important to remember that all the results obtained are the product of a simulation with approximate and merely precise data since cybersecurity, not only in the energy sector but in any area and consequently in any company, has most of its data restricted and protected.

Therefore, this simulation has been conducted with studies, analyses, and official documents published by companies dedicated to this sector, consulting firms with projects associated with the energy sector, particularly wind energy, where data offer percentage estimates and global statistics.

Thus, by adapting the situation of Cortijo de Iruelas and the thorough analysis carried out, it has been possible to evaluate this wind farm to enhance its cybersecurity.

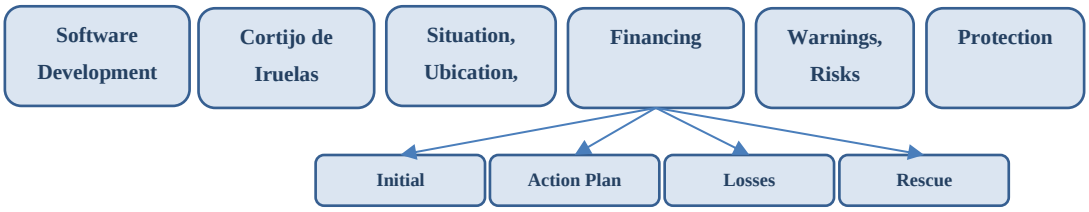

Ilustración 3: Simulation Phases. Source: Own Elaboration

4. Results

To provide a comprehensive overview of the impact that the cyber threat is having, not only on an industrial level but globally, a final visualization chart has been created. It is divided into three series:

The red series corresponds to the sectors willing to finance a ransom in case their system is threatened by a cyberattack. The blue series shows whether companies in that sector currently implement cybersecurity measures. The orange series shows the percentage of companies in each sector that have a recovery plan in case of a cyber threat.

The simulation yielded the following result: the energy sector has the highest number of companies willing to pay a ransom in case their system is threatened by a cyberattack. Moreover, it is the best-prepared sector with the highest number of action plans and measures in place in case of a cyberattack.

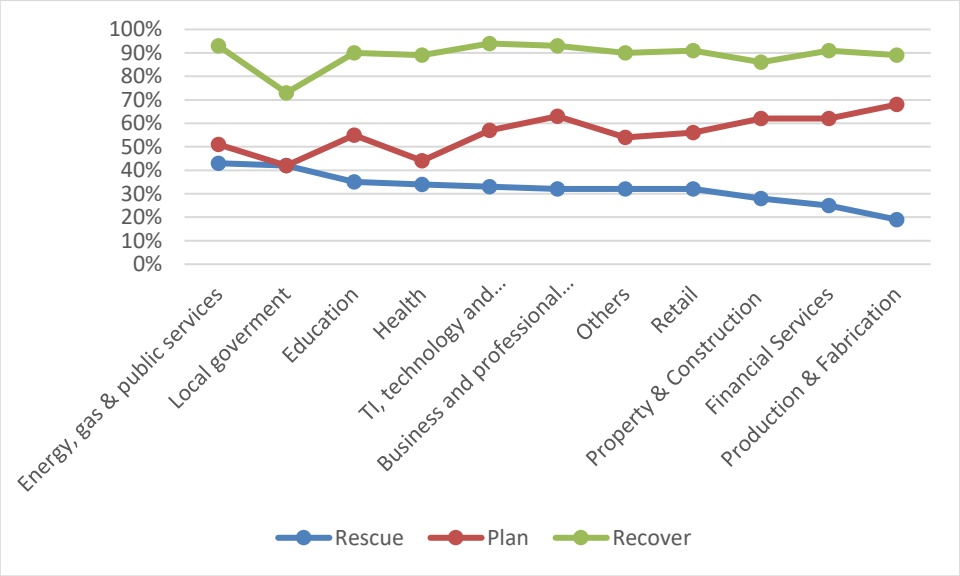

Ilustración 4: Simulation Result. Source: Own Elaboration

5. Conclusions

Through the development of this simulation, several key variables have been observed that can strengthen cybersecurity in our country and better combat threats.

First, it is essential to choose the right software to protect the entire critical infrastructure. The implementation of this software is accompanied by a considerable initial expenditure by the energy company.

It is important to note that, although the cost of cybersecurity is significant, it does not guarantee 100% security of the critical infrastructure. Currently, the development of new technologies is increasingly rapid and encompasses much stronger and more severe threats than before. Therefore, it has been concluded that the initial protection is not as important as the capacity for reaction and resolution when an attack occurs. (Chen, 2010)

Here, companies in the energy sector show more vulnerability. Unlike other sectors, the disabling of the wind farm's operating system involves a complicated restart process compared to the theft of information in the financial sector, which could be resolved with continuous backups. (Centeno, 2015)

6. References

- Arteaga, F. (2019). Ciberseguridad y seguridad integral en el sector energético. Real Instituto Elcano, 9(7).

- Chen, Thomas. Stuxnet, the real start of cyber warfare? [Editor's Note].Network, IEEE 24.6 (2010): 2-3.

- Centeno, F. J. U. (2015). CIBERATAQUES, la mayor amenaza actual. Prebie3, (1), 42.

- Zuluaga, D. (2020). Ciberseguridad para la operación centralizada y distribuida de generación de energía eléctrica en ISAGEN. Ingeniería y Ciencia, 16(32), 171-194. https://publicaciones.eafit.edu.co/index.php/ingciencia/article/download/628 2/5066/2260

Índice de la memoria

Índice de figuras

Índice de tablas

Capítulo 1. INTRODUCCIÓN

En este capítulo se hace una introducción de este proyecto despertando el interés del lector por el proyecto y describiendo la motivación del proyecto.

1.1 MOTIVACIÓN DEL PROYECTO

Actualmente, el crecimiento exponencial de las redes sociales nos expone a riesgos imperceptibles en nuestra vida diaria.

Aunque no siempre somos conscientes de ello, el incremento de ciberataques en nuestro país se convierte cada vez en un hecho más frecuente. La elección de mi Trabajo de Fin de Grado (TFG) fue acompañada por una investigación de todas las opciones disponibles. Aunque lo que realmente me hizo escoger este TFG fue la gran curiosidad al descubrir la creciente vulnerabilidad del sector industrial español, especialmente el ámbito de la energía, ante estos ataques cibernéticos.

Aunque no sean amenazas que nos expongan todos los días ante diversos peligros, son cada vez más frecuentes los ataques con fines bélicos, por ejemplo, la invasión de Ucrania.

Por eso, considero que este proyecto no solo es fascinante, sino también educativo, y me brinda la oportunidad de adquirir conocimientos de gran interés. La necesidad de abordar la seguridad cibernética en el sector energético español resalta la importancia de comprender y contrarrestar los peligros emergentes en un mundo cada vez más interconectado.

Con esta elección, busco contribuir al fortalecimiento de la infraestructura digital y a la protección de sectores energéticos ante amenazas que podrían afectar significativamente nuestra sociedad.

Capítulo 2. ESTADO DE LA CUESTIÓN

Para analizar el principal problema de los ciberataques en el sector energético he querido estudiar uno de los ataques más famosos del mundo para analizar que causas lo motivaron, que consecuencias tuvo y como se solucionó. Se ha de tener en cuenta que las empresas energéticas son las que más ciberataques sufrieron en 2023, con casi el 40% de las ofensivas. El transporte, otro de los puntos primordiales en las economías actuales, fue el segundo con el 22% aproximadamente. El sector financiero acumuló casi el 18% de los ataques y el agua fue víctima del 8%. (Interempresas, 2023)

Un ciberataque que ha llamado mi atención ha sido el de **Stuxnet.**

Stuxnet, es conocido por ser un malware de magnitudes extraordinarias. Su existencia se reconoce en el verano de 2010 al dirigirse específicamente a infraestructuras industriales en Irán, cuyo enfoque principal residía en centrales nucleares y plantas de energía. (Chen, 2010) Este sofisticado virus, el cual es considerado el más avanzado hasta la fecha, logró infiltrarse en los sistemas energéticos, robar información y, posteriormente, ordenar la autodestrucción de las máquinas afectadas.

El impacto de este malware en el programa nuclear iraní fue de gran importancia, aunque el gobierno nunca reveló oficialmente los datos sobre los daños causados. Expertos aseguran que Stuxnet contribuyó significativamente a retrasar el progreso nuclear en Irán. Su desarrollo requeriría meses de trabajo y un respaldo económico considerable.

El virus Stuxnet llevó afectó directamente la infraestructura física del mundo real. Controló aproximadamente mil máquinas en una planta nuclear, instruyéndolas para generar su propia destrucción. Este evento marcó la primera vez que un ciberataque logró causar daños tangibles a la infraestructura crítica.

El modus operandi de Stuxnet involucró la penetración en la red a través de una memoria USB infectada. Una vez dentro, se propagó a través de los ordenadores, identificó y

reprogramó el software que controlaba las máquinas. Lo que les hacía tan importantes a estas centrifugadoras, era que facilitaban el enriquecimiento del Uranio.

Stuxnet llevó a cabo dos tipos de ataques:

El primero fue, que aceleró peligrosamente las centrifugadoras durante un corto período antes de restaurar la velocidad normal.

Y el segundo fue que, aproximadamente un mes después, las desaceleró durante un período más prolongado. Esto causó tensiones en las máquinas, resultando eventualmente en su destrucción.

Stuxnet, estudió y aprovechó cuatro puntos débiles desconocidos hasta entonces por el sistema operativo Windows de Microsoft. Utilizando una "firma digital" robada, este malware se camufló como un programa legítimo durante su infiltración. Además, permaneció inactivo, y en modo fantasma, durante un mes, observando y registrando datos antes de desencadenar la autodestrucción de las máquinas.

Por lo que sabiendo esto, concluyo que, para prevenir ciberataques similares, es necesario subrayar la importancia de seguir prácticas de seguridad efectivas. Un ejemplo de estas sería, adoptar las medidas de seguridad que ISAGEN elaboró en Colombia. ISAGEN, es la segunda empresa de generación eléctrica de Colombia, que se ha preocupado ampliamente por alistarse y ayudar al sector en su preparación frente a posibles ataques cibernéticos (Zuluaga, 2020).

El caso de Stuxnet, al igual que la respuesta de ISAGEN ante los ciberataques, sirven como recordatorio de la necesidad de mantenerse alerta frente a amenazas sofisticadas y adoptar medidas proactivas para proteger la infraestructura crítica

Capítulo 3. DEFINICIÓN DEL TRABAJO

3.1 JUSTIFICACIÓN

En el sector eólico, la mayoría de las empresas no muestran a sus clientes ni publican la inversión ni las medidas aplicadas a la ciberseguridad, esto es obvio de explicar, ya que esos datos son confidenciales para prevenir ataques y amenazas a cualquier empresa.

La ciberseguridad es una actividad presente en la vida de todas las empresas, no solo industriales. Es cierto que, dependiendo del tipo de empresa, tamaño y manejo de la información se le puede dar más o menos importancia a la seguridad frente a las ciber amenazas.

Pero ¿hasta qué punto se conoce el impacto de la ciberseguridad en los sectores industriales, en concreto el eólico? ¿Cuánto invierten las empresas de dicho sector en ciberseguridad? ¿Se obtiene rendimiento? La respuesta a esta pregunta es complicada de responder ya que únicamente conocemos estimaciones y estudios que aportan distintas empresas dedicadas a la ciberseguridad. Es por eso, por lo que no es fácil y la mayoría de las veces casi imposible encontrar datos exactos de lo destinado a la ciberseguridad de una empresa concreta.

3.2 OBJETIVOS

Los objetivos que persigo en la ejecución de este TFG abarcan diversos aspectos cruciales.

- Estudio/Análisis ciberataques: En primer lugar, trataré de explicar en lo que constituye un ciberataque, cuáles son las causas, efectos y el problema que esto supone. A continuación, profundizaré en el análisis de las razones que posicionan al sector de la energía como el más vulnerable ante ciberataques.
- Evolución impacto económico y social: Además, pretendo recopilar y analizar estadísticas y datos concernientes al volumen de ciberataques en el parque eólico

de Tahivilla "El Cortijo de Iruelas", proporcionando una visión cuantitativa del problema.

- Estrategias y propuestas: Asimismo, pretendo abordar medidas estratégicas destinadas a reducir la incidencia de estos ataques, contribuyendo así a fortalecer la ciberseguridad de dicho parque eólico.

3.3 METODOLOGÍA

La metodología que se ha seguido en el proyecto consta de los siguientes pasos:

1. Búsqueda de información de la ciberseguridad, tipo de ciberataques, recorrido a lo largo de la historia, ciberataques más famosos, impacto en la sociedad.
2. Búsqueda de información de los parques eólicos, su funcionamiento, generación, producción y desarrollo de la energía.
3. Estudio de los distintos parques eólicos de Tarifa para su posterior análisis.
4. Profundización en el parque eólico escogido, en este caso, "El Cortijo de Iruelas", funcionamiento, generación, desarrollo de la energía, localización, situación actual
5. Impacto económico de dicho parque eólico, su repotenciación, inversión, gastos, etc.
6. Cálculo de los distintos costes del parque eólico, en función de la ciberseguridad
7. Medidas y plan de acción del parque eólico
8. Riesgos y amenazas del sector
9. Consecuencias de una posible amenaza/ataque. Repercusión económica y social.
10. Futuros trabajos planteados para la consecución del objetivo final.

Capítulo 4. CONTEXTO ACTUAL

Para comenzar a desarrollar el contenido de mi Trabajo de Fin de Grado, es necesario comenzar exponiendo su protagonista, el viento. Él es el que hace posible el funcionamiento de los parques eólicos y él que produce la energía que se nos transfiere a nuestros hogares.

4.1 EL VIENTO

El viento es el resultado del flujo de aire entre zonas causado por la diferencia de presiones de aire, que se calientan debido a la incidencia de radiación solar, de esta manera, la energía eólica es energía solar convertida en energía eólica.

Es complicada predecir cómo aparece el viento (velocidad, dirección, turbulencia, ...), ya que depende de factores globales y locales: rotación de la tierra, posición de la luna, diferencia de temperaturas global y local, orografía de terreno, rugosidad de la superficie, obstáculos, etc.

Sólo estudios y observaciones exhaustivos, gracias a la mayor potencia de los ordenadores y los métodos estadísticos, son capaces de acercarnos a valores reales. Con estos modelos de datos se puede intentar estimar el potencial eólico en un emplazamiento concreto.

Los datos principales del viento son los de la velocidad expresada en metros por segundos [m/s] y los de la dirección en grados [º].

4.1.1 LA ROSA DE LOS VIENTOS

Para determinar el emplazamiento de la instalación es fundamental La Rosa de los Vientos. Su utilidad principal radica en que proporciona la dirección o direcciones principales con su frecuencia en un diagrama circular del permitiendo así ubicar el aerogenerador en el sitio idóneo.

Cada punta de la rosa representa una dirección cardinal o intermedia, como norte, sur, este, oeste, noreste, noroeste, sureste y suroeste. Según expresa el "diccionario náutico" también representa cuatro rumbos laterales, ocho colaterales y 16 co-colaterales. La Rosa de los Vientos de 32 puntas es la más completa de todas. Ya que esta representa la misma cantidad de direcciones que toma el viento, los 32 diferentes rumbos posibles.

Sin embargo, en el análisis usaré para mayor facilidad la Rosa de los Vientos de 16 puntas.

Esta Rosa de los Vientos de 16 puntas proporciona buena precisión en la orientación y la navegación, esto hace que sea especialmente útil en situaciones donde se requiere un alto grado de precisión en las direcciones.

Las direcciones marcadas son:

Norte **(N),** Norte-Noreste **(NNE),** Noreste **(NE)** Noroeste **(NO),** Norte-Noroeste **(NNO)**

Este-Noreste **(ENE),** Este **(E),** Este-Sureste **(ESE)**

Sureste **(SE)**, Sur-Sureste **(SSE),** Sur **(S),** Sur-Suroeste **(SSO),** Suroeste **(SO)**

Oeste-Suroeste **(OSO),** Oeste **(O),** Oeste-Noroeste **(ONO)**

En el ejemplo, la dirección dominante es NNE, orientación que se debe mantener libre de obstáculos, para su posterior construcción de parques eólicos.

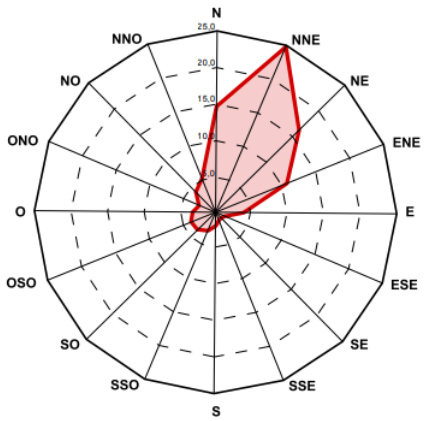

Ilustración 5: Rosa de los Vientos. Fuente AAE

En caso de que no se distinga claramente el viento dominante, se utiliza además un diagrama que muestra las direcciones principales de máxima potencia, siendo la potencia proporcional al cubo de la velocidad del viento.

4.1.2 OBSTÁCULOS

En la mayoría de los casos los obstáculos son edificios y árboles que desvían el viento y producen turbulencias, por lo que deben ser tenidos en cuenta y evitados al buscar la mejor ubicación. Hay dos tipos de obstáculos, los que dejan pasar partes del viento (porosos) y los que no (no porosos).

- Porosos: Como arbustos, árboles, verjas, vallas, torres de celosía e incluso otros aerogeneradores. En la práctica, y si es imposible evitarlos, y se recomienda instalar el aerogenerador a entre 7 y 10 veces el diámetro del obstáculo.

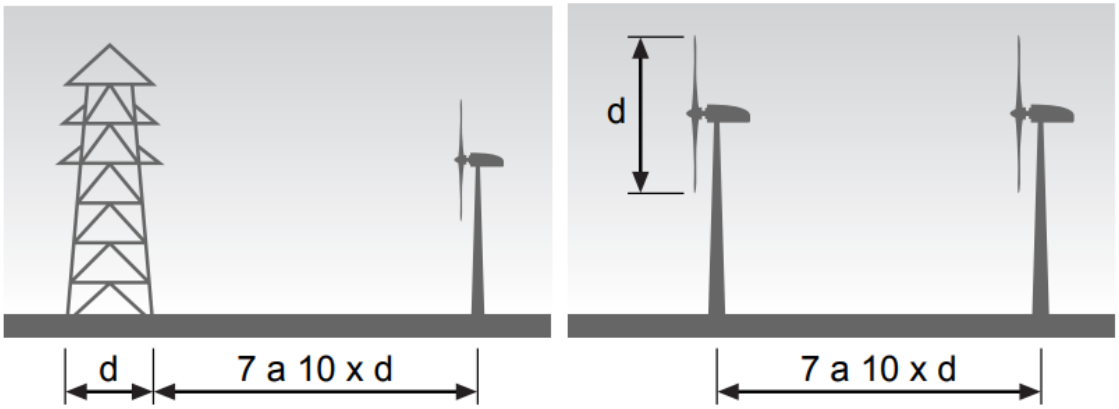

Ilustración 5: Obstáculos porosos. Fuente: AAE

- No porosos: Un ejemplo de estos serían casas, muros y vallas o densas arboladas que no dejan pasar el viento y crean fuertes turbulencias. Es muy aconsejable instalar el aerogenerador a barlovento del obstáculo (por delante).

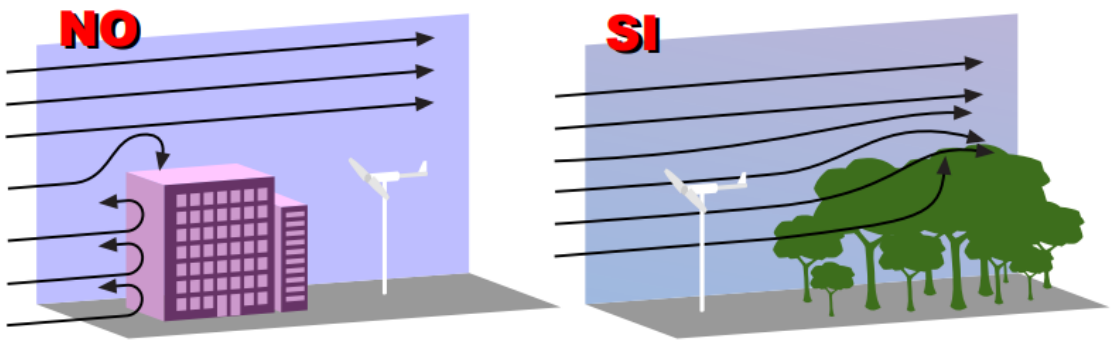

Ilustración 6: Obstáculos no porosos. Fuente: AAE

4.2 ENERGÍA EÓLICA

La energía eólica es aquella que se genera al transformar el movimiento de las corrientes de aire en energía eléctrica. Para aprovechar el viento que se produce en tierra, se construyen enormes complejos eólicos capaces de extraer el máximo potencial de este recurso limpio y renovable.

4.3 PARQUES EÓLICOS

Los parques eólicos terrestres son las infraestructuras encargadas de producir energía eléctrica a partir del viento que se produce en emplazamientos en tierra. Para ello, se diseñan y construyen una serie de elementos capaces de transformar la energía cinética del viento en energía eléctrica, primero, y de convertirla en electricidad apta para el consumo, después, e integrarla en la red de distribución.

4.3.1 FUNCIONAMIENTO

La energía eléctrica se produce en el aerogenerador. Se trata de una estructura que se sustenta sobre una cimentación de hormigón armado para garantizar su estabilidad y funcionalidad. Cuenta con un controlador que inicia y detiene la turbina según las condiciones climáticas, así como con un mecanismo que determina la dirección del viento y le permite orientarse correctamente. (AAE, 2011)

La fuerza del viento hace girar las palas del aerogenerador, que están diseñadas para captar al máximo esa energía cinética: pueden moverse incluso con vientos muy suaves, desde 11 kilómetros por hora. Las palas están unidas a la turbina a través del buje, que a

su vez está conectado al eje lento, que gira a la misma velocidad de las aspas (entre 7 y 12 revoluciones por minuto).

Una multiplicadora eleva esa velocidad más de 100 veces y la transfiere al eje rápido, que se mueve a más de 1.500 revoluciones por minuto. Dicha fuerza se transmite al **generador** (algunas tecnologías utilizan generadores de baja velocidad acoplados directamente al eje lento), **donde la energía cinética se transforma en energía eléctrica.** Y de ahí pasa al convertidor, que la transforma en corriente alterna. (AAE, 2011)

La energía eléctrica producida es de baja tensión, por lo que se conduce hasta un transformador que la eleva a media tensión (entre 20 y 66 kV) para que pueda ser transportada por el parque.

Desde allí se traslada hasta la **subestación, que convierte la energía en corriente de alto voltaje** (más de 132 kV). Esta electricidad, ya apta para el consumo, se transfiere a través de la línea de evacuación (generalmente aérea) hasta las instalaciones conectadas a la red de distribución, que la lleva finalmente a los hogares.

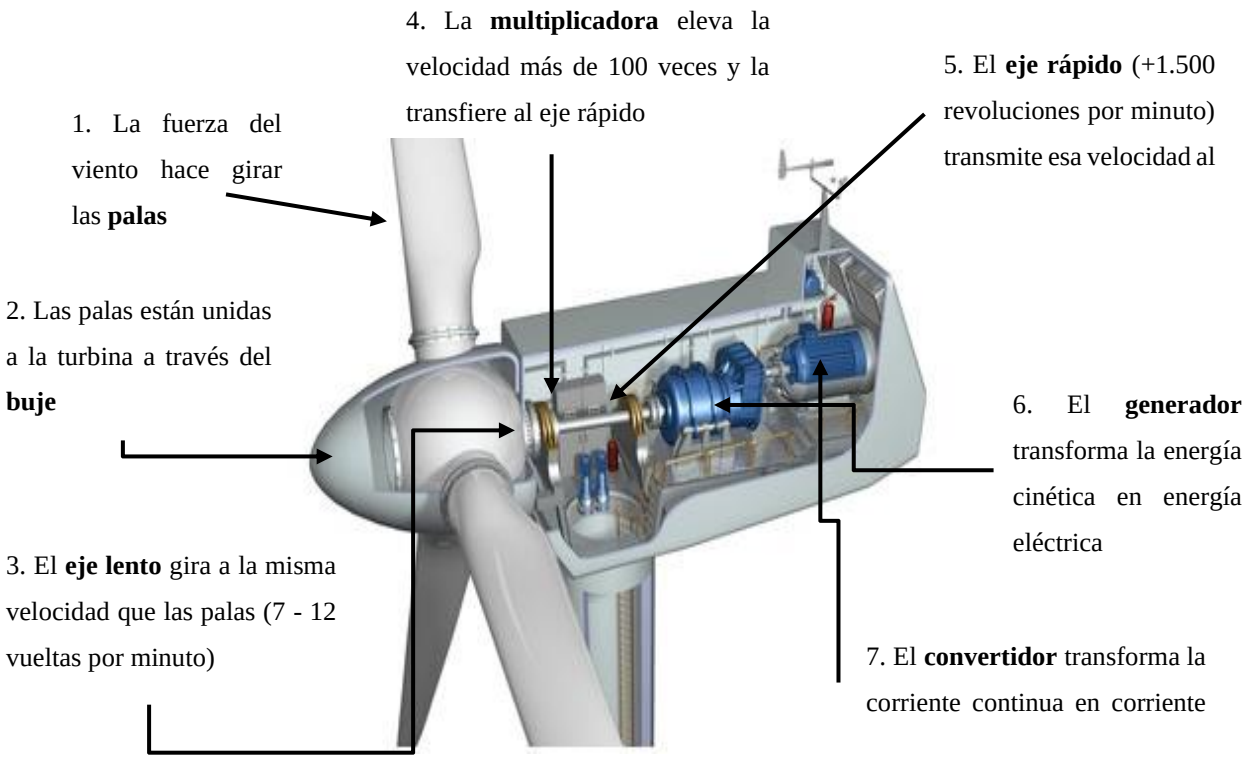

Ilustración 7: Esquema aerogenerador. Fuente: Elaboración Propia.

Una vez fuera del aerogenerador, podemos destacar los siguientes procesos:

8. El transformador eleva la tensión (20 – 66 kV) para poder transportar la corriente por el parque.

9. La energía se transmite mediante cables de media tensión hasta la subestación.

10. En la subestación, la energía se convierte en corriente de alto voltaje (+132 kV)

11. La línea de evacuación transfiere la electricidad hasta las instalaciones conectadas a la red de distribución.

12. La red de distribución transporta la electricidad hasta los hogares. (Eólico, 2019)

4.3.2 ALTURA DE MONTAJE

Por altura de montaje se entiende como la altura del buje desde el suelo. Para dicho montaje es aconsejable tomar una altura de buje mínima de 10 metros, contando desde la altura de desplazamiento. La altura de desplazamiento se toma en cuenta siempre y cuando el aerogenerador está montado dentro de un área de vegetación específica y suele coincidir con la mitad de la altura media de la vegetación circundante excepto si se trata de vegetación muy densa y poco porosa.

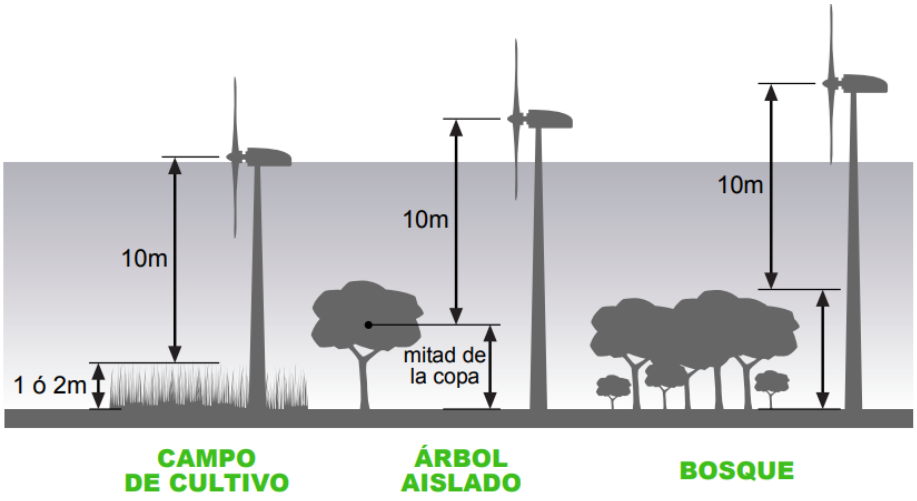

Ilustración 8: Altura de montaje. Fuente: AAE

4.3.3 EMPLAZAMIENTO

Para obtener el máximo rendimiento del aerogenerador, y prolongar también su vida útil, el emplazamiento debe estar bien expuesto al viento y contar con un bajo grado de turbulencias (poca rugosidad).

Se ha demostrado que es poco aconsejable los emplazamientos urbanos (muy rugosos) excepto en edificios altos o zonas periurbanas. En cuanto a la alineación de varios aerogeneradores, es preferible agruparlos en una hilera perpendicular a la dirección principal del viento.

4.3.4 INSTALACIÓN

Los parques eólicos se instalan normalmente en **áreas rurales despobladas,** aisladas de los núcleos de población. A la hora de elegir la ubicación de un parque eólico terrestre, hay que considerar varias cuestiones:

- **Impacto ambiental**: La ubicación de un parque eólico terrestre debe considerar cuidadosamente su impacto en el entorno natural. Esto incluye evaluar cómo afectará a la fauna, la flora, los ecosistemas locales y la calidad del aire y el agua.
- **Potencial energético de la zona**: La elección del emplazamiento debe basarse en el potencial de generación de energía eólica. Se analiza la velocidad y dirección del viento en la zona para determinar cuánta energía se puede producir. (Eólico, 2019)
- **Variación espacial, temporal y vertical del viento**: El viento no es uniforme en todas las áreas ni en todos los momentos. Se deben estudiar las variaciones a lo largo del año, en diferentes alturas y en distintas ubicaciones dentro del parque.
- **Condiciones geológicas y geotécnicas**: La estabilidad del suelo y la capacidad de soporte son cruciales para la construcción de las cimentaciones de los aerogeneradores. (Eólico, 2019)
- **Viabilidad ambiental, legal y territorial**: Además de los aspectos técnicos, se deben considerar los permisos legales y la viabilidad económica. Esto implica evaluar las restricciones normativas, la propiedad de la tierra y la aceptación social.

4.3.5 VENTAJAS

En primer lugar, los aerogeneradores producen energía limpia y segura a partir del viento, una fuente inagotable. Además, al utilizar esta energía, se reduce el consumo de combustibles fósiles, lo que contribuye significativamente a la lucha contra el cambio climático y promueve la transición hacia una matriz energética más sostenible.

Otro punto positivo es que los aerogeneradores apenas generan residuos y no emiten gases tóxicos ni radiaciones. Además, al ser instalaciones móviles, el área en la que se encuentran puede recuperarse una vez que se desmantelan, lo que minimiza su impacto ambiental.

En cuanto a los costes de mantenimiento, los aerogeneradores son una opción económica, ya que requieren poco mantenimiento a lo largo de su vida útil. Además, las instalaciones eólicas no interrumpen las actividades agrícolas y ganaderas que se desarrollan alrededor de los parques, lo que favorece la coexistencia con otras actividades humanas.

Por último, es importante destacar que la energía eólica también genera puestos de trabajo en la fabricación, instalación y mantenimiento de los aerogeneradores (Iberdrola, 2023)

4.3.6 TIPOS

- Parque eólico on-shore: Son los más comunes en la actualidad. Se sitúan en tierra a no menos de 3 kilómetros de la costa y se alimentan de las corrientes de aire terrestre.
- Parque eólico offshore: Estas estructuras se construyen en mar abierto a varias millas de la costa. Entre sus principales beneficios frente a las instalaciones terrestres está el que la fuerza del viento es superior, a menor altura.
- Parque eólico near-shore: También se ubican en tierra, pero a menos de 3 kilómetros de la costa. La ventaja de optar por esta localización es que puede aprovechar tanto los vientos terrestres como marinos para producir energía.

4.4 CIBERSEGURIDAD

4.4.1 QUÉ ES

Se le llama ciberataque a cualquier esfuerzo o propósito intencionado para robar, dañar o exponer datos de aplicaciones u otros activos a la red, sistema informático o dispositivo legal, de manera no autorizada.

Lo que propulsa el desarrollo de los ciberataques, es decir, el motivo de sus amenazas, llegan desde pequeños robos hasta actos de guerra. Se utilizan diversas tácticas y movimientos, como ataques de malware, estafas de ingeniería e incluso robos de contraseñas para poder adquirir un acceso no autorizado a los sistemas de destino.

El daño que puede causar un ciberataque es alarmante, ya que estos pueden llegar a interrumpir, dañar e incluso destruir negocios. El coste medio de una filtración de datos puede suponer un coste de 4,35 millones de dólares, como veremos después. Dicha cantidad, responde a los costes de descubrir y responder a la violación, el tiempo de inactividad y la pérdida de ingresos. Además, hay que tener en cuenta el daño a la reputación a largo plazo no solo de la empresa, pero también de la marca.

Sin embargo, no todas las amenazas de ciberataques oscilan entorno a la misma cantidad que he mencionado anteriormente. Los ataques de "ransomware" (que describiré a continuación en los próximos capítulos) han supuesto el pago de un rescate de hasta 40 millones de dólares. (Sophos, 2021)

Estafas de compromiso de correo electrónico empresarial, han llegado a robar hasta 47 millones de dólares a las víctimas en un solo ataque. Esto tiene grandes repercusiones, ya que, los ciberataques comprometen la información de identificación (PII) de los clientes pueden provocar la pérdida de la confianza de los clientes, multas reglamentarias e incluso accidentes legales. (Dir&ge, 2022)

4.4.2 RECORRIDO HISTÓRICO

- El primer ciberataque registrado fue ***"Melissa"*** (1999)

Este malware fue el primero que se difundió por correo electrónico. Sucedió en Estados Unidos y causó 80 millones de dólares de pérdidas en empresas.

- Uno de los ciberataques más caros de la historia fue "***MyDoom"*** (2004)

El nombre de este ciberataque se debe a que es el malware que ha causado un mayor número de pérdidas económicas en toda la historia de los ataques registrados. Se estima que los daños ascendieron a más de 38.000 millones de dólares. (mrHoutson, 2021)

MyDoom se propagaba inutilizando las herramientas de seguridad de Windows, moviéndose con total independencia y sin supervisión por el sistema operativo. Creaba aperturas de red permitiendo acceder a otros y pudiendo abrir programas de manera aleatoria.

- El siguiente ciberataque muy conocido fue "***Mirai"***, una red que casi acaba con internet (2016)

Mirai consistió en un ataque DDoS (denegación de servicios) mediante la creación de una red botnet. Una botnet es una red de equipos informáticos que han sido infectados con un software malicioso que permite su control remoto. (mrHoutson, 2021)

Esta red de bots fue la más grande de la historia, se formó a partir de la instalación de un malware infectando a dispositivos inteligentes conectados a internet como impresoras, routers, cámaras IP, etc.

Mirai estuvo esperando la orden de los hackers para empezar a propagarse. Cuando la orden fue dada, este ataque fue masivo dejando páginas como Netflix, Spotify o Airbnb inoperativas al ser la responsable de la caída de los servidores DNS del proveedor Dyn.

- Otro ciberataque fue ***WannaCry***, el ataque que marcó un antes y un después en materia de ciberseguridad (2017)

Este ransomware se propagó gracias a una debilidad en el sistema de Microsoft.

Esta debilidad había sido resuelta por la Agencia de Seguridad Nacional de EE.UU. creando un parche de seguridad. Este parche se creó 2 meses antes, pero se llegó a propagar debido a que muchas personas no actualizaron el software. (mrHoutson, 2021)

Wannacry se propagó por todo el mundo afectando en España a Telefónica y también a varios hospitales. Se paralizaron sistemas informáticos de 150 países y provocó pérdidas de más de 4.000 millones de dólares. Debido a este ataque se empezaron a tomar medidas preventivas y a realizar planes de concienciación sobre la ciberseguridad. (mrHoutson, 2021)

- Uno de los más recientes fue ***SolarWinds***, el ataque que afectó a la cadena de valor (2020)

La estrategia que desarrolló fue que si atacaba a los proveedores afectaba indirectamente a todos sus clientes. Esta fue la estrategia que pensaron los ciberdelincuentes en el ataque más grande de nuestra historia reciente. SolarWinds disponía de un software CRM llamado

Orión. Este software era utilizado por grandes empresas de EE.UU., organizaciones gubernamentales como la NASA o el Pentágono aparte de muchas empresas a lo largo del mundo.

Esto provocó que el gobierno de EE.UU. tuviera que intervenir. Uno de los posibles motivos fue que un becario tenía una contraseña muy sencilla (solarwinds123), y además esa contraseña estuvo públicamente expuesta en un repositorio de GitHub. Este ataque se le atribuye a Rusia, país que se presupone que tiene a un "ejército" de hackers contratados para realizar ciberataques. (mrHoutson, 2021)

4.4.3 MOTIVACIÓN

No podemos describir con seguridad cual es la motivación de cualquier cabeza pensante detrás de los ciberataques. Sin embargo, sí que las podemos distinguir en 3 categorías: criminal, política y personal.

Los atacantes **con motivaciones delictivas** buscan obtener ganancias financieras mediante el robo de dinero, el robo de datos o la interrupción del negocio. Los ciberdelincuentes pueden piratear una cuenta bancaria para robar dinero directamente o utilizar estafas de ingeniería social para engañar a las personas para que les envíen dinero. Los piratas informáticos pueden robar datos y utilizarlos para cometer robos de identidad o venderlos en la Dark Web o guardarlos para un rescate.

Los agresores **con motivaciones personales**, como los empleados actuales o antiguos descontentos, buscan principalmente la retribución por algún desaire percibido. Pueden tomar dinero, robar datos confidenciales o interrumpir los sistemas de una empresa.

Hay también amenazas cuya motivación es política. Es decir, lo podemos llamar también ciberterrorismo o el "hacktivismo". En la guerra cibernética los actores de dichas amenazas suelen atacar las agencias gubernamentales o las infraestructuras críticas de sus enemigos.

Los atacantes **con motivaciones políticas** suelen asociarse con la guerra cibernética, el ciberterrorismo o el "hacktivismo". En la ciberguerra, los actores de los estados-nación suelen atacar las agencias gubernamentales o la infraestructura crítica de sus enemigos.

Por ejemplo, desde el inicio de la Guerra de Rusia y Ucrania, ambos países han experimentado una gran cantidad de ciberataque hacia sus enemigos. Los piratas informáticos activistas, llamados "hacktivistas", pueden no causar grandes daños a sus objetivos. En cambio, suelen buscar atención por sus causas dando a conocer sus ataques al público.

Sin embrago, contamos también con que hay algunos hackers simplemente piratean por diversión, saboreando el desafío intelectual.

4.4.4 TIPOS

Los ciberdelincuentes utilizan muchas herramientas y técnicas sofisticadas para lanzar ataques cibernéticos contra sistemas de TI empresariales, computadoras personales y otros objetivos.

Algunos de los tipos más comunes de ciberataques son:

- **Programa malicioso (malware):**

El malware es un software malicioso que puede hacer que los sistemas infectados no funcionen. Los programas maliciosos pueden destruir datos, robar información o incluso borrar archivos críticos para la capacidad de ejecución del sistema operativo (IBM, 2024)

El malware se presenta en muchas formas, incluidas:

- Los caballos de Troya se disfrazan de programas útiles o se esconden dentro de software legítimo para engañar a los usuarios para que los instalen.
- El ransomware: Malware sofisticado que utiliza un cifrado sólido para mantener como rehenes los datos o los sistemas. Los ciberdelincuentes exigen el pago a cambio de liberar el sistema y restaurar la funcionalidad. Se considera el ransomware como el segundo tipo más común de ciberataque y representa el 17% de los ataques.
- Scareware: Utiliza mensajes falsos para atascar a las víctimas a descargar malware o pasar información confidencial a un estafador.

- Spyware: Un tipo de malware que recopila secretamente información confidencial, como nombres de usuario, contraseñas y números de tarjetas de crédito. Luego envía esta información al hacker.
- Rootkits: Paquetes de malware que permiten a los piratas informáticos obtener acceso de nivel de administrador al sistema operativo de una computadora u otros activos.
- Gusanos: Códigos maliciosos autorreplicantes que pueden propagarse automáticamente entre aplicaciones y dispositivos. (INCIBE, 2020)

- **Ingeniería Social**

Los ataques de ingeniería social manipulan a las personas para que hagan cosas que no deberían hacer, como compartir información que no deberían compartir, descargar software que no deberían descargar o enviar dinero a los delincuentes.

El Phishing es uno de los ataques de ingeniería social más generalizados. Es la segunda causa más común de infracciones.

Los mensajes de phishing suelen estar diseñados para verse como si fueran de una fuente legítima. Normalmente dirigen a la víctima a hacer clic en un hipervínculo que los lleva a un sitio web malicioso o abre un archivo adjunto de correo electrónico que resulta ser malware. (IBM, 2024)

- **Ataques de denegación de servicios**

Los ataques de denegación de servicio (DoS) y denegación de servicio distribuido (DDoS), inundan los recursos de un sistema con tráfico fraudulento.

Este tráfico abrumará al sistema, evitando las respuestas a solicitudes legítimas y reduciendo la capacidad del sistema de realizar. Un ataque de denegación de servicio puede ser un fin en sí mismo o una configuración para otro ataque. (Centeno, 2015)

La diferencia entre los ataques DoS y los ataques DDoS es simplemente que los ataques DoS utilizan una única fuente para generar tráfico fraudulento, mientras que los ataques DDoS utilizan múltiples fuentes.

Los ataques DoS suelen llevarse a cabo con una botnet, una red de dispositivos conectados a Internet e infectados con malware bajo el control de un hacker. Las redes de bots pueden incluir portátiles, smartphones y dispositivos de Internet de las cosas (IoT). Las víctimas a menudo no saben cuándo una botnet ha secuestrado sus dispositivos (IBM, 2024).

- **Compromiso de cuenta**

Llamamos compromiso de cuenta, a cualquier ataque en el que los piratas informáticos secuestran la cuenta de un usuario legítimo para realizar actividades maliciosas.

Los ciberdelincuentes pueden entrar en la cuenta de un usuario de muchas maneras. Pueden robar credenciales a través de ataques de phishing o comprar bases de datos de contraseñas robadas de la web oscura. (IBM, 2024)

- **Ataques de intermediario**

En un ataque de intermediario (MiTM), también llamado "escuchas no autorizadas", un hacker intercepta en secreto las comunicaciones entre dos personas o entre un usuario y un servidor.

Los ataques MitM se llevan a cabo comúnmente a través de redes wifi públicas no seguras, donde es relativamente fácil para los actores de amenazas espiar el tráfico.

Los piratas informáticos pueden leer los correos electrónicos de un usuario o incluso alterarlos en secreto antes de que lleguen al destinatario.

En un ataque de **secuestro de sesiones**, el hacker interrumpe la conexión entre un usuario y un servidor que aloja activos importantes, intercambia su dirección IP con la del usuario, haciendo que el servidor piense que es un usuario legítimo conectado a una sesión legítima. (IBM, 2024)

- **Ataques a la cadena de suministro**

Los ataques a la cadena de suministro son ataques cibernéticos en los que los hackers infringen una empresa dirigiéndose a sus proveedores de software, proveedores de materiales y otros proveedores de servicios.

Un ejemplo de esto es que, en 2020, los actores estatales rusos piratearon al proveedor de software SolarWinds mencionado anteriormente. (IBM, 2024)

4.4.5 PREVENCIÓN

Muchas organizaciones implementan una estrategia para la gestión de amenazas, para identificar y proteger sus activos y recursos más importantes. La gestión de amenazas puede incluir políticas y soluciones de seguridad como:

- Las plataformas políticas d**e gestión de identidades y accesos (IAM)**, incluido el acceso con privilegios mínimos, la autenticación multifactorial y políticas de contraseñas seguras, pueden ayudar a garantizar que solo las personas adecuadas tengan acceso a los recursos adecuados.
- Las empresas también pueden exigir que los empleados remotos utilicen redes privadas virtuales (VPN) cuando accedan a recursos confidenciales a través de wifi no seguro.
- **Una plataforma integral de seguridad de datos y herramientas de prevención de pérdida de datos (DLP)** pueden cifrar datos confidenciales, monitorizar su acceso y uso, y generar alertas cuando se detecta actividad sospechosa.
- **Los cortafuegos** pueden ayudar a impedir que los actores de amenazas ingresen a la red en primer lugar. Los cortafuegos también pueden bloquear el tráfico malicioso que sale de la red, como el malware que intenta comunicarse con un servidor de comando y control.
- **La capacitación en concientización sobre seguridad** puede ayudar a los usuarios a identificar y evitar algunos de los vectores de ciberataque más comunes, como el phishing y otros ataques de ingeniería social. (IBM, 2024)

- Las políticas de gestión de vulnerabilidades, incluidas las programaciones de gestión de parches y las pruebas de penetración regulares, pueden ayudar a detectar y cerrar vulnerabilidades antes de que los piratas informáticos puedan aprovecharlas.

4.5 SECTOR ENERGÉTICO Y LOS CIBERATAQUES

Se considera extraña toda aquella actividad que provea cualquier servicio en la que no esté involucrada la presencia de la energía eléctrica o las tecnologías de la información y la comunicación (TIC).

Podríamos confirmar que estos dos sectores se ven claramente interrelacionados en el desarrollo de las Smart grids[1], que suponen la conexión de estos dos dominios separados y distintos. Tanto el sector energético como el de las TIC son vitales, ya que la sociedad actual para su sostenimiento, bienestar y desarrollo precisa cubrir necesidades como la alimentación, la salud, la educación o la justicia y otras más elaboradas.

Las infraestructuras que dan soporte a estos servicios son amplias y complejas, en muchas ocasiones con dependencias entre sí, y la caída de una puede provocar un gran impacto en otras e incluso una caída en cascada bien en las mismas o en la degradación de los servicios que prestan. (Martínez et al., 2020)

Teniendo en cuenta lo expuesto anteriormente, los Estados tienen la responsabilidad de proteger las infraestructuras que proveen de los servicios esenciales a sus ciudadanos, conocidas como Infraestructuras Críticas (IC).

La integración de la nueva infraestructura cibernética con la infraestructura eléctrica tradicional abre un nuevo abanico de posibilidades, pero a la vez aparecen una serie de problemáticas en materia de seguridad. Los ciberataques en las smart grids tienen consecuencias que abarcan desde grandes pérdidas económicas hasta el propio bienestar social e integridad física de los habitantes de un país.

Además, es importante destacar que, en las nuevas redes eléctricas inteligentes, el robo de la información intercambiada entre los diferentes dispositivos puede dar lugar a problemas de seguridad para los clientes, ya que la información substraída está clasificada como sensible. (Alonso et. al., 2020)

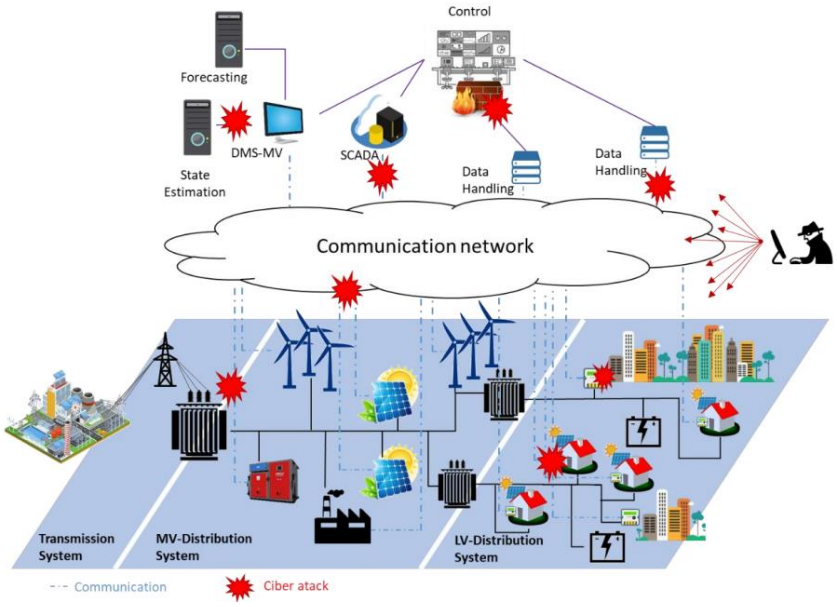

Ilustración 9: Conexión ciber-física sistema energético. Fuente Retos SmartGrids

En el campo de la operación de las Smartgrids, el National Electric Sector Cybersecurity Organization Resource[2] establece los principales escenarios de fallo en función de 6 niveles funcionales a los que pueda ser dirigido el ciberataque:

[1]Smart Grids: Redes de distribución eléctrica inteligentes

[2]El **National Electric Sector Cybersecurity Organization Resource (NESCOR)** tiene como objetivo fortalecer la postura de ciberseguridad del sector eléctrico mediante una asociación público-privada con el Departamento de Energía.

i. La infraestructura de medida

ii. Los recursos energéticos distribuidos: Nos referimos a fuentes de energía descentralizadas, como paneles solares o turbinas eólicas conectadas a la red eléctrica.

iii. Los sistemas de monitorización, protección y control: Estos sistemas tienen como función supervisar y controlar la operación de la red eléctrica, asegurando su estabilidad y confiabilidad.

iv. El transporte eléctrico: Aquí se consideran los componentes de transmisión de alta tensión que transportan la electricidad desde las plantas generadoras hasta las subestaciones.

v. La gestión de la demanda: Trata de involucrar estrategias para equilibrar la oferta y la demanda de electricidad, como la gestión de cargas y la respuesta a la demanda.

vi. Los sistemas encargados de la gestión de las redes eléctricas de distribución: Estos sistemas administran la distribución de electricidad a los usuarios finales, como hogares y empresas. (Alonso et. al, 2020)

4.5.1 CIBERATAQUES EN INFRAESTRUCTURAS CRÍTICAS

"BlackEnergy" en 2015, que afectó a una planta de energía eléctrica de Ucrania, un año después, el 17 de diciembre de 2016, otro ciberataque dejó sin luz durante una hora a unas 2.9 millones de personas. (INCIBE, 2024)

Más reciente en el tiempo, en plena pandemia y auge del ransomware, la compañía de oleoducto norteamericana, Colonial Pipeline, responsable del suministro combustible a gran parte de la población, era víctima de un ataque del ransomware DarkSide que forzaba la interrupción de sus sistemas y el corte de suministro.

Esto provocó largas filas en las estaciones de servicio y sembró el pánico ante la posibilidad de no tener combustible. Incluso provocó un aumento del precio del combustible en las zonas afectada.

Además de los ataques a sectores como el de la salud, el energético o el de servicios financieros, los cibercriminales no temen en hasta incluso afectar los sistemas críticos de agua y saneamiento.

En febrero de 2021, se pudo frenar un intento de lo que podría haber sido un episodio muy trágico, atacantes accedieron a los sistemas de una planta de tratamiento de agua en una ciudad de Florida, en Estados Unidos, y modificaron los niveles químicos de hidróxido de sodio. Al parecer, los cibercriminales lograron acceso a través del software de gestión remota Team Viewer. (INCIBE, 2024)

Capítulo 5. SIMULACIÓN "CORTIJO DE IRUELAS"

El objetivo de mi trabajo de Fin de Grado es integrar la ciberseguridad en la nueva reforma que se va a realizar en el parque eólico de Tarifa. Dicha reforma consiste en la reducción del número de aerogeneradores y el aumento de la energía generada a su vez. De esta manera se llevaría a cabo una reducción de gastos y el alcance a los hogares de las distintas provincias andaluzas se extendería.

Primero, voy a comenzar por explicar la situación actual en la provincia de Andalucía con mayor número de parques eólicos, Cádiz.

El viento allí, toma cierta personalidad propia. Este es un **recurso natural al que se le saca especial partido en Cádiz, debido a su situación geográfica, para generar energía** de una manera más limpia para el medio ambiente.

No es de extrañar, que los molinos que se extienden por toda la provincia forman ya parte de su paisaje, aunque no siempre estuvieron ahí. La **alta presencia de estos gigantes con aspas no es casualidad en una zona donde el viento sopla**, con más o menos intensidad, todas las semanas. El movimiento de las aspas causado por la fuerza del viento hace que los aerogeneradores produzcan electricidad (DiariodeCádiz, 2023)

Los parques eólicos en Cádiz lideran la producción de energía eólica en Andalucía. La provincia produjo el 39,5% de la energía eólica andaluza en 2022. Hasta 71 parques eólicos conectados a red en funcionamiento en suelo gaditano, siendo Tarifa la localidad con más instalaciones, un total de 32.

PARQUE EÓLICO	MUNICIPIO	POTENCIA INSTALADA (MW)
Loma de Lázaro	Alcalá de los Gazules	16
Viento de Alcalá	Alcalá de los Gazules	42
Buenavista	Barbate	7,8
La Victoria	Chiclana de la Frontera	24
Alijar	Jerez de la Frontera	24
Bolaños	Jerez de la Frontera	24
Chorreaderos Bajos	Jerez de la Frontera	30
Doña Benita Cuellar	Jerez de la Frontera	32
El Olivillo	Jerez de la Frontera	25,5
Jerez	Jerez de la Frontera	46,2
La Rabia	Jerez de la Frontera	21,71
Los Isletes	Jerez de la Frontera	10
Roalabota	Jerez de la Frontera	28,5
El Pino	Los Barrios	21
El Pino	Los Barrios	12
Almeriques	Medina-Sidonia	24
Almeriques	Medina-Sidonia	1,72
El Venzo	Medina-Sidonia	8
Las Monjas	Medina-Sidonia	12,6
Las Monjas	Medina-Sidonia	12
Las Monjas	Medina-Sidonia	1,4
Las Monjas Fase II	Medina-Sidonia	8
Las Vegas	Medina-Sidonia	23
Los Alburejos	Medina-Sidonia	10
Rancho Viejo	Medina-Sidonia	14,4
Zorreras	Medina-Sidonia	38
Cortijo de Guerra I	Puerto Real	51
Cortijo de Guerra I Ampliación	Puerto Real	1,2
Cortijo de Guerra II	Puerto Real	28
La Castellana	Puerto Real	34
La Castellana	Puerto Real	12
Chorreaderos Altos	San José del Valle y Jerez de la Frontera	22
Los Isletes	San José del Valle y Jerez de la Frontera	25,3

Almendarache	Tarifa	22
Aviadores	Tarifa	6
Cortijo de Iruelas (Sin repotenciar)	Tarifa	13,6
Eee (Repotenciado)	Tarifa	32
El Bancal	Tarifa	20
El Cabrito / La Locustura	Tarifa	1,65
El Gallego	Tarifa	24
El Pandero	Tarifa	20
El Ruedo	Tarifa	16
Hinojal I	Tarifa	12
Hinojal I	Tarifa	1,8
Hinojal II	Tarifa	5,4
Hinojal II	Tarifa	1,8
Kw Tarifa (El Cabrito)	Tarifa	36,9
La Herrería	Tarifa	46,76
La Joya (PEESA)	Tarifa	6
La Manga	Tarifa	12
La Risa	Tarifa	12
La Tahuna	Tarifa	20
La Torre I	Tarifa	16
Las Zorreras	Tarifa	20
Levantera	Tarifa	0,5
Levantera	Tarifa	0,15
Loma de Almendarache	Tarifa	12
Los Lances	Tarifa	5,4
Los Lances	Tarifa	5,28
Los Siglos	Tarifa	20
Monteahumada I	Tarifa	1,3
Monteahumada I	Tarifa	0,8
Monteahumada I	Tarifa	0,33
Pasada de Tejeda	Tarifa	10,02
Pedregoso A	Tarifa	16,2
Pedregoso B	Tarifa	16,2
Pedregoso D	Tarifa	16,2
Pesur (Repotenciado)	Tarifa	42
Prototipo Desa Hinojal/Tahivilla	Tarifa	0,6
Prototipo Ecotécnia	Tarifa	0,5

Prototipo Ecotècnia	Tarifa	0,6
Puerto Facinas	Tarifa	12
Río Almodóvar	Tarifa	12,8
Tahivilla	Tarifa	30
Tarifa II	Tarifa	0,15
Tarifa III	Tarifa	0,2
Zarzuela II	Tarifa	10,8
Zarzuela II	Tarifa	4
Cerro Conilete	Vejer de la Frontera	9
Loma del Suyal (Fase A)	Vejer de la Frontera	6
Loma del Suyal (Fase B)	Vejer de la Frontera	3
Lomas de las Peñuelas	Vejer de la Frontera	9
Los Granujales	Vejer de la Frontera	24
Mostaza	Vejer de la Frontera	18
Tejonero	Vejer de la Frontera	32
Total Provincia de Cadiz		**1356,27**

Tabla 1: Parques eólicos conectados a Red en Cádiz. Fuente: AAE

5.1 ENERGÍA EÓLICA EN ANDALUCÍA

La energía eólica, como he explicado anteriormente, es la energía obtenida del viento. Es considerado como uno de los recursos energéticos más antiguos explotados por el ser humano, y hoy en día está valorada como la energía más madura y eficiente de todas las energías renovables. La energía eólica trata de convertir la energía que produce el movimiento de las palas de un aerogenerador impulsadas por el viento en energía eléctrica.

Los parques eólicos emplean aerogeneradores con una altura total de unos 120 metros aproximada y principalmente, son instalados en tierra firme, aunque también pueden situarse en el mar *(off-shoring)*, proyecto que se llegó a estudiar para la capital de Cádiz, pero que, finalmente ha sido descartado. (DiariodeCádiz, 2023)

Las potencias de los aerogeneradores han experimentado un cambio importante en las últimas décadas, pasando de potencias de alrededor de 100 kW en la década de los 80, a los 2MW.

Según datos de la Junta de Andalucía, a finales del año 2022 había 158 parques eólicos, con un total de **3.535,2 MW** instalados, aunque Cádiz es la gran productora de energía eólica en Andalucía.

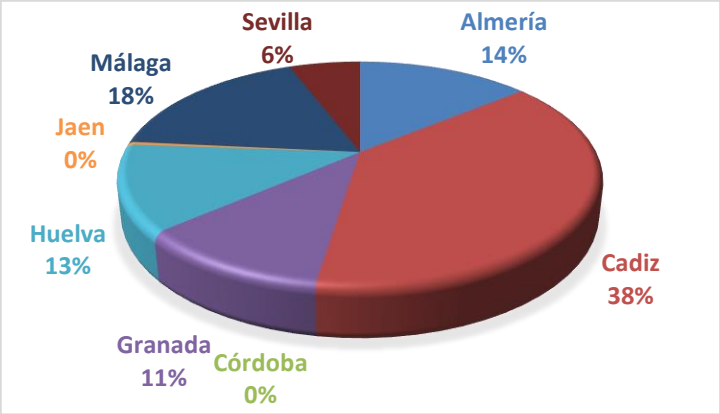

Ilustración 10: Energía Eólica Andalucía. Fuente: Elaboración propia

En la comunidad autónoma andaluza existen 158 parques eólicos con un total de 3.535,2 MW instalados, de los cuáles Cádiz produce 1.395,97 MW lo que se traduce en el 39,5% del total, según datos de la Junta de Andalucía. (DiariodeCádiz, 2023)

Podemos observar que la producción en los parques eólicos gaditanos es más del doble que en cualquier otra provincia andaluza.

Málaga es la segunda de este ranking con una potencia instalada de 643 MW en sus instalaciones, una cifra bastante inferior a la de Cádiz.

Con 511,30 MW Almería cierra el podium.

Le siguen el Huelva (427,31 MW), Granada (407,21 MW), Sevilla (135,50 MW) y Jaen (15,18 MW), ya que de Córdoba la Junta de Andalucía no aporta datos, es una provincia que en el año 2009 llegó a ser la única sin producir energía eólica en Andalucía.

La potencia eléctrica instalada en Cádiz está basada hoy en día en las tecnologías no renovables: los ciclos combinados de Algeciras, Campo de Gibraltar y Arcos de la Frontera, la central de carbón de Los Barrios, que está pendiente de su cierre, pero entre las energías renovables, la eólica supuso en 2022 el 63% de la potencia eléctrica renovable en la provincia gaditana, que se cifra en 2.207,42 MW, ahora a cierre de 2023 se ha contabilizado una potencia de **3.535,2 MW.** (DiariodeCádiz, 2023)

La producción de energía eólica (1.395,97 MW) en Cádiz supera la producción de energía fotovoltaica (699,94 MW) o Termosolar (100,00 MW).

Dentro de la provincia gaditana, nos encontramos con que en Tarifa se encuentra el parque eólico de mayor producción en todo el territorio, se trata del parque de Herrería con 44,80 MW instalados, seguido del parque eólico Jerez (42,50 MW) en Jerez de la Frontera. Seasa Pesar (42 MW) completa el top 3. Jerez con 12 instalaciones y Vejer con 7 son las otras dos localidades con más parques eólicos en sus territorios.

Sin embargo, nuestro enfoque se hará en el parque eólico: Tahivilla, Tarifa.

Tarifa, municipio situado al sur de Cádiz entre Vejer de la Frontera y Algeciras, tiene una extensión de 419 km^2 y 18.085 habitantes, dando lugar a una densidad de población de 42,26 hab/km^2. (DiariodeCádiz, 2023)

Tahivilla y Facinas forman los dos grandes núcleos de población de la zona. Se trata de un terreno poco accidentado, con una orografía prácticamente llana y al nivel del mar.

Hasta cinco ríos atraviesan Tarifa, desembocando cuatro de ellos en el mar del Estrecho. En cuanto a comunicación terrestre hay que destacar la carretera del Mediterráneo 340 (N-340), la más larga del territorio español. Recorre toda la costa del Mediterráneo uniendo Cádiz con Barcelona, atravesando también Tahivilla y Facinas

5.2 REFORMA EN TARIFA

La reforma que tendrá lugar en Tarifa en los próximos años será protagonizada por Acciona Energía, ya que se encargará de repotenciar los parques eólicos de Tahivilla (Río Almodóvar, El Gallego, La Manga, El Ruedo y Cortijo de Iruelas). Es considerado una de las zonas de la península **con mejor recurso eólico**. Dicha reforma disminuirá el número de aerogeneradores en los parques eólicos, que pasará de estar formado por 98 aerogeneradores a 13 turbinas Nordex y que prevén entrar en servicio **en 2026**.

La sustitución de los aerogeneradores antiguos por nuevos de última generación comenzará este mismo año y permitirá incrementar la potencia total del parque eólico de **78,4 a 84,4 megavatios**. (Europa Sur, 2024)

La capacidad de evacuación del parque es aquella línea que transfiere la electricidad hasta las instalaciones conectadas a la red de distribución.

La producción del parque eólico de Tahivilla, una vez repotenciado, **aumentará en un 72%**, pasando de generar electricidad limpia cuyo consumo puede llegar a suministrar a 42.000 hogares españoles, a producir la suficiente como para poder cubrir las necesidades energéticas de **73.000 hogares**. (Europa Sur, 2024)

La repotenciación de Tahivilla ha recibido **8,3 millones de euros** de fondos del Plan de Recuperación, Transformación y Resiliencia (PRTR), financiado por la Unión Europea NextGenerationEU, si bien Acciona no ha difundido a cuánto ascenderá la inversión total.

El objetivo del proyecto consiste en la sustitución de las turbinas antiguas por modelos más modernos, potentes y eficientes. Esto pretende optimizar el funcionamiento y aumentar la capacidad de generación de energía.

Acciona destaca las ventajas de repotenciar un parque respecto a la construcción de una instalación totalmente nueva.

Una de ellas es que adquiere **mayor aceptación social** al ubicarse en lugares que ya están acostumbrados a tener renovables.

Otras ventajas son el menor impacto medioambiental, al utilizar **menos aerogeneradores** y reaprovechar las instalaciones existentes; la reducción de los plazos de desarrollo y el aprovechamiento de ubicaciones con buen recurso y los costes y el riesgo de inversión son menores.

En 2030, habrá en España en torno a 20 gigavatios eólicos con más de 20 años en operación, tiempo que coincide con la vida útil media de un parque, según ha destacado la empresa. (El Español, 2024)

De estos 20 gigavatios, en torno a 7,4 tienen posibilidades para de ser repotenciados, lo que multiplicaría la potencia instalada entre 1,5 y 3 veces e incorporaría al sistema eléctrico español entre 4 y 15 gigavatios renovables adicionales (EuropaSur, 2024)

Mi Trabajo de Fin de Grado se va a centrar en el **parque eólico Cortijo de Iruelas**. Este se sitúa en el término municipal de Tarifa en la provincia de Cádiz, Andalucía.

La poligonal se enmarca en la hoja número 1077 del Mapa Topográfico Nacional (MTN) a escala 1:25.000 del Instituto Geográfico Nacional (IGN).

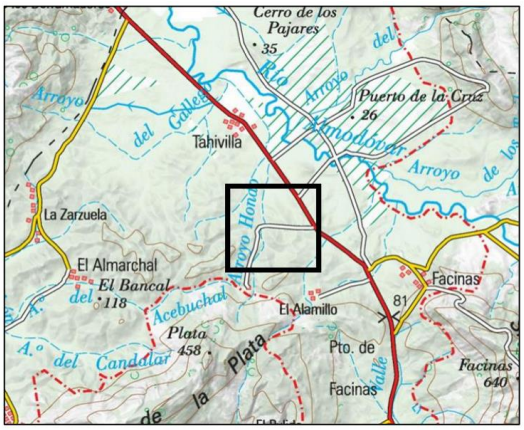

Ilustración 11: Localización Cortijo de Iruelas. Fuente: Acciona

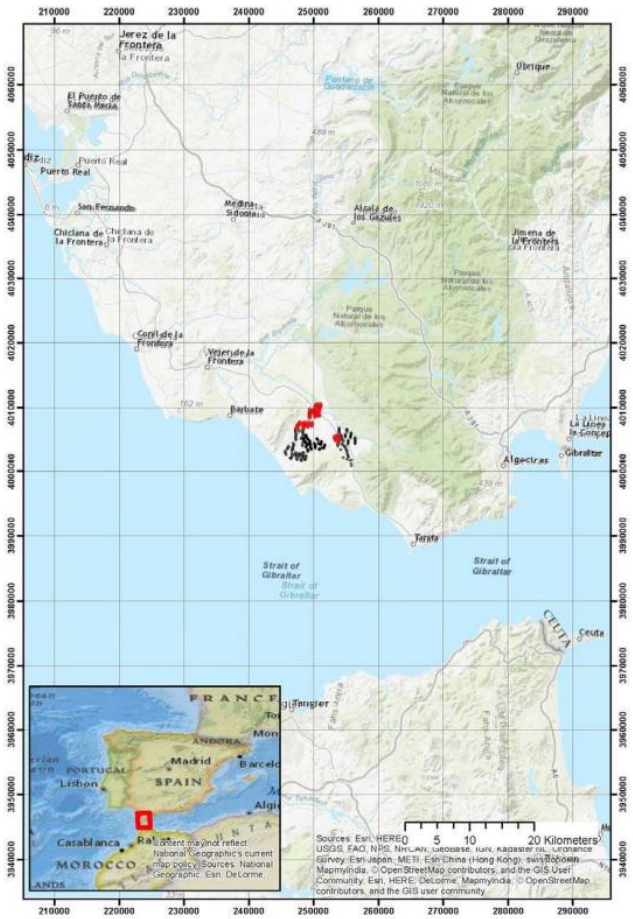

Ilustración 12: Ubicación del emplazamiento. Fuente: Acciona

5.2.1 EMPLAZAMIENTO

Como hemos descrito anteriormente, llamamos energía eólica a aquella que se genera al transformar el flujo de aire en energía eléctrica. Para aprovechar el viento que se produce en tierra, se construyen parques eólicos, cuya finalidad es ser capaz de extraer el máximo potencial de este recurso.

Para aprovechar y sacar el máximo rendimiento a los parques eólicos, se debe tener en cuenta su posterior construcción en ubicaciones que favorezcan la producción de energía eólica.

La ubicación de los parques eólicos es de gran importancia para la construcción de estos, ya que de nada serviría construir un parque eólico sin su recurso clave, el viento.

Por eso Tarifa es gran protagonista de la construcción de los parques eólicos.

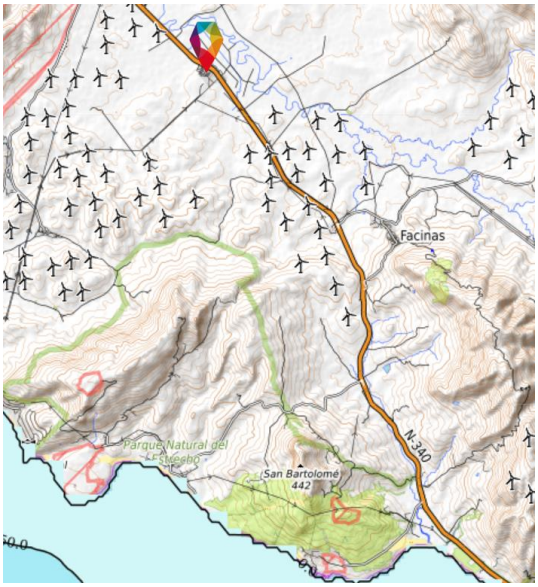

Ilustración 13: Disposición eólica del Cortijo de Iruelas. Fuente: IDEA

Ilustración 14: Disposición nuevos aerogeneradores Nordex 163/6X de 7000 kW. Fuente: Acciona

La Rosa de los Vientos para Tarifa muestra el número de horas al año que el viento sopla en la dirección indicada.

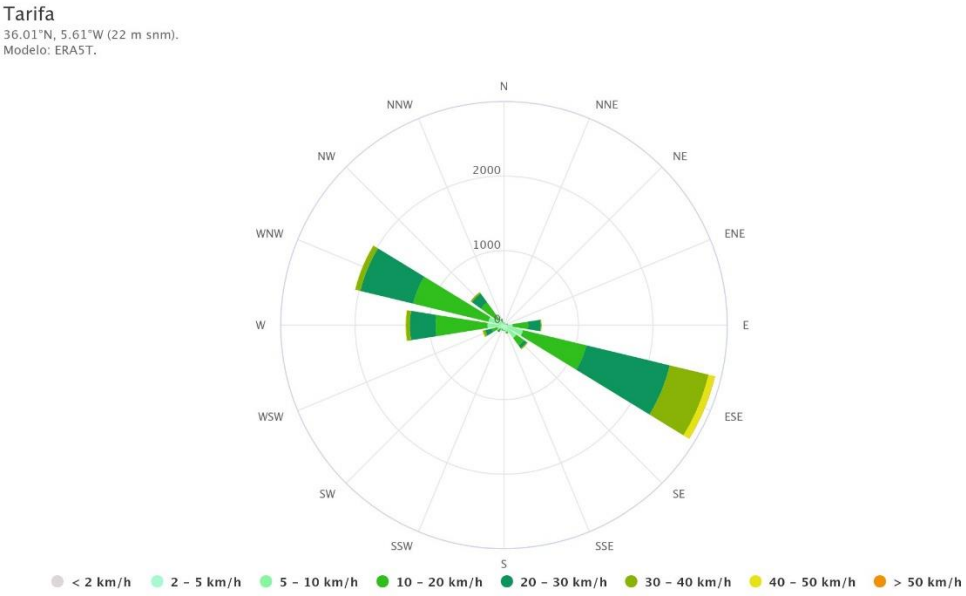

Ilustración 15: Rosa de los Vientos Tarifa. Fuente: Meteoblue

De la ilustración anterior sacamos las siguientes conclusiones: los vientos de mayor intensidad pueden llegar a alcanzar rachas de entre 40km/h y 50km/h en dirección Este-Sureste.

Lo hacen también de manera transversal con rachas de menor magnitud (entre los 30 km/h y 40 km/h) en dirección Oeste-Noroeste.

Las perpendiculares a los círculos concéntricos, mide la cantidad de horas al año en las que el viento sopla en la dirección que se muestra.

Dicho esto, podríamos deducir que en dirección Este-Sureste, el viento sopla con mucha frecuencia la mayor parte del año, llegando a sobrepasar las 2000 horas. En dirección Oeste-Noroeste, consigue alcanzar las 2000 horas y ya en menor frecuencia siguen las rachas de viento en dirección Oeste.

En Tarifa, estas rachas pueden ser especialmente fuertes debido a las condiciones locales, como la topografía y la influencia del viento de levante.

Hay que tener en cuenta el efecto del viento, ya que hay diferentes fenómenos que modifican la velocidad del viento e interfiere en la energía aprovechable por los aerogeneradores.

Uno de ellos es el llamado abrigo del viento. La aparición de un obstáculo en la dirección del viento provoca que su velocidad disminuya. El principal parámetro del que depende esa disminución de la velocidad es la porosidad del obstáculo (no es lo mismo que se trate de un árbol que de un edificio).

Cuanto mayor sea la porosidad, mayor es la velocidad al dejar atrás el obstáculo. El hecho de atravesar la turbina del aerogenerador hace que el viento aumente su turbulencia y pierda energía cinética. Una turbulencia excesiva alrededor de las máquinas puede dañarlas y disminuir su vida útil, por lo que se deben tomar medidas para evitar este efecto.

Además, si hay demasiada proximidad entre los aerogeneradores, se desaprovecha gran parte del potencial eólico debido a la pérdida de energía cinética. Este efecto recibe el nombre de efecto estela. Lo ideal es separarlos lo máximo posible, pero el elevado coste del terreno obliga a adoptar una solución de compromiso (Danish Wind Industry Association, 2003).

Otra opción para situar los aerogeneradores es ubicarlo entre dos montañas, dando lugar al efecto túnel. El viento choca con las dos montañas y se comprime, produciendo una aceleración en el hueco entre las dos. Como ocurre con el efecto colina, hay que tener en cuenta que se trate de una zona poco accidentada para que no aumenten en exceso las vibraciones.

5.2.2 AEROGENERADORES

En 2023, la Corporación Acciona Eólica propuso reemplazar los aerogeneradores antiguos del parque eólico Cortijo de Iruelas por componentes más eficientes. El objetivo era reducir el número de aerogeneradores y minimizar el impacto ambiental del proyecto. Estos fueron los principales motivos por el que nació el proyecto de repotenciación del parque eólico Cortijo de Iruelas. (Acciona, 2024)

El proyecto repotenciación del parque eólico Cortijo de Iruelas parte de la sustitución de los 17 aerogeneradores existentes MADE 56-800, por nuevos modelos de tecnología más moderna y mayor generación, en concreto dos aerogeneradores Nordex modelos 163/6X de 7000 kW de potencia nominal

La lista de aerogeneradores existentes, que serán sustituidos, en el parque eólico Cortijo de Iruelas, son los siguientes:

AERO	MODELO	COORDENADAS SEXAGESIMALES								ALTURA AERO	
		LATITUD				LONGITUD				ALTURA TORRE	ALTURA MÁXIMA (BUJE +
		º	'	''		º	'	''			
1	S-800	36	9	45	N	5	44	36	W	60	88
2	S-800	36	9	41	N	5	44	35	W	60	88
3	S-800	36	9	39	N	5	44	33	W	60	88
4	S-800	36	9	36	N	5	44	31	W	60	88
5	S-800	36	9	33	N	5	44	29	W	60	88
6	S-800	36	9	30	N	5	44	27	W	60	88
7	S-800	36	9	26	N	5	44	26	W	60	88
8	S-800	36	9	31	N	5	44	10	W	60	88
9	S-800	36	9	34	N	5	44	10	W	60	88
10	S-800	36	9	31	N	5	44	10	W	60	88
11	S-800	36	9	34	N	5	44	10	W	60	88
12	S-800	36	9	38	N	5	44	11	W	60	88
13	S-800	36	9	41	N	5	44	12	W	60	88
14	S-800	36	9	44	N	5	44	14	W	60	88
15	S-800	36	9	46	N	5	44	16	W	60	88
16	S-800	36	9	49	N	5	44	18	W	60	88
17	S-800	36	9	52	N	5	44	19	W	60	88

Tabla 2: Disposición aerogeneradores existentes Cortijo de Iruelas. Fuente: Acciona

La lista de aerogeneradores que serán instalados en el parque eólico Cortijo de Iruelas, como parte del proyecto de repotenciación, son los siguientes:

CÓDIGO AEROGENERADOR	MODELO	COORDENADA X (ETRS89.UTM-30N)	COORDENADA Y (ETRS89.UTM-30N)	ALTURA TORRE (m)	DIÁMETRO ROTOR (m)	ALTITUD TERRENO RESPECTO A NIVEL DEL MAR (m)	ALTURA TOTAL DE PALA (m respecto a terreno)
CI1	NORDEX 163/6.X (7000 kW)	253.556	4.005.192	159	163	32	240,5
CI2	NORDEX 163/6.X (7000 kW)	253.690	4.004.881	159	163	53	240,5

Tabla 3: Disposición nuevos aerogeneradores Cortijo de Iruelas. Fuente: Acciona

Aerogenerador *MADE AE-56 Serie 800:*

El aerogenerador AE-56 es producción de Made - Endesa, fabricante de España. Desde el 2003 dicho fabricante ya no está activo. Posteriormente fue adquirido por Gamesa Corporación Tecnológica (Grupo Auxiliar Metalúrgico, SA). Con una velocidad de viento de 3,3 m/s, la turbina eólica comienza a trabajar. El diámetro del rotor es de 56 m, y su área de 2.463 m². El aerogenerador está equipado con 3 palas, y la velocidad máxima que consigue alcanzar el rotor es de 23,8 U/min. El Made - Endesa AE-56 está equipado con una caja de cambios planetaria[3]. La caja de engranajes tiene 2 etapas. (MADE-ENDESA, 2018).

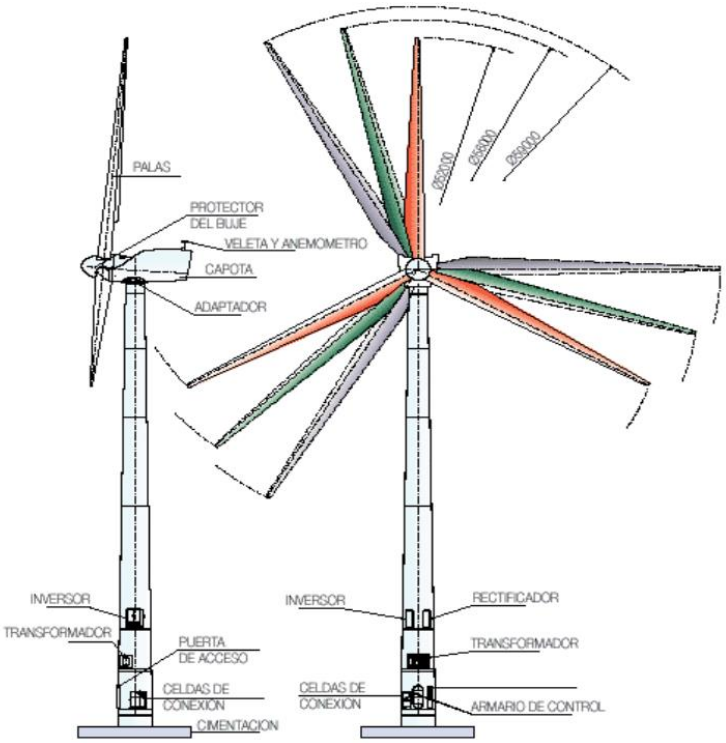

Ilustración 16: MADE Serie 800 AE-56. Fuente: MADE ENDESA

[3]*Planetaria: La caja de cambios planetaria consta de un engranaje solar, engranajes planetarios, una corona y un transportista. Dado que las cajas de engranajes planetarios contienen varios engranajes planetarios, varios dientes engranan simultáneamente durante el funcionamiento. Esta distribución de potencia garantiza una mayor eficiencia que otros tipos de engranajes y, por lo tanto, también permite un mayor par transmisible con un diseño más compacto.*

- Características:

  - Se caracterizan por ser aerogeneradores de paso y velocidad variables 800 kW.
  - Consta de un generador síncrono que aporta alto rendimiento a bajas cargas, capaz de adaptarse a la velocidad del tiempo en todo el rango, y optimiza su producción.
  - Es de paso variable, lo que indica que aporta adaptación al perfil de la pala, y tiene una gran superficie de barrido.
  - Además, conlleva una gran gama de rotores, lo que permite optimizar en todos los regímenes de velocidad del tiempo.
  - Es un solo dispositivo el que controla toda la corriente, ventaja que no produzca averías por falta de sincronismo.
  - El generador no lleva escobillas, lo cual no hace falta mantenimiento.
  - Se puede asegurar una total seguridad de operación, debido a su mano independiente de paso en cada pala.
  - Consta de componentes de última tecnología, lo que permite asegurar fiabilidad a largo plazo. (MADE-ENDESA, 2018)

Aerogenerador *NORDEX 163.6/6.x (7000Kw):*

La turbina, conocida como N163/6.X, se lanzó en septiembre de 2021 como la última actualización de la serie Delta4000 de Nordex. En comparación con su modelo hermano de 5 megavatios, es capaz de producir hasta un 7% más de energía anual gracias a su mayor potencia nominal.

Gracias a su configuración flexible, puede adaptarse a las condiciones específicas de cada proyecto, lo que da lugar a una solución a medida para cada cliente. La vida útil del diseño es de 25 años, con una vida útil ampliada de 35 años disponible para emplazamientos específicos. (Renewable Press, 2021)

Lo que le diferencia del resto del mercado es que es un modelo mucho más silencioso, lo que es considerado una gran ventaja frente al resto de sus competidores.

Ilustración 17: NORDEX 163.6/6.x (7000Kw). Fuente: Nordex SE

- Características:

  - Los aerogeneradores instalados en este parque corresponden al modelo 163/6X y tiene una altura de 159 metros de torre y tres palas que al girar abarcan una circunferencia de 163 metros de diámetro.
  - Los aerogeneradores suministran una potencia de 7000 kW y la energía producida por los aerogeneradores se recoge mediante dos circuitos. El generador DFIG (Generador Doblemente Alimentado) se conecta con el transformador de 7800 kVA, 950/20 kV, del cual se deriva un circuito que alimenta a un transformador para los servicios auxiliares (fuerza, iluminación y control) del aerogenerador.
  - Las palas de los aerogeneradores con longitud de 79,7 m y peso 24.000 Kg. El 163/6.X consta de una multiplicadora, de tipo planetario también. (Renewable Press, 2021)

Dicho cambio en los aerogeneradores del parque eólico del Cortijo de Iruelas propiciará una serie de ventajas:

- En primer lugar, **se dará una reducción de la Dependencia Energética**. La sustitución de los aerogeneradores antiguos por componentes más eficientes contribuirá a disminuir la dependencia de fuentes de energía no renovables, como los combustibles fósiles. Además, al aprovechar la energía eólica, se diversifica la matriz energética y se reduce la vulnerabilidad ante fluctuaciones en los precios del petróleo y el gas.
- Otro punto que destacar es que se tratará de **aprovechar los Recursos de Energías Renovables**, es decir, los nuevos aerogeneradores capturan la energía cinética del viento y la convierten en electricidad. Al utilizar de dichos recursos renovables, se estará contribuyendo a la sostenibilidad y se minimiza el agotamiento de recursos no renovables.
- Se estará **diversificando también las fuentes de suministro**. La repotenciación permite incorporar tecnologías más limpias y sostenibles al sistema eléctrico. Y al diversificar las fuentes de suministro, se reduce la dependencia de una sola fuente y se mejora la seguridad energética.
- Se procederá a una **reducción en las Tasas de Emisión de Gases de Efecto Invernadero**, ya que los aerogeneradores no emiten gases contaminantes durante su operación. Y al reducir la quema de combustibles fósiles, se contribuye a mitigar el cambio climático y se protege el medio ambiente.
- Y, además, se facilitará **el Cumplimiento del Plan Nacional Integrado de Energía y Clima (PNIEC) 2021-2030**. (Acciona, 2024)

El PNIEC establece objetivos ambiciosos para la transición hacia una economía baja en carbono. La repotenciación del parque eólico Cortijo de Iruelas está alineada con estos objetivos y contribuye a cumplir las metas de reducción de emisiones.

5.3 ANÁLISIS ECONÓMICO

En esta sección, me enfocaré en analizar los aspectos económicos que afectarán nuestro proyecto. Identificaremos dos tipos de costes en dicho modelo: los costes de inversión y los costes de producción.

5.3.1 COSTES DE INVERSIÓN

Los costes de inversión son aquellos gastos necesarios para llevar a cabo la construcción del proyecto. En el contexto de parques eólicos, destacamos los siguientes costes principales:

1. Coste de los aerogeneradores: Se incluye el coste de suministro de las turbinas eólicas, así como los trabajos necesarios para su instalación, el transporte hasta el emplazamiento y el montaje de los componentes de la máquina. El precio puede variar según el alcance de responsabilidades acordado entre el suministrador de turbinas y el constructor.
2. Equipos eléctricos: Estos equipos forman parte de la adaptación eléctrica necesaria para conectar el parque a la red. Incluyen subestaciones, transformadores y otros componentes de conexión, que también representan una parte significativa de los costos de inversión.
3. Obra civil: Comprende los trabajos en el emplazamiento para la construcción del parque y la adecuación del terreno. Los costos principales están asociados con las cimentaciones de los aerogeneradores, los viales y caminos de acceso, así como las zanjas para enterrar los cables.
4. Línea de Media Tensión y comunicaciones: Aquí se incluye todo el cableado necesario para la conexión de Media Tensión, desde la salida de las celdas de transformación hasta la entrada a la subestación. También se considera el cableado de fibra óptica para las comunicaciones.
5. Otros costes: Esta categoría agrupa los costes relacionados con el diseño, los estudios del emplazamiento, la gestión del proyecto, los controles de calidad y las medidas para minimizar el impacto ambiental.

Para simular los gastos de dicho modelo, he tenido que estudiar los costes y datos relacionados a otras infraestructuras críticas establecidas alrededor del territorio español. Primero, se ha realizado el balance de costes de todos los parques eólicos de Tahivilla, ya que la información general de la Localidad Tarifeña era más clara a nivel global que por cada parque eólico reestructurado individual.

En el modelo de emplazamiento del parque eólico de Tarifa, se usan13 aerogeneradores *NORDEX 163.6/6.x (7000Kw)*, que como resultado da una potencia instalada de 84,4 MW.

En particular, me he basado en el proyecto inicial de la construcción de los aerogeneradores del parque eólico de Tarifa, "Cortijo de Iruelas" que se dieron lugar en el 2003, para tener un coste aproximado en la disposición del terreno, seguridad, subestaciones eléctricas y cimentaciones.

PARQUE EÓLICO PROYECTO 84,4 MW			
	P.U.	**UDS**	**SUBTOTAL**
AEROGENERADORES			
Suministro, transporte, montaje, puesta en marcha	2.500.000,00 €	13	32.500.000,00 €
TOTAL AEROGENERADORES			32.500.000,00 €
OBRA CIVIL			
Viales y caminos de acceso a parque, plataformas	1.600.000,00 €	1	1.600.000,00 €
Cimentaciones	800.000,00 €	1	800.000,00 €
Restauración Ambiental	100.000,00 €	1	100.000,00 €
Varios (zanjas, torres meteo)	220.000,00 €	1	220.000,00 €
TOTAL OBRA CIVIL			2.720.000,00 €
INFRAESTRUCTURA ELÉCTRICA			
Subestación elevadora (Equipos y materiales, montaje y obra civil)	1.500.000,00 €	1	1.500.000,00 €
Conexión MT (cables, celdas y varios)	340.000,00 €	1	340.000,00 €
TOTAL INSTALACIÓN ELÉCTRICA Y DE CONTROL			1.840.000,00 €
OTROS COSTES			
Gestión de proyecto	500.000,00 €	1	500.000,00 €
Control de calidad	40.000,00 €	1	40.000,00 €
Estudios de seguridad y salud	50.000,00 €	1	50.000,00 €
Estudios ingeniería (Geotécnico, Topográfico, Hidrológico)	60.000,00 €	1	60.000,00 €
Estudios de Impacto Ambiental	150.000,00 €	1	150.000,00 €
TOTAL OTROS COSTES			800.000,00 €
TOTAL			**37.860.000,00 €**

Tabla 4: Simulación Costes Tahivilla. Fuente: Elaboración Propia

Para conseguir el precio del nuevo aerogenerador *NORDEX 163.6/6.x (7000Kw),* basta con investigar en su página web y en el plan de obra de desarrollo del proyecto, publicado por Acciona.

Con esta tabla conseguimos ver los costes iniciales que nos va a suponer la reestructuración de los parques eólicos de Tahivilla. Lo habitual para analizar estos costes, es utilizar un ratio por megavatio instalado, de esta manera nos podrá permitir hacer comparaciones con otros proyectos y valorar si el coste es más o menos elevado.

En este caso tenemos 84,4 MW de potencia, por lo que obtenemos un valor de 2,22 M€/MW.

A partir del análisis anterior, particularizamos los costes para nuestro parque eólico “El Cortijo de Iruelas” a menor escala.

PARQUE EÓLICO PROYECTO 14 MW			
	P.U	**UDS**	**SUBTOTAL**
AEROGENERADORES			
Suministro, transporte, montaje, puesta en marcha	2.500.000,00 €	2	5.000.000,00 €
TOTAL AEROGENERADORES			5.000.000,00 €
OBRA CIVIL			
Viales y caminos de acceso a parque, plataformas	265.402,84 €	1	265.402,84 €
Cimentaciones	132.701,42 €	1	132.701,42 €
Restauración Ambiental	16.587,68 €	1	16.587,68 €
Varios (zanjas, torres meteo)	36.492,89 €	1	36.492,89 €
TOTAL OBRA CIVIL			451.184,83 €
INFRAESTRUCTURA ELÉCTRICA			
Subestación elevadora (Equipos y materiales, montaje y obra civil)	248.815,17 €	1	248.815,17 €
Conexión MT (cables, celdas y varios)	56.398,10 €	1	56.398,10 €
TOTAL INSTALACIÓN ELÉCTRICA Y DE CONTROL			305.213,27 €
OTROS COSTES			
Gestión de proyecto	82.938,39 €	1	82.938,39 €
Control de calidad	6.635,07 €	1	6.635,07 €
Estudios de seguridad y salud	8.293,84 €	1	8.293,84 €
Estudios ingeniería (Geotécnico, Topográfico, Hidrológico)	9.952,61 €	1	9.952,61 €
Estudios de Impacto Ambiental	24.881,52 €	1	24.881,52 €
TOTAL OTROS COSTES			132.701,43 €
TOTAL			**5.889.099,53 €**

Tabla 5: Simulación Costes Cortijo de Iruelas. Fuente: Elaboración Propia

En este caso tenemos 14 MW de potencia, por lo que obtenemos un valor de 2,38 M€/MW.

5.3.2 COSTES DE EXPLOTACIÓN

Este tipo de costes son los que intervienen una vez que el proyecto de construcción de nuestro parque eólico se ha puesto en marcha. Es clave diferenciar los dos tipos de costes que incurren. Costes de explotación y costes de financiación.

Los costes de explotación son aquellos que engloban la operación y el mantenimiento necesario en el parque eólico durante su vida útil. Esto incluye, el alquiler de los terrenos en los que se encuentra el parque situado, los seguros, comisiones e impuestos.

Sin embargo, los costes de financiación son aquellos que vienen dados por los intereses producidos debido a una financiación externa, la cual es necesaria para llevar a cabo el proyecto, en la mayoría de los casos.

En cuanto a nuestro proyecto, detallaremos ambos costes, tomando como referencia órdenes de magnitud de parques con un valor de potencia instalada similar como he especificado en el apartado anterior.

Además, hay que recalcar que; los gastos de administración del proyecto se calcularán mediante un porcentaje con respecto a la facturación anual, en nuestro caso, y por el tamaño de dicho parque eólico, aplicaremos el 1% de los ingresos.

Los costes de financiación serán calculados mediante unos datos e hipótesis iniciales, de forma que consigamos determinar las condiciones de dichos costes y repercutirlos en el proyecto (7% Interés anual).

COSTES DE EXPLOTACIÓN	
Acción	Coste
Operación y mantenimiento	700.000,00 €
Alquiler de terrenos	160.000,00 €
Seguros e Impuestos	110.000,00 €
TOTAL	**970.000,00 €**

Tabla 6: Simulación Costes de Explotación. Fuente: Fernández, 2015

5.3.3 INGRESOS

Otro punto para comentar en el análisis financiero son los ingresos.

Los ingresos generados por el parque estarán directamente vinculados a la tarifa eléctrica vigente de cada país. Para nuestro análisis, tomaremos como referencia la tarifa media existente en España, que es de 60 € por megavatio-hora (MWh). A partir de esta tarifa y considerando la producción total del parque, se podría calcular el importe total de ingresos.

Es importante tener en cuenta los efectos de la inflación a lo largo del tiempo. Por tanto, se deberá asumir también una tasa de inflación inicial del 2.5%. Esto significa que tanto los ingresos como los costes se actualizarán anualmente para reflejar los cambios en el valor del dinero.

Además, durante la vida útil del parque, se establecerá una regulación de tarifas. En los primeros 5 años, utilizaremos el 90% de la tarifa media como base. Durante los siguientes 10 años, esta cifra se reducirá al 85%. Finalmente, hasta el final de la vida útil del parque, aplicaremos un 80% de la tarifa media para calcular los ingresos.

5.4 CIBERSEGURIDAD

5.4.1 PROTECCIÓN DE LA INFRAESTRUCTURA CON SCADA

La manera más eficaz de proteger a las Infraestructuras críticas es fundamentalmente con los sistemas SCADA. Estos sistemas, se conocen en español como Control Supervisor y Adquisición de Datos. SCADA permite la gestión y control de cualquier sistema local o remoto gracias a una interfaz gráfica que comunica al usuario con el sistema.

Dicho modelo es el más utilizado por las empresas de seguridad cibernética para proteger las infraestructuras frente a un ciberataque.

Por ello, considero que, para favorecer la seguridad frente a ataques cibernéticos en la reconstrucción del parque eólico, debería hacerse con sistemas SCADA.

Para poder entender mejor la simulación de este modelo, es de gran importancia explicar el funcionamiento de este sistema.

5.4.2 QUÉ ES SCADA

Un sistema SCADA es una aplicación o conjunto de aplicaciones de software especialmente diseñadas para funcionar sobre ordenadores de control de producción, con acceso a la planta mediante la comunicación digital con instrumentos y actuadores, e interfaz gráfica de alto nivel para el operador (pantallas táctiles, ratones o cursores, lápices ópticos, etc.).

Inicialmente era un programa que permitía la supervisión y adquisición de datos en procesos de control, pero, sin embargo, en los últimos tiempos ha surgido una serie de productos de hardware que han sido diseñados o adaptados directamente para este tipo de sistemas.

El sistema permite comunicarse con los dispositivos de campo (controladores autónomos, autómatas programables, sistemas de dosificación, etc.) para controlar el proceso en forma automática desde la pantalla del ordenador, que es configurada por el usuario y puede ser

modificada con facilidad. Además, provee a diversos usuarios de toda la información que se genera en el proceso productivo.

Los SCADA se utilizan en el control de oleoductos, **sistemas de transmisión de energía** eléctrica, yacimientos de gas y petróleo, redes de distribución de gas natural y generación energética (convencional y nuclear).

Llámese oleoductos a las tuberías provistas de bombas y de otros aparatos para conducir el petróleo a larga distancia.

5.4.3 MONITORIZACIÓN SCADA

La función de monitoreo de estos sistemas se realiza sobre un computador industrial, ofreciendo una visión de los parámetros de control sobre la pantalla de ordenador, lo que se denomina un HMI (Human Machine Interface), como en SCADA, pero solo ofrecen una función complementaria de monitorización: observar mediante aparatos especiales el curso de uno o varios parámetros fisiológicos o de otra naturaleza para detectar posibles anomalías. (Cerrada, 2011)

Es decir, los sistemas de automatización de interfaz gráfica tipo HMI básicos ofrecen una gestión de alarmas básica, mediante las cuales la única opción que le queda al operario es realizar una parada de emergencia, reparar o compensar la anomalía y hacer un reset.

Los sistemas SCADA utilizan un HMI interactivo que permite detectar alarmas y a través de la pantalla solucionar el problema mediante las acciones adecuadas en tiempo real. Esto les otorga una gran flexibilidad. En definitiva, el modo supervisor del HMI de un SCADA no solo señala los problemas, sino que, lo más importante, orienta en cuanto a los procedimientos para solucionarlos. (Cerrada, 2011)

5.4.4 CARACTERÍSTICAS SCADA

Según Gómez et al. (2008), las características principales de un SCADA son las siguientes:

- Adquisición y almacenado de datos para recoger, procesar y almacenar la información recibida en forma continua y confiable.
- Representación gráfica y animada de variables de proceso y su monitorización por medio de alarmas
- Ejecutar acciones de control para modificar la evolución del proceso, actuando ya sea sobre los reguladores autónomos básicos (consignas, alarmas, menús, etc.) o directamente sobre el proceso mediante las salidas conectadas.
- Conectividad con otras aplicaciones y bases de datos, locales o distribuidas en redes de Tecnología en Marcha.
- Supervisión, para observar desde un monitor la evolución de las variables de control.
- Transmisión de información con dispositivos de campo y otros PC.
- Base de datos, gestión de datos con bajos tiempos de acceso.
- Presentación, representación gráfica de los datos. Interfaz del Operador o HMI.
- Alertar al operador sobre cambios detectados en la planta, tanto aquellos que no se consideren normales (alarmas) como los que se produzcan en su operación diaria (eventos). Estos cambios son almacenados en el sistema para su posterior análisis.

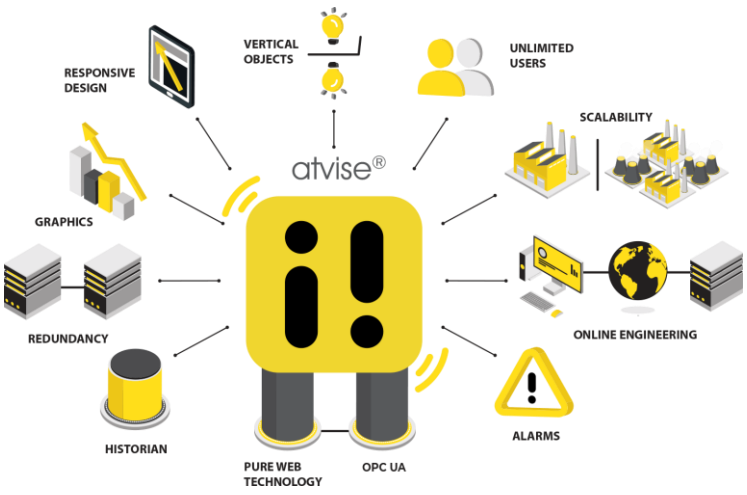

Ilustración 18: SCADA Software. Fuente: Atvise SCADA

5.4.5 PRESTACIONES SCADA

El paquete SCADA, comprende una serie de funciones y utilidades encaminadas a establecer una comunicación lo más clara posible entre el proceso y el operador.

Según Cerrada (2011), el clásico supervisor soportado por un SCADA es un sistema de control que integra las tareas de detección y diagnóstico de fallas, como una actividad previa que permite incorporar de manera natural el control de fallas.

Las prestaciones que ofrece un sistema SCADA son las siguientes:

- Posibilidad de crear paneles de alarma, que exigen la presencia del ordenador para reconocer una parada o situación de alarma, con registro de incidencias.
- Generación de datos históricos de señal de planta, que pueden ser incorporados para su proceso sobre una hoja de cálculo.
- Creación de informes, avisos y documentación en general.
- Ejecución de programas que modifican la ley de control o incluso el programa total sobre el autómata (bajo ciertas condiciones).
- Posibilidad de programación numérica, que permite realizar cálculos aritméticos de elevada resolución sobre la CPU del ordenador.

Ilustración 19: Prestaciones SCADA. Fuente: ATvise SCADA

5.4.6 ELEMENTOS SCADA

1. Componentes de Hardware:

Para Gómez et al. (2008), un sistema SCADA, como aplicación de software industrial específica, necesita ciertos componentes inherentes de hardware en su sistema para poder tratar y gestionar la información captada, que se describen a continuación.

Ordenador Central o MTU (Master Terminal Unit): Se trata del ordenador principal del sistema, el cual supervisa y recoge la información del resto de las subestaciones, ya sean otros ordenadores conectados (en sistemas complejos) a los instrumentos de campo o directamente sobre dichos instrumentos.

Este ordenador suele ser un PC que soporta el HMI. Con esto se consigue que el sistema SCADA más sencillo, es el compuesto por un único ordenador, que es el MTU que supervisa toda la estación.

Ordenadores Remotos o RTU (Remote Terminal Unit): Estos ordenadores están situados en los nodos estratégicos del sistema gestionando y controlando las subestaciones; reciben las señales de los sensores de campo y comandan los elementos finales de control ejecutando el software de la aplicación SCADA.

Estos ordenadores no tienen que ser PC, ya que la necesidad de soportar un HMI no es tan grande a este nivel, por lo tanto, suelen ser ordenadores industriales tipo armarios de control, aunque en sistemas muy complejos puede haber subestaciones intermedias en formato HMI.

Red de comunicación: Este es el nivel que gestiona la información que los instrumentos de campo envían a la red de ordenadores desde el sistema. El tipo de BUS utilizado en las comunicaciones puede ser muy variado según las necesidades del sistema y del software escogido para implementar el sistema SCADA, ya que no todos los softwares (ni los instrumentos de campo como PLC) pueden trabajar con todos los tipos de BUS. Hoy en día, gracias a la estandarización de las comunicaciones con los dispositivos de campo, se puede implementar un sistema SCADA sobre prácticamente cualquier tipo de BUS.

Instrumentos de Campo: Son todos aquellos que permiten realizar tanto la automatización o control del sistema (PLC, controladores de procesos industriales y actuadores en general) como los que se encargan de la captación de información del sistema (sensores y alarmas). Una característica de los SCADA es que sus componentes son diseñados por distintos proveedores, sin coordinación entre sí. De manera que se tienen diferentes proveedores para las RTU (incluso es posible que un sistema utilice RTU de más de un proveedor), módems, radios, minicomputadores, software de supervisión e interfaz con el operador, de detección de pérdidas, etc.

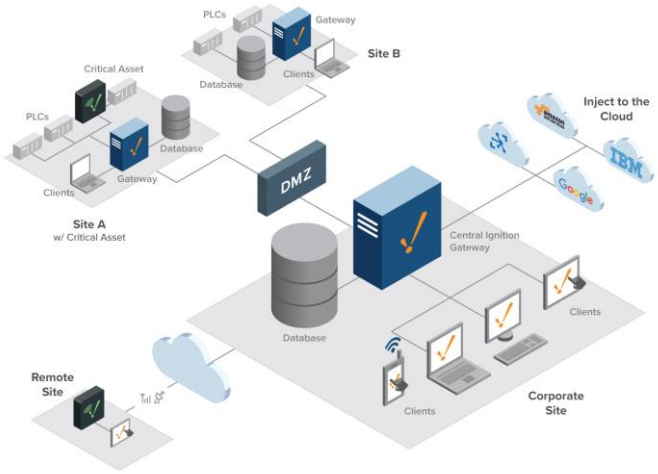

Ilustración 20: Elementos SCADA. Fuente: NVTec

2. Estructura y componentes de un software SCADA:

Para Gómez et al. (2008), los módulos o bloques de software que permiten las actividades de adquisición, supervisión y control son los siguientes:

Configuración: permite definir el entorno de trabajo de la aplicación según la disposición de pantallas requerida y los niveles de acceso para los distintos usuarios. En este módulo, el usuario define las pantallas gráficas o de texto que va a utilizar, importándolas desde otra aplicación o generándolas en el propio SCADA.

Interfaz gráfica del operador: proporciona al operador las funciones de control y supervisión de la planta. El proceso que se supervisará se representa mediante sinópticos gráficos almacenados en el ordenador y generados desde el editor incorporado en el SCADA o importados desde otra aplicación de uso general (Paintbrush, DrawPerfect, AutoCAD, etc.) durante la configuración del paquete.

Módulo de proceso: ejecuta las acciones de mando preprogramadas a partir de los valores actuales de variables leídas. Sobre cada pantalla se pueden programar relaciones entre variables del ordenador o del autómata que se ejecutan continuamente mientras esté activa.

La programación se realiza por medio de bloques de programa en lenguaje de alto nivel (C, Basic, etc.). Es muy frecuente que el sistema SCADA confíe a los dispositivos de campo, principalmente autómatas.

Gestión y archivo de datos: se encarga del almacenamiento y procesado ordenado de los datos, según formatos inteligibles para elementos periféricos de hardware (impresoras, registradores) o software (bases de datos, hojas de cálculo) del sistema, de forma que otra aplicación o dispositivo pueda tener acceso a ellos.

Pueden seleccionarse datos de planta para ser capturados a intervalos periódicos y almacenados como un registro histórico de actividad, o para ser procesados inmediatamente por alguna aplicación de software para presentaciones estadísticas, análisis de calidad o mantenimiento.

Para ello, el SCADA actúa como un servidor DDE que carga variables de planta y las deja en la memoria para su uso por otras aplicaciones Windows, o las lee en memoria para su propio uso después de haber sido escritas por otras aplicaciones.

Una vez procesados, los datos se presentan en forma de gráficas analógicas, histogramas, representación tridimensional, etc., que permiten analizar la evolución global del proceso.

5.4.7 ANÁLISIS ECONÓMICO SCADA

El uso de sistemas SCADA permite monitorear y controlar de manera remota diferentes procesos utilizando una interfaz gráfica de usuario, posibilitando al operador detener o modificar varias etapas del sistema a la vez. La producción automatizada ha experimentado cambios tremendos a partir de la llega de los controladores programables. Este equipo hace que los procesos industriales sean más precisos y eficientes.

De esta forma se reduce el gran coste que comprende el reemplazo del enredado sistema de control convencional basado en contactores y relés (Hurtado, 2017)

La inserción de controladores programables hace que los sistemas industriales sean más eficientes. Esto genera una reducción de costes al sustituir los de sistemas de panel de control complejos (Guerrero et. al, 2017).

Una ventaja a la hora de usar los buses de campo es que pueden suplir sistemas centralizados de control por medio de una red de control, esto mejora significativamente el rendimiento del proceso optimizando recursos y disminuyendo costos. La información enviada de dispositivo a otro es digital; esto genera precisión en el sistema (Guerrero et. al, 2017).

5.5 DISTRIBUCIÓN ECONÓMICA

Como se ha podido recalcar anteriormente, los datos en ciberseguridad de la mayoría de las empresas, dentro del sector energético y sin incluir estas, no aparecen de forma visible en casi ningún documento a los que podamos tener acceso sin ningún tipo de restricción.

Ya que, dichos documentos son privados para garantizar así la seguridad de cada empresa. Por lo que a través de estudios y artículos de distintas consultoras he podido analizar la posible cantidad necesaria a cubrir este gasto.

En concreto, un estudio de IDC estima que 2022 se cerró con una inversión media del 7,7% en ciberseguridad por parte de las empresas, lo que supone un gasto total de 1.749 millones de euros.

No obstante, esta partida continuará incrementándose en los próximos años de manera que en el año 2025 alcanzaría los 2.200 millones de euros en un contexto de incremento de la necesidad de protección en las empresas frente a un complejo escenario de amenazas y a la generalización de entornos tic más abiertos y digitalizados. (Dir&ge, 2022)

- Principales áreas de inversión

Respecto a las áreas de inversión en ciberseguridad, las empresas españolas, destaca estos tres ámbitos:

- Gestión unificada de amenazas: 11%
- Integración de sistemas: 11%
- Servicios de externalización de redes y endpoint[4]: 10%

Dotar de prioridad a estos puntos, permitirán poder asegurar el proceso de digitalización que se está viviendo en la actualidad, al mismo tiempo que se minimiza, o se reduce, el impacto que supone sobre la gestión de datos y procesos de negocio con la actual transformación digital del puesto de trabajo.

Se ha de tener en cuenta que estas prioridades son muy dependientes del tamaño de la empresa. Con esto se consigue que la gestión unificada de amenazas, la integración de sistemas y los servicios de externalización de redes y en endpoint, son objeto de una mayor preocupación en empresas de tamaño grande y mediano.

En el caso de pymes[5] y micro pymes sus prioridades tienen que ver con la protección de punto final (endpoint), centrándose en ordenadores y dispositivos móviles (Dir&ge, 2022)

[4]Endpoint: Dispositivo informático remoto que se comunica a través de una red a la que está conectado.

[5]Pymes: pequeñas y medianas empresas

Según Dir&ge, (2022) las observaciones para el 2023, basadas en algunas investigaciones recientes de los ESG fueron las siguientes:

Primero, las cifras.

En ciberseguridad, el 65% de las organizaciones tiene previsto aumentar su gasto en 2023.

Las inversiones serán más tácticas que estratégicas. Los equipos de seguridad ya están evitando los contratos a largo plazo y posponiendo proyectos complejos que requieren muchos recursos. Esto significa que dividirán las iniciativas de proyectos y plataformas en partes digeribles, invirtiendo en necesidades prioritarias.

El gasto en servicios dominará los presupuestos. La investigación de ESG indica que casi la mitad (45%) de las organizaciones afirman tener una escasez problemática de competencias en ciberseguridad. Esto significa que no tienen una plantilla de tamaño adecuado y que carecen de algunas habilidades de ciberseguridad avanzadas pero necesarias. A pesar de los despidos en el sector, los profesionales de la ciberseguridad seguirán teniendo una gran demanda.

El gasto mundial en productos y servicios de ciberseguridad va a crecer un 13,2% en 2023 (Canalys, 2022). La cifra total de inversión de las empresas podría llegar hasta los 223.800 millones de dólares. Canalys prevé que el gasto mundial en ciberseguridad aumentará un 13,2% durante este año, y se elevará a 223.800 millones de dólares en el mejor de los escenarios previstos por la consultora, cuyos expertos destacan que el crecimiento que se producirá en la categoría de servicios.

En su análisis sostiene que los niveles de amenazas persistentes mantendrán la ciberseguridad de las empresas en un lugar destacado de la lista de prioridades de inversión de las organizaciones.

Sin embargo, los resultados en 2023 fueron estos:

El mercado de la ciberseguridad en España muestra un crecimiento respecto al año pasado del 9,2%, alcanzando los 2.130 millones de euros en 2023, según IDC (Informe de Datos de Cotización). Los segmentos de mayor incremento son los relativos a servicios gestionados de seguridad (12,4%), análisis, inteligencia, respuesta y orquestación de la ciberseguridad (13,8%) y servicios de identidad (12,4%).

5.5.1 EN EL SECTOR ENERGÉTICO

Primero, hemos de estudiar los elementos clave en los que se dividen los gastos destinados a la ciberseguridad en el parque eólico. Un estudio realizado por Deloitte nos muestra los respectivos % a los que se han dividido el gasto en España este último año.

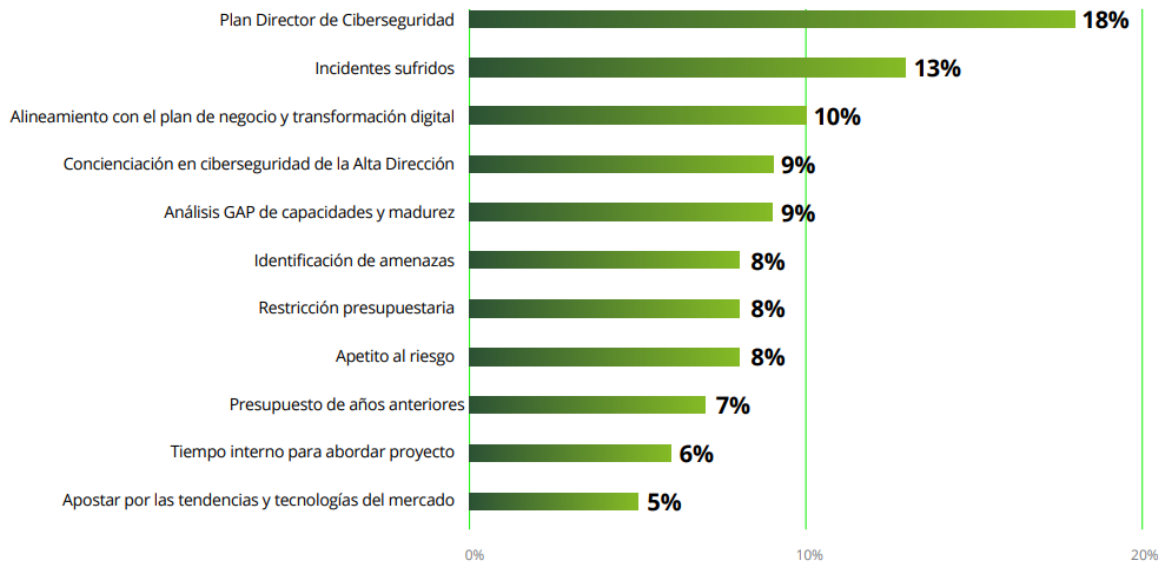

Ilustración 21: Priorización reparto del presupuesto de ciberseguridad. Fuente: Deloitte

Esta perspectiva estratégica no solo implica una inversión en seguridad, sino también en el éxito y la sostenibilidad de la organización. Al considerar la ciberseguridad como parte integral de la estrategia empresarial, es posible identificar y mitigar de manera proactiva los riesgos existentes, lo que a su vez garantiza la continuidad operativa de la empresa.

La distribución de la inversión en ciberseguridad en instalaciones industriales se basa en varios factores clave.

- En primer lugar, el **Plan Director de Ciberseguridad** representa el **18%** del presupuesto total. Este requiere un enfoque estratégico más amplio y alineado con los objetivos del negocio.

- El **13%** del presupuesto se destina a abordar los **incidentes de seguridad sufridos previamente**, lo que garantiza una respuesta efectiva ante amenazas.

- La **alineación con el plan de negocio y la transformación digital** también es crucial, representando el **10%** de la inversión. Esto asegura que la ciberseguridad esté integrada en la estrategia general de la empresa.

- La **alta dirección** también juega un papel importante, con un **9%** del presupuesto dedicado a la concienciación de ciberseguridad en este nivel.

- Las **restricciones presupuestarias** (8%), el **apetito al riesgo** (8%), los **presupuestos de años anteriores** (7%), el **tiempo interno para abordar proyectos** (6%) y la **inversión en tendencias y tecnologías del mercado** (5%) completan la distribución de recursos para fortalecer la seguridad en las instalaciones industriales.

Se puede identificar también la distribución de los gastos por área.

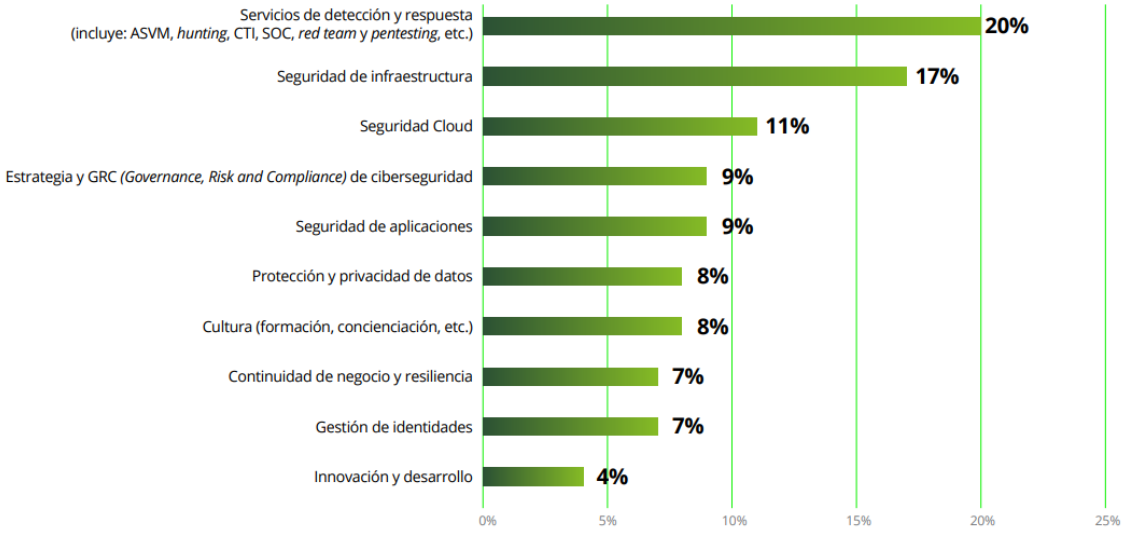

Ilustración 22: Distribución media presupuesto de ciberseguridad en áreas. Fuente: Deloitte

Las áreas corresponden con:

- **Servicios de detección y respuesta**: Estos servicios se centran en identificar y responder a amenazas de seguridad. Incluyen la monitorización constante de eventos y la detección temprana de actividades sospechosas.

- **Seguridad de infraestructura**: Se refiere a proteger los componentes tecnológicos fundamentales, como servidores, redes y dispositivos, para prevenir ataques y garantizar su funcionamiento seguro.

- **Seguridad en la nube**: Aborda los riesgos específicos asociados con el uso de servicios en la nube. Esto incluye la protección de datos almacenados y transmitidos en entornos de nube.

- **Estrategia GRC de ciberseguridad**: GRC (Gobierno, Riesgo y Cumplimiento) se enfoca en establecer políticas, procesos y controles para gestionar riesgos y cumplir con regulaciones. En ciberseguridad, esto implica alinear estrategias con objetivos de seguridad.

- **Seguridad de aplicaciones**: Se concentra en proteger aplicaciones y software contra vulnerabilidades y ataques. Esto incluye pruebas de seguridad, parches y buenas prácticas de desarrollo.

- **Protección y privacidad de datos**: Asegura que los datos personales y confidenciales estén protegidos adecuadamente, cumpliendo con regulaciones como el RGPD.

- **Cultura (formación, concienciación…)**: Fomenta la conciencia y la formación en seguridad cibernética entre los empleados. Una cultura de seguridad sólida es esencial para prevenir incidentes.

- **Continuidad de negocio y resiliencia**: Se refiere a la capacidad de una organización para mantener operaciones incluso después de un incidente de seguridad. Esto implica planes de recuperación y medidas preventivas.

- **Gestión de identidades**: Controla el acceso a sistemas y datos, asegurando que solo las personas autorizadas tengan permisos adecuados.

- **Innovación y desarrollo:** Busca soluciones creativas y nuevas tecnologías para abordar los desafíos de seguridad cibernética en constate evolución.

Analizando los resultados del dicho diagrama llegamos a la conclusión de:

Observando la distribución del presupuesto por áreas, en proporción, se llega a apreciar el elevado coste asociado a mantener los servicios de detección y respuesta.

Por otro lado, “innovación y desarrollo” apenas recibe presupuesto. Esto puede llegar a suponer un gran riesgo ante la rápida sofisticación de los ataques que ya vimos al principio de este documento.

Además, existe un ligero desalineamiento evidente entre las preocupaciones recogidas en este estudio, como son la “sofisticación de las amenazas y presupuesto elevado de los

atacantes" con la distribución de los presupuestos, donde se destina menor cantidad a cuestiones como continuidad de negocio y gestión de identidades.

Ambos son aspectos fundamentales para garantizar la seguridad: el primero, ante retos como la continuidad de las operaciones; y el segundo, para los riesgos de ciberseguridad procedentes de terceros.

5.5.2 INVERSIÓN TOTAL

Una vez obtenido el desglose de costes en ciberseguridad en relación con el sector energético. Es necesario poder averiguar para dicha simulación, que cantidad es la necesaria para cubrir todos estos gastos del patrimonio total. Es decir, cuál debe ser la inversión inicial únicamente para cubrir los costes en ciberseguridad.

Como he podido recalcar anteriormente, los datos en ciberseguridad de la mayoría de las empresas, dentro del sector energético y sin incluir estas, no aparecen de forma visible en casi ningún documento a los que podamos tener acceso sin ningún tipo de restricción.

Ya que, dichos documentos son privados para garantizar así la seguridad de cada empresa. Por lo que a través de estudios y artículos de distintas consultoras he podido realizar esta simulación, acercándome de la manera más próxima posible al posible gasto en ciberseguridad del Parque eólico de Tarifa.

COSTES CIBERSEGURIDAD	
2023	25.000,00€
2024	28.500,00 €

Tabla 7: Simulador aumento costes en Ciberseguridad. Fuente: Elaboración propia

En la tabla anterior, aplicamos el % aproximado que darían las empresas a los gastos en ciberseguridad en este 2024. Como he detallado anteriormente, este sería un 14%.

En el análisis de costes desarrollado anteriormente, podíamos ver organizado un coste como "Seguridad y Salud". Al ser únicamente un simulador de gastos, he repartido dicho epígrafe equitativamente, es decir, 50% ciberseguridad, y un 50% en seguridad de personal (aquí se incluiría seguros, infraestructuras…)

COSTES CIBERSEGURIDAD 2024	
ACCIÓN	COSTE
Servicios detección y respuesta	5.700,00 €
Seguridad Infraestructura	4.845,00 €
Seguridad Cloud	3.135,00 €
Estrategia GRC de ciberseguridad	2.565,00 €
Seguridad de aplicaciones	2.565,00 €
Protección y privacidad de datos	2.280,00 €
Cultura (formación, concienciación…)	2.280,00 €
Continuidad de negocio y resiliencia	1.995,00 €
Gestión de identidades	1.995,00 €
Innovación y desarrollo	1.140,00 €
TOTAL COSTES CIBERSEGURIDAD 2024	**28.500,00 €**

Tabla 8: Desglose Simulador Costes en Ciberseguridad. Fuente: Elaboración propia

En la tabla anterior he distribuido el coste total en ciberseguridad empleado en las distintas áreas de este sector.

Por lo que a la hora de organizar la distribución de gastos en la simulación de dicho modelo del Parque eólico de Tarifa ("Cortijo de Iruelas"), considero que la inversión en ciberseguridad (correspondiente al gasto en seguridad) en su P&L, debería ser un 14% mayor al 2023, lo que correspondería a 28.500,00 €

5.5.3 GASTO ADICIONAL EN CASO DE CIBERATAQUE

Según los datos de las investigaciones de Check Point Research, el pago del rescate por la recuperación de los datos robados en estos ataques es solo una pequeña parte del coste que las víctimas deben asumir.

En realidad, el coste total que supone la volver a la normalidad tras un ataque de ransomware con todos los datos y sistemas reestablecidos es hasta siete veces mayor que el precio del rescate.

Así lo constata el hecho de que, en España, durante el primer trimestre de este 2021, un ataque de ransomware afectó a una de cada 54 empresas. Se trata de una cifra sensiblemente superior a la media Europa ya que, durante el mismo período, una de cada 80 empresas se ha visto afectadas por esta amenaza.

Este aumento de los ataques de ransomware parece que seguirá a lo largo de los próximos meses ya que se han convertido en una de las amenazas más lucrativas para los ciberdelincuentes. Según los datos aportados por Check Point, el precio que los atacantes suelen pedir a las víctimas por la recuperación de sus **datos robados es proporcional a sus ingresos anuales.**

En este sentido, la cantidad exigida en estas extorsiones oscila entre el 0,7% y el 5% de las ganancias anuales de las organizaciones. Un importe que los expertos recomiendan no pagar ya que no siempre es garantía de recuperación de los datos extraídos.

5.5.4 COSTES ADICIONALES DEL RANSOMWARE

Los atacantes están perfeccionando sus estrategias a la hora de negociar para conseguir el pago del rescate y, a lo largo del pasado año también se experimentó una disminución de los días en los que las víctimas eran extorsionadas, pasando de 15 a 9 días.

Si bien el montante de este rescate ya es una cifra muy golosa, los investigadores de Check Point ponen el foco en los costes ocultos adicionales que conllevan los ataques de ransomware.

En este sentido, destacan el coste lateral ya que, en el caso de los que abogan por pagar el rescate deben tener en cuenta que esa es solo una parte del coste total. La intervención y el restablecimiento de los sistemas, los honorarios y los costes de monitorización pueden elevar el montante hasta en 7 veces el pago de la extorsión.

Aquí también es importante tener en cuenta la duración del ataque si bien, de acuerdo con los expertos de Check Point, en el último año se ha reducido en seis días menos de lo que duraba la extorsión en 2020.

No obstante, los ciberdelincuentes siempre buscarán sacar el mayor rédito de sus ataques. Para ello suelen seguir una serie de reglas definidas con las que tratan de exprimir al máximo sus posibilidades de éxito. Estas tienen en cuenta la postura financiera de la víctima, la calidad de los datos expuestos, la posible existencia de un ciberseguro, e incluso la propia reputación del grupo de ransomware. Asimismo, a la hora de negociar, el enfoque y los intereses de las partes negociadoras resulta clave.

Tal y como destaca Eusebio Nieva, director técnico de Check Point Software para España y Portugal, es clave tener en cuenta que el rescate no es una cifra decisiva ya que existen estas otras consideraciones financieras relacionadas.

5.5.5 CONTRIBUCIÓN O AYUDA ECONÓMICA

- Fondos de Inversión:

Como estos gastos van aumentando progresivamente, las empresas están recurriendo a fondos de inversión.

Los fondos de inversión son instrumentos con el cual los inversores, también llamados partícipes, ponen en común su capital o patrimonio para que sea organizado e invertido por una gestora profesional, con el fin de obtener una rentabilidad. (De la Cruz, 2024)

Por tanto, sirven como instrumento de ahorro que permite a los inversores acceder al mercado financiero confiando su capital en profesionales.

No se trata de una sociedad, sino de la unión de un capital que no está dotado de personalidad jurídica.

En un fondo de inversión **hay tres partes**:

1. **Partícipes**: son las personas que destinan su capital al fondo para que éste lo gestione y lo invierta. Las aportaciones económicas pueden ser únicas (un solo pago) o bien periódicas. Estos también son llamados inversores.
2. **Gestora**: su función es la de gestionar e invertir el capital de los partícipes del fondo, teniendo plena independencia en la toma de decisiones. De esta manera decide en qué mercados se invierte el capital, cuándo, qué cantidad, cuándo se vende. A cambio, la gestora cobra a los participantes una comisión por su trabajo.
3. **Depositario**: es la entidad que se encarga de la custodia de los activos del fondo. Suelen ser los bancos.

He aquí una recopilación de los fondos que podrían ser de interés para esta simulación.

Fondos	**Inversor**	**Estado del Fondo**	**Tamaño del Fondo**[7]	**Moneda**	**Objetivo del Fondo**
Elaia Fund III	Elaia Partners	Abierto	60,00	€	120.00
GapMinder Venture Fund II	GapMinder Venture Partners	Abierto		€	80.00
Brienne IV	Tikehau Ace Capital, Tikehau Capital	Abierto	226,00	€	500.00
European Cyber Tech Fund V	TIN Capital	Abierto		€	100.00
Programma 103	P101	Abierto	150,00	€	250.00
The Swanlaab Tech Fund II	Swanlaab Venture Factory	Abierto	45,00	€	60.00 - 80.00
VCC Deep Tech Fund	Value Creation Capital	Abierto	21,00	€	50.00
33N Cybersecurity and Infrastructure Software Fund	33N Ventures	Abierto	150,00	€	150.00
Alantra Global Technology Fund	Alantra Partners	Evergreen[6]		$	
CDP Evolution Fund	CDP Venture Capital	Open		€	700.00
Digital Ventures Fund I	Orange Ventures	Evergreen	350,00	€	
Metavallon VC Fund II	Metavallon VC	Abierto	22,20	€	

Tabla 9: Características Económicas de los Fondos

[6]Evergreen: Perenne, que permanece en el tiempo. En este caso, el fondo tiene fecha de cierre.

[7]El tamaño del fondo se mide en millones de cada unidad monetaria

Para obtener estos datos en tiempo real se ha utilizado la plataforma de inversión Pitchbook. Pitchbook es la fuente definitiva de datos sobre los mercados de capitales globales y de investigaciones expertas exclusivas. Con acceso a los datos de mercado privados más completos, se consigue seguir la evolución del panorama financiero, identificar tendencias rápidamente, tomar decisiones mejor fundamentadas y más.

Fondo	**Localización del Fondo**	**Interés del Fondo**
Elaia Fund III	Paris, Francia	Inteligencia Artificial & Machine Learning, Ciberseguridad.
GapMinder Venture Fund II	Amsterdam, Países Bajos	Ciberseguridad, FinTech
Brienne IV	Paris, Francia	Ciberseguridad
European Cyber Tech Fund V	Naarden, Netherlands	Ciberseguridad
Programma 103	Milan, Italia	Ciberseguridad, EdTech, FinTech, Tecnología Inmobiliaria
The Swanlaab Tech Fund II	Alcobendas, España	Ciberseguridad, FinTech, Robots and Drones, Space Technology
VCC Deep Tech Fund	Bilthoven, Países Bajos	Artificial Intelligence & Machine Learning, Ciberseguridad, Nanotecnología
33N Cybersecurity and Infrastructure Software Fund	Porto, Portugal	Ciberseguridad, Infraestructuras
Alantra Global Technology Fund	Madrid, España	Inteligencia Artificial & Machine Learning, Coches automáticos, Cryptocurrency/Blockchain, Ciberseguridad.

Tabla 10: Información adicional de los Fondos

La repotenciación de Tahivilla ha recibido 8,3 millones de fondos del Plan de Recuperación, Transformación y Resiliencia (PRTR), financiado por la Unión Europea NextGenerationEU.

- Ayudas del Gobierno:

Además de los fondos de inversión, podemos recurrir a las ayudas que ofrece el gobierno, un ejemplo de estas seria la convocatoria "Activa Ciberseguridad". Dicha ayuda se aplica a pymes, y es una iniciativa del Ministerio de Industria, Comercio y Turismo en el desarrollo de su Estrategia nacional de Industria Conectada 4.0 que tiene entre sus objetivos el impulso de la transformación digital de la industria española aumentando su potencial de crecimiento.

El programa, que cuenta con la colaboración INCIBE[8] y está gestionado a través de la Escuela de Organización Industrial (EOI), tiene como objetivo otorgar ayudas en especie dirigidas a mejorar los niveles de ciberseguridad de las pequeñas y medianas empresas.

Este programa ofrece un estudio de la situación actual de la empresa en relación con la Ciberseguridad para conocer su nivel de seguridad actual y así conseguir llegar a la **elaboración de un Plan de Ciberseguridad específico** para la misma.

El programa 'Activa Ciberseguridad' para pymes está dotado con un presupuesto inicial de **9,63 millones de euros** para prestar el asesoramiento a un total estimado de **4.500 pymes** de todo el territorio nacional.

La cuantía individualizada de las ayudas en especie que se concedan, entendida como el equivalente de subvención bruta, será de **2.140 euros** por empresa beneficiaria.

Aunque no es una cantidad abrumadora para cualquier empresa, teniendo en cuenta el desglose de costes en el capítulo de análisis financiero, serviría para cubrir cualquier gasto en ciberseguridad de nuestro parque eólico en Tarifa. (Plan Recuperación del Gobierno, 2024)

[8]INCIBE: Instituto Nacional de Ciberseguridad en España

5.5.6 DISPOSICIÓN A PAGAR EL RESCATE

Aunque se inviertan grandes cantidades en la ciberseguridad de una empresa, no siempre se recurre a pagar el rescate.

En 2021, Sophos (empresa de ciberseguridad) realizó una encuesta independiente a 550 responsables de TI. En dicha encuesta se llegaron a las siguientes conclusiones;

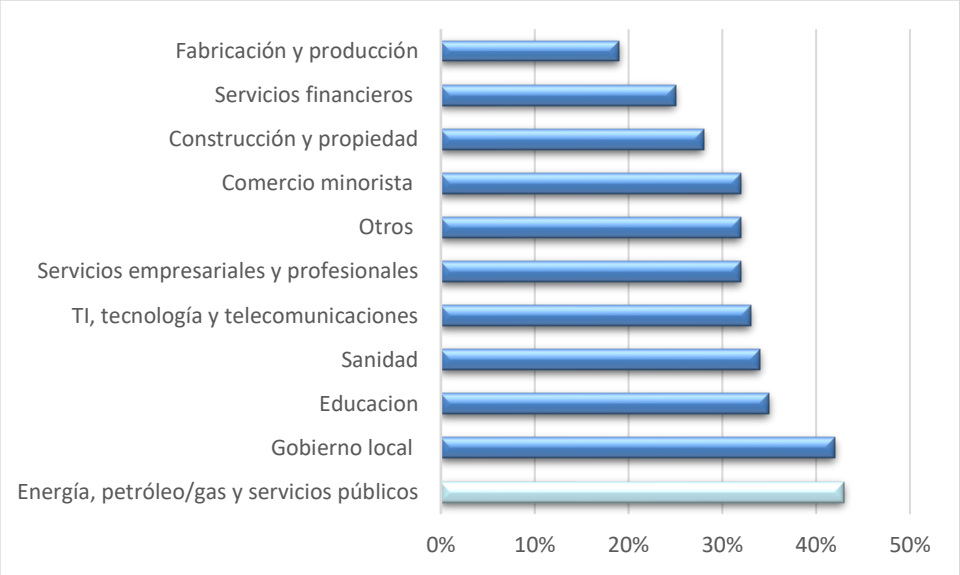

Ilustración 23: Sectores que pagarían el rescate. Fuente: Deloitte

La encuesta reveló que el sector de la energía, petróleo/gas y servicios públicos es el más predispuesto a pagar el rescate, ya que el (aproximadamente) 43 % accedió a la demanda de un rescate. Este sector suele tener mucha infraestructura heredada que no puede actualizarse fácilmente, de modo que las víctimas podrían sentirse obligadas a pagar el rescate a fin de permitir la continuidad de los servicios. Otra posible explicación de esto es la dificultad que tiene el sector para restaurar los datos cifrados a partir de copias de seguridad.

Se puede observar, que el gobierno local es el sector con el segundo nivel más alto de pagos de rescates (42 %). Pero es de añadir que también es el sector con más probabilidades de que se cifren sus datos. Es muy posible que la predisposición de las entidades de gobiernos

locales a pagar esté provocando que los delincuentes dirijan sus ataques más complejos y efectivos contra este colectivo.

Pero ¿qué sectores son los más propensos a realizar copias de seguridad y así evitar la desaparición de sus datos?

En el mismo estudio mencionado anteriormente, sacaron los siguientes resultados:

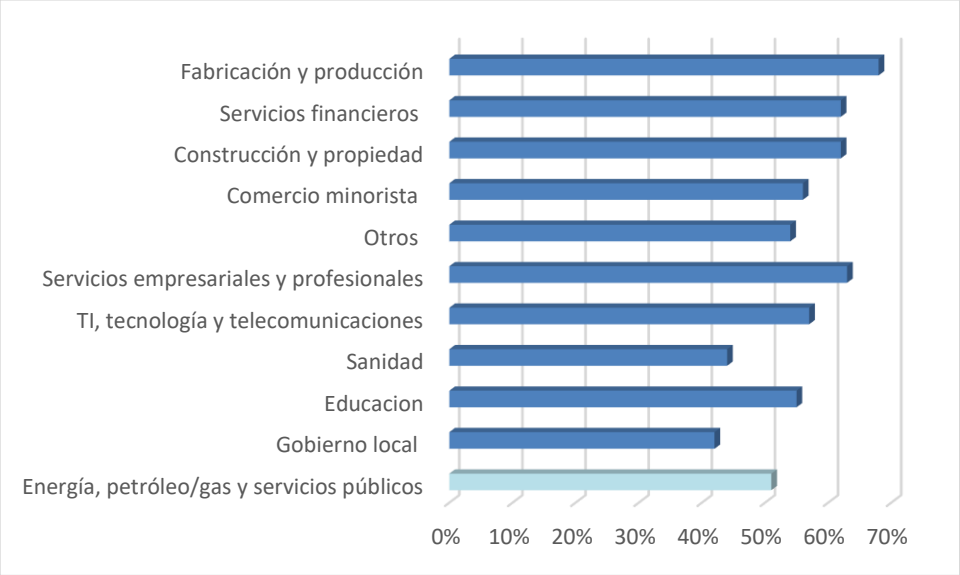

Ilustración 24: Sectores que realizan copia de seguridad. Fuente: Deloitte

Podemos observar, que los sectores financieros con un 62% fueron de los más capaces para restaurar datos cifrados a partir de copias de seguridad. Es probable que esto se deba a que los bancos y muchas otras organizaciones de servicios financieros están obligados a tener planes de continuidad empresarial y de recuperación de desastres (BC-DR) a fin de evitar enormes pérdidas si se produce un desastre o una filtración de datos. Crear copias de seguridad y practicar la restauración de datos a partir de ellas será una parte integral de cualquier buen plan.

Sin embargo, pagar el rescate no implica la recuperación total de los datos. Lo que los atacantes no mencionan al exigir un rescate es que, aunque pague, las probabilidades de que recupere todos sus datos son escasas.

5.5.7 EL COSTE DEL RANSOMWARE

De forma global en todos los sectores, el importe de rescate medio este último año, fue de 170404 USD, (158.475,72 €). Sin embargo, hemos de tener en cuenta que pagar un rescate puede exponer a las empresas del sector energético a un mayor riesgo legal y de cumplimiento.

Estas cifras divergen mucho de los pagos de ocho cifras en USD que suelen verse en los titulares por varias razones.

Tamaño de la organización. Los encuestados pertenecen a organizaciones medianas de entre 100 y 5000 usuarios que, por lo general, tienen menos recursos financieros que las organizaciones de mayor tamaño. Los responsables del ransomware adaptan los rescates que exigen a la capacidad de pago de sus víctimas, por lo que normalmente aceptan importes menores de empresas más pequeñas. Es decir, los datos lo demuestran, ya que el rescate medio para organizaciones de 100 a 1000 empleados fue de 107 694 USD (100.155,42 €), mientras que el rescate medio pagado por las organizaciones de 1001 a 5000 empleados asciende a 225 588 USD, (209.796,84 €).

Tipo de ataque. Hay muchos responsables del ransomware y muchos tipos de ataques de ransomware, desde atacantes altamente cualificados que utilizan tácticas, técnicas y procedimientos (TTP) sofisticados que se centran en objetivos individuales, hasta operadores menos habilidosos. Los atacantes que realizan una gran inversión en un ataque dirigido exigen un elevado rescate que compense su esfuerzo, mientras que los responsables de ataques genéricos suelen aceptar un menor retorno de la inversión (ROI).

Ubicación. Como hemos visto al comienzo, esta encuesta cubre 30 países de todo el mundo, con distintos niveles de PIB. Los atacantes exigen los rescates más altos en economías

occidentales desarrolladas, basándose en su percepción de que pueden pagar sumas mayores. Los dos importes de rescate más elevados fueron mencionados por encuestados de Italia. En cambio, en la India, el rescate medio fue de 76 619 USD, (71.255,67 €).

Sin embargo, el rescate es solo una pequeña parte del coste total de la recuperación de un ataque de ransomware. Las víctimas se enfrentan a una amplia variedad de gastos adicionales, como el coste de reconstruir y proteger sus sistemas de TI, costes de RR. PP. y análisis forenses.

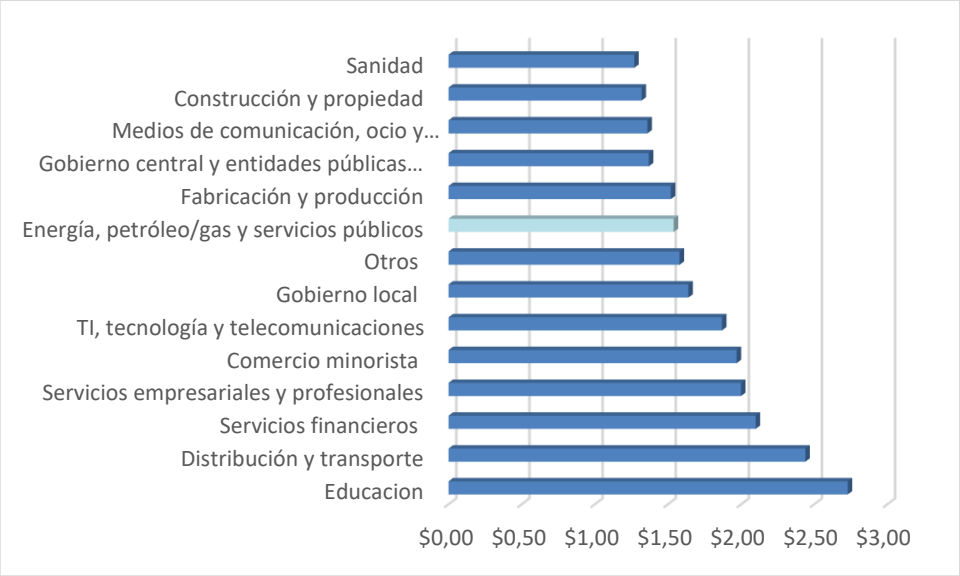

Ilustración 25: Coste medio remediación Ciberataque. Fuente: Elaboración Propia

La encuesta reveló que el sector energético, registra un coste medio de remediación del ransomware de 1,54 millones de USD (considerando el tiempo de inactividad, las horas perdidas, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, las sanciones legales y por incumplimiento, etc.)

Hay varios factores que podrían explicar esto.

En principio, las organizaciones de servicios energéticos, aunque no guarden una gran cantidad de datos confidenciales de personas, empresas y organizaciones públicas, son las

responsables del suministro de energía a todos los hogares. De modo que incurren en altos costes de notificación de filtraciones de datos como parte de sus esfuerzos de remediación.

En segundo lugar, la interrupción de las operaciones de las organizaciones de servicios energéticos puede causar estragos a escala mundial. Esto ejerce una enorme presión sobre los negocios para volver a ponerse en marcha lo antes posible y a cualquier coste. Ya que involucra al funcionamiento en mayor parte al resto de sectores.

Y, por último, como normalmente los clientes pueden cambiar de proveedor con facilidad, las organizaciones de servicios energéticos están totalmente expuestas al impacto empresarial de los daños en su reputación, que conlleva la pérdida de clientes.

5.5.8 RESPUESTA

Contar con un plan de respuesta a incidentes efectivo es una forma segura de minimizar el impacto. Un factor clave a tener en cuenta es saber, que sectores cuentan con un plan de acción y que beneficios conlleva tenerlo.

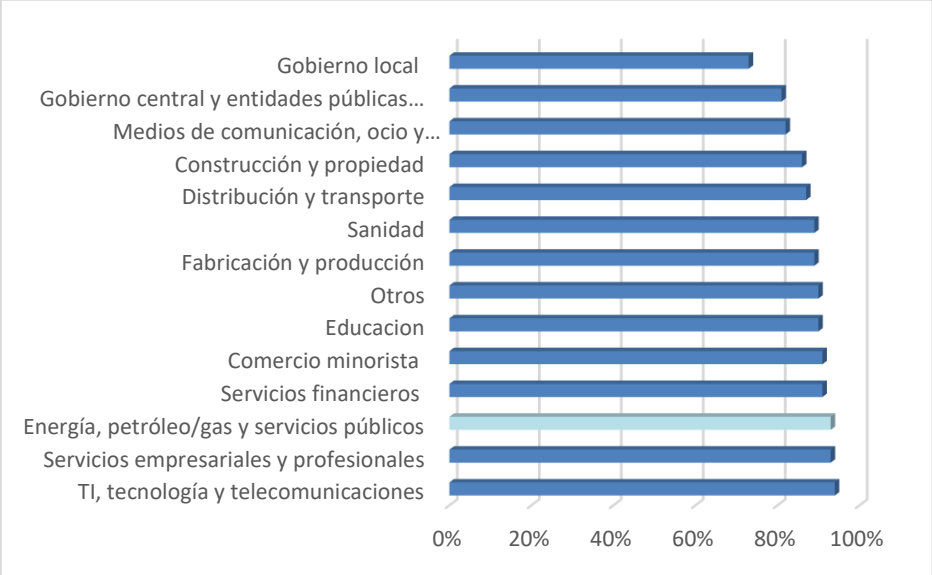

Ilustración 26: Sectores con plan de recuperación ciberatque

La encuesta reveló que hoy en día la mayoría de los sectores se encuentran en disposición de un plan de acción en el supuesto caso de que se sometieran a una ciber-amenaza. En el pódium se encuentran TI, tecnologías de comunicación, los servicios empresariales y profesionales y el sector energético.

Todos los sectores se encuentran por encima del 75%, es decir, la mayoría de las empresas que confrontan dicho sector se encuentran con un plan de acción y posibilidad de respuesta positiva ante un ataque.

Capítulo 6. ANÁLISIS DE RESULTADOS

El objetivo de dicho TFG era estudiar y analizar el impacto de los ciberataques en el sector eólico español. Como se ha podido observar a lo largo de este proyecto, es que las amenazas cada vez son más frecuentes y alcanzan unos niveles de sofisticación que provoca en las empresas una inversión y protección mayor de sus infraestructuras.

6.1.1 COSTES

Analizando los costes de la inversión aproximada que se ha realizado en el parque eólico y la disposición en ciberseguridad, observamos un aumento en la protección cibernética del 14% con respecto al año anterior. Haciendo hincapié en los servicios detección y respuesta.

Se ha podido comprobar que no es más importante la protección si no también la capacidad de reacción, y que la mayoría de las empresas cuenta con un plan de acción ante cualquier ataque.

En la casuística de que al parque eólico le afectase un ciberataque, se estimaría que; Según los datos aportados por Check Point, el precio que los atacantes suelen pedir a las víctimas por la recuperación de sus datos robados es proporcional a sus ingresos anuales.

Además, la cantidad exigida en estas extorsiones oscilaría entre el 0,7% y el 5% de las ganancias anuales de las organizaciones. Es un importe que los expertos recomiendan no pagar ya que no siempre es garantía de recuperación de los datos extraídos.

Otro coste que también habría que tenerse en cuenta, es el coste adicional del Ransomware, donde hace referencia a la intervención y el restablecimiento de los sistemas, los honorarios y los costes de monitorización

Estos costes pueden elevar el montante hasta en 7 veces el pago de la extorsión.

Por ello es clave tener en cuenta que el rescate no es una cifra final y única, ya que existen estas otras consideraciones financieras relacionadas.

6.1.2 CONSECUENCIAS EN EMPRESAS

Los efectos de los ciberataques dependen de si van acompañados de su posterior éxito o no. Si se da el primer caso y tienen éxito, los ataques cibernéticos dañan a las empresas. Pueden llegar a causar tiempo de inactividad, pérdida de datos y pérdida de dinero.

Supongamos una serie de ejemplos:

Llamamos a los atacantes, piratas informáticos, estos pueden utilizar programas maliciosos o ataques de denegación de servicio para provocar fallos del sistema o del servidor. Lo que acompaña a dicho ataque es el tiempo de inactividad, este puede provocar importantes interrupciones del servicio y pérdidas financieras.

Los ataques de inyección permiten a los piratas informáticos alterar, eliminar o robar datos de un sistema.

Los ataques de cibersecuestro pueden desactivar un sistema hasta que la empresa pague al atacante un rescate. La cantidad requerida para afrontar dicho rescate se ha especificado anteriormente.

Además de dañar directamente al objetivo, se pueden abordar una serie de repercusiones que no están claras desde el principio. Los ciberataques también pueden tener consecuencias para las víctimas más allá del objetivo inmediato.

Por ejemplo, que ocurriría si en el parque eólico “Cortijo de Iruelas” se produjese un ciberataque.

El Cortijo de Iruelas, como uno de los parques eólicos más fuertes de la localidad tarifeña, consta del mayor sistema de aerogeneradores refinados de la Península Ibérica. Los atacantes pueden llegar a ingresas a la red de la empresa utilizando una contraseña comprometida. El parque eólico que suministra a casi 13.000 hogares del territorio español. Esto provocaría una escasez energética a gran parte de la ciudad de Cádiz.

6.1.3 DETECCIÓN

Es imposible evitar completamente los intentos de ciberataques, por lo que los parques eólicos también pueden utilizar la monitorización continua de la seguridad y los procesos de detección temprana para identificar y marcar los ciberataques en curso. Algunos métodos de detección que se pueden emplear podrían ser:

- Los Sistemas SIEM, estos son sistemas de **gestión de eventos e información de seguridad.** Su funcionamiento se basa en centralizar y rastrear las alertas de diversas herramientas internas de ciberseguridad, incluidos sistemas de detección de intrusiones (IDS), sistemas de detección y respuesta de puntos finales (EDR) y otras soluciones de seguridad.

- Además, existen también las plataformas de inteligencia sobre amenazas, y lo que se consigue con esto es enriquecer las alertas de seguridad para así poder ayudar a los equipos de seguridad a comprender los tipos de amenazas de ciberseguridad a las que se enfrentan.

- Otro método de detección es el **software antivirus,** este es capaz de analizar regularmente los sistemas informáticos en busca de programas maliciosos y erradicar automáticamente el malware identificado.

- Los procesos de búsqueda proactiva de amenazas pueden realizar un seguimiento de las ciber-amenazas que acechan secretamente en la red, como las amenazas persistentes avanzadas (APT).

Capítulo 7. CONCLUSIONES Y TRABAJOS FUTUROS

7.1.1 PREDICCIONES

Una vez analizado todos los resultados, procedo a realizar una serie de conclusiones y predicciones para este 2024 y 2025

Para finales del 2024, el 60% de las principales empresas europeas habrán aumentado su gasto anual en ciberresiliencia en un 20% para proteger sus inversiones digitales contra el ciberriesgo, lo que supondrá un gasto adicional de 5.900 millones de euros en ciberseguridad en este 2024. (itReseller, 2023)

Los ciberataques han tenido un impacto significativo en el sector eólico español. A medida que la digitalización avanza, las empresas energéticas se vuelven más vulnerables a estas amenazas. Los ataques cibernéticos pueden afectar la producción, interrumpir operaciones y, en última instancia, dañar el medio ambiente. Además, el sector eólico contribuye al empleo directo e indirecto en España, por lo que cualquier interrupción tiene consecuencias económicas y sociales. Para protegerse, las empresas deben implementar medidas de seguridad robustas y estar preparadas para enfrentar estos desafíos en constante evolución.
Se llega a la conclusión de distintos métodos de detección de ciberataques que se han explicado en los resultados. (Calzada, 2021)

Por lo tanto, la seguridad cibernética se ha convertido en una prioridad para garantizar la sostenibilidad y el crecimiento continuo de la energía eólica en el país.

Un estudio de PwC afirma que el creciente uso de tecnologías digitales y el panorama de amenazas en constante evolución ya ha dado como resultado mejoras en la seguridad de TI. (itReseller, 2023)

Diversos estudios de PwC concluyen con que este 2024, Pymes y grandes empresas aumentarán hasta un 14% su gasto en ciberseguridad, valor que tomamos como variable en el análisis de costes antes. (itReseller, 2023)

7.1.2 OBJETIVOS CUBIERTOS

En primer lugar, se ha explicado lo que constituye un ciberataque, cuáles son las causas, efectos y el problema que esto supone. Y se ha profundizado en el análisis de las razones que posicionan al sector de la energía como el más vulnerable ante ciberataques.

Además, se han analizado estadísticas y datos concernientes al volumen de ciberataques en el parque eólico de Tahivilla "El Cortijo de Iruelas", proporcionando una visión cuantitativa del problema, es decir, se ha conseguido evaluar el impacto económico y social que tendría el parque eólico en caso de un ciberataque.

Asimismo, se han abordado las medidas estratégicas destinadas a reducir la incidencia de estos ataques, contribuyendo así a fortalecer la ciberseguridad de dicho parque eólico.

Todos estos objetivos se han conseguido con el desarrollo de una metodología basada en la búsqueda de información de la ciberseguridad, tipo de ciberataques, recorrido a lo largo de la historia, ciberataques más famosos, impacto en la sociedad. Recopilación de información de los parques eólicos, su funcionamiento, generación, producción y desarrollo de la energía. Además de su estudio de los distintos parques eólicos de Tarifa para su posterior análisis.

Se ha realizado también una profundización en el parque eólico, en este caso, "El Cortijo de Iruelas", funcionamiento, generación, desarrollo de la energía, localización, situación actual, acompañado de su consiguiente cálculo de los distintos costes del parque eólico, en función de la ciberseguridad
Se han aportado medidas y un plan de acción del parque eólico, además de estudiar los riesgos y amenazas del sector.

En los últimos capítulos del proyecto se han desarrollado las consecuencias de una posible amenaza/ataque y repercusiones económicas y sociales. Al igual que futuros trabajos y recomendaciones planteadas para la consecución del objetivo final.

Capítulo 8. BIBLIOGRAFÍA

AAE. (2011). *Guía Técnica de Energía Eólica*

Acciona, 2024 https:Proy. Repot. PE Cortijo I. acciona.pdf

Albán Guerrero, J. E., & Paguay Llamuca, N. J. (2017). *Diseño e implementación de un sistema SCADA con comunicación PROFIBUS para el control y monitoreo de procesos industriales en el laboratorio de automatización de la Facultad de Mecánica* (Bachelor's thesis, Escuela Superior Politécnica de Chimborazo)

Alonso Martínez, M., Amarís Duarte, H. E., Pastrana Portillo, S., Turanzas, J., Gálvez, L., & Ledo, A. T. (2020). Retos en materia de ciberseguridad en smart grids.

Arteaga, F. (2019). Ciberseguridad y seguridad integral en el sector energético. Real Instituto Elcano, 9(7).

Atvise SCADA, 2022 https: SCADA Software for Industry 4.0 - First HMI SCADA Web | atvise (vesterbusiness.com)

Bailey, D., & Wright, E. (2003). *Practical SCADA for industry*. Elsevier

Calzada, J. S. H. (2021). CIBERSEGURIDAD EN LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS ELÉCTRICAS. Telemática, 20(1), 36-46.

Cerrada, M., Cardillo, J., y Prada, A. (2011). Diagnóstico de fallas basado en modelos: Una solución factible para el desarrollo de aplicaciones SCADA en tiempo real. *Ciencia e ingeniería*, *32*(3), 163-172.

Centeno, F. J. U. (2015). CIBERATAQUES, la mayor amenaza actual. Prebie3, (1), 42.

Chen, Thomas. Stuxnet, the real start of cyber warfare? [Editor's Note].Network, IEEE 24.6 (2010): 2-3.

Computerworld España, 2023 https: "En 2023 continuará el aumento de las inversiones para integrar completamente la ciberseguridad y la tecnología" | Computerworld.es

Diario de Cádiz, 2023 https: ¿Cuántos parques eólicos hay en Cádiz y qué cantidad de energía producen? (diariodecadiz.es)

Dir&ge, 2022 https: La inversión media de las empresas en ciberseguridad alcanzará en España un 7,7% durante 2022 (directivosygerentes.es)

DWI Association. (2003). Danish Wind Industry Association'. *línea] http://xn--drmstrre-64ad. dk/wpcontent/wind/miller/windpower\% 20web/es/tour/wres/park. htm.[Último acceso: Enero 2018]*.

El Español, 2024 https: Acciona Energía repotencia un 72% su planta de Tarifa (Cádiz) y pasa a 254 GWh anuales (elespanol.com)

Eólico, A. A. E. E. A. (2019). La voz del Sector.

Europa Sur, 2024 https: https://www.europasur.es/tarifa/Acciona-parque-eolico-tahivilla-turbinas_0_1906910623.html

Fernández Sánchez, Á. (2015). Evaluación técnico-económica de un parque eólico.

Gómez, D., Baeyens, E., Cárdenas, C., & Moya, E. J. (2011). Supervisión de sistemas lógicos de control utilizando el diagrama de evolución del estado. *Revista Iberoamericana de Automática e Informática Industrial RIAI*, *8*(3), 196-203.

Gómez, J., Reyes, R., & Guzmán del Río, D. (2008). Temas especiales de instrumentación y control. *Cuba: Editorial Félix Varela*.

Iberdrola, 2023 https: Funcionamiento de los parques eólicos terrestres - Iberdrola - Iberdrola

IBM, 2024 https: https://www.ibm.com/es-es/topics/cyber-attack

INCIBE, (2020). *Guía de Ciberataques*

INCIBE, 2024 https: Estudio del análisis de malware en SCI: BlackEnergy (incibe.es)

Interempresas, 2024 https:El sector energético fue el más ciberatacado en España en el último año (interempresas.net)

itReseller, 2023 https: Pymes y grandes empresas aumentarán hasta un 14% su gasto en ciberseguridad | Seguridad | IT Reseller

Ismael de la Cruz, 2024 https: Qué es un fondo de inversión y cómo funciona - Investing.com

Lella, I., Ciobanu, C., Tsekmezoglou, E., Theocharidou, M., Magonara, E., Malatras, A., & Svetozarov Naydenov, R. (2023). ENISA threat landscape 2023: July 2022 to June 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape2023/@@download/fullReport

MADE-ENDESA, 2018 https: https://www.sotaventogalicia.com/recursos/custom/area_tecnica/instalacions_eolicas/caracteristicas_maquinas/esp/docs/doc_006.pdf

mrHoutson, 2021. https: Los 10 ciberataques más importantes de la historia - Mr. Houston Tech Solutions (mrhouston.net)

NVTec, 2022 https: (nvtecnologias.com)

Plan recuperación Gobierno. https: Conoce las ayudas de la iniciativa 'Activa Ciberseguridad' para pymes | Plan de Recuperación, Transformación y Resiliencia Gobierno de España. (planderecuperacion.gob.es)

Renewable Press, 2021 https: Nordex announces entry into the 6 MW class with the N163/6.X turbine - renewablepress

Sophos (2021). *El estado del ransomware en el sector de los servicios financieros 2021*

Zuluaga, D. (2020). Ciberseguridad para la operación centralizada y distribuida de generación de energía eléctrica en ISAGEN. Ingeniería y Ciencia, 16(32), 171-194. https://publicaciones.eafit.edu.co/index.php/ingciencia/article/download/6282/5066/2260

ANEXO I: ODS

Objetivos de Desarrollo Sostenible (ODS) de Naciones Unidas

Hemos de tener en cuenta que los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas no abordan de una manera tan directa el número de ciberataques del sector energético industrial. No obstante, se pueden identificar algunos ODS que guardan alguna relación. La relación entre los ODS y los ciberataques en la sociedad española varía y depende de cada análisis realizado. Sin embargo, algunos de los ODS que podrían estar relacionados son:

ODS 7: Energía asequible y no contaminante

La gran cantidad de número de ciberataques pueden llegar a afectar la disponibilidad y confiabilidad de las infraestructuras energéticas, comprometiendo de esta manera el suministro de energía sostenible.

ODS 9: Industria, innovación e infraestructura

Para la protección y para garantizar la seguridad en el sector industrial, la ciberseguridad es de gran importancia.

ODS 11: Ciudades y comunidades sostenibles.

ODS 16: Paz, justicia e instituciones sólidas

Para mantener la paz y estabilidad en el sector energético, es necesario garantizar la ciberseguridad.

ODS 17: Alianzas para lograr los objetivos

Es importante abordar los temas relacionados con los ciberataques y ciberseguridad con máxima cooperación entre países.