UNIVERSIDAD MIGUEL HERNÁNDEZ DE ELCHE

Facultad de Ciencias Sociales y Jurídicas de Elche

DOBLE GRADO EN DERECHO Y ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

Trabajo de Fin de Grado

Curso Académico: 2022/2023

LA CIBERSEGURIDAD EN EL TRANSPORTE Y LA LOGÍSTICA.

Alumno: Sofía Esclapez Ferrández

Tutor: Ramón Miralles Soler

ÍNDICE

ÍNDICE ILUSTRACIONES

ÍNDICE GRÁFICOS

ÍNDICE FIGURAS

1. INTRODUCCIÓN.

La ciberseguridad se ha convertido en una herramienta muy importante en el sector del transporte y la logística debido al creciente uso de tecnologías innovadoras y la necesidad de utilizar sistemas informáticos en las empresas. Los ciberataques cada vez tienen un nivel de sofisticación mayor y se producen con mayor frecuencia, esto puede tener graves consecuencias para las empresas que no estén preparadas o no tengan los recursos suficientes para hacer frente a este tipo de ataques. Por lo tanto, es fundamental comprender la importancia de la ciberseguridad en este sector y tomar medidas adecuadas para proteger los sistemas y la información perteneciente a la empresa.

La finalidad de la ciberseguridad es asegurar la confidencialidad, integridad y disponibilidad de la información digital, y proteger tanto los sistemas como las redes contra accesos no autorizados y ataques malintencionados.

Este trabajo de fin de grado tiene como objetivo exponer la importancia de la ciberseguridad en un sector tan importante y amplio como el transporte y la logística, los diversos riesgos que puede ocasionar el no implementar medidas efectivas, los principales ataques que puede sufrir una empresa, así como la vulnerabilidad de las PYMES ante los ciberataques y las posibles soluciones para garantizar la seguridad de la empresa. Por tanto, se pretende proporcionar una visión completa sobre la importancia de la ciberseguridad en el sector.

2. RESUMEN.

El presente Trabajo de Fin de Grado tiene como objetivo analizar la importancia de la ciberseguridad en el transporte y la logística. Para ello, se ha definido qué es la ciberseguridad y se han identificado los principales ataques existentes, como el virus informático, *ransomware*, *phishing* o suplantación de identidad y la denegación de servicio.

Además, se ha analizado el papel del Instituto Nacional de Ciberseguridad (INCIBE) en la lucha contra los ciberataques y se ha estudiado las consecuencias que tienen los ataques en el sector del transporte y la logística, tales como la pérdida de datos, la pérdida económica, la paralización de la actividad empresarial y la pérdida de reputación.

Por último, se ha destacado la vulnerabilidad de las PYMES ante los ciberataques y se ha propuesto una serie de medidas que se pueden llevar a cabo para implantar la ciberseguridad en el sector. En conclusión, se ha puesto de manifiesto la necesidad de prestar atención a la ciberseguridad en el sector y se han presentado soluciones para minimizar el impacto de los ciberataques en la actividad empresarial.

Palabras clave: Ciberseguridad, transporte, logística, PYMES.

3. ABSTRACT.

The aim of this Degree Final Project is to analyse the importance of cybersecurity in transportation and logistics. To do so, the concept of cybersecurity has been defined and the main existing attacks have been identified, such as computer viruses, ransomware, phishing or identity theft and denial of service.

Additionally, the role of the National Cybersecurity Institute (INCIBE) in the fight against cyberattacks has been analyzed and the consequences of attacks on the transportation and logistics sector have been studied, such as data loss, economic loss, business activity shutdown, and reputational damage.

Finally, the vulnerability of SEMs to cyberattacks has been highlighted and a set of measures to implement cybersecurity in the sector has been proposed. In conclusion, the need to pay attention to cybersecurity in the sector has been spotlighted and solutions to minimize the impact of cyberattacks on business activity have been presented.

Key words: Cybersecurity, transportation, logistics, SEMs.

4. LA CIBERSEGURIDAD EN EL TRANSPORTE Y LA LOGÍSTICA.

4.1. ¿Qué es la ciberseguridad en el transporte y la logística?

La ciberseguridad es la protección de los sistemas informáticos, dispositivos electrónicos, redes, datos e información digital contra amenazas, vulnerabilidades y ataques malintencionados, esta incluye medidas técnicas, organizativas y legales para prevenir y proteger contra ataques cibernéticos, incluyendo virus, *malware, phishing,* ataques de denegación de servicio, robo de datos y otros tipos de amenazas.

El objetivo de la ciberseguridad es garantizar la confidencialidad, la integridad y la disponibilidad de la información digital, proteger tanto los sistemas como redes contra accesos no autorizados y ataques malintencionados.

La protección que brinda la ciberseguridad es crítica en la era digital, ya que los sistemas y la información digital son esenciales para la mayoría de las organizaciones, empresas e individuos. Cuando se realiza una adecuada implantación de la ciberseguridad permite proteger los activos digitales, garantizar la continuidad de los negocios y la privacidad de la información personal.

Ilustración 1: La ciberseguridad en el transporte y la logística.

Fuente: MUYPYMES

Además, la ciberseguridad posee un papel fundamental en el sector de la logística, tanto para las actividades y procesos que son necesarios para planificar, implementar y control los flujos de bienes, servicios e información desde su origen hasta el destino final.

La logística tiene como objetivo principal satisfacer las necesidades del cliente al tiempo que se optimiza la eficiencia y la rentabilidad. Dentro de las actividades de la logística se incluyen la planificación de la demanda, la gestión de la cadena de suministro, el transporte, el almacenamiento, la distribución y la gestión de la información.

El sector de la logística es crítico para la economía global, ya que permite a las empresas mover productos y servicios a nivel nacional e internacional, facilitando el comercio y el crecimiento económico. La logística también es importante a fin de garantizar la disponibilidad de bienes y servicios para los consumidores y con el objetivo de mejorar la eficiencia y la rentabilidad de las empresas.

En resumen, el sector de la logística hace referencia a las actividades y procesos necesarios para planificar, implementar y controlar el flujo de bienes, servicios e información desde su origen hasta su destino final, con el objetivo de satisfacer las necesidades del cliente y optimizar la eficiencia y la rentabilidad.

Por tanto, se podría establecer, enlazando ambos conceptos, que la ciberseguridad en el sector de la logística se refiere a los esfuerzos para proteger los sistemas tecnológicos, la información y los datos relacionados con la logística de posibles ataques cibernéticos. Esto incluye medidas de seguridad como la encriptación de datos sensibles, la autentificación de usuarios y la implementación de políticas de seguridad sólidas para prevenir intrusiones y garantizar la integridad de los sistemas y datos logísticos.

La ciberseguridad es esencial en el sector de la logística, ya que una brecha de seguridad puede tener graves consecuencias, como puede ser la perdida de datos confidenciales o la o interrupción del flujo de suministros.

4.2. Impacto de la ciberseguridad en el transporte y la logística.

La protección de los sistemas informáticos, dispositivos electrónicos, redes, etc. mediante la ciberseguridad, tiene un impacto significativo en el transporte y la logística, ya que ambos sectores dependen cada vez más de las tecnologías de la información y la comunicación (TIC) para su funcionamiento eficiente.

De hecho, "España se posicionó en 2022 como el tercer país a nivel mundial en materia de ciberataques. Así se advierte en un reciente estudio publicado por Deloitte en el que se pone de manifiesto que el 94% de las empresas españolas ha sufrido al menos un incidente grave en materia de ciberseguridad en el último año" (González, 2023).

Enfocándonos en el sector de la logística y el transporte, "la organización sectorial UNO estima que más del 20 % de las empresas del sector en España han sufrido infecciones por virus informáticos en el último año; el 10 % se han visto expuestas a secuestros de datos o brechas de ciberseguridad; y el 8 % han sido víctimas de intentos de fraude electrónico" (Controla Plus, 2022).

Algunos de los impactos más relevantes en los que se puede incurrir debido a estos ataques incluyen:

- Vulnerabilidad a ataques cibernéticos: La infraestructuras y sistemas de transporte y logística están expuestos a una amplia gama de amenazas cibernéticas, como virus informáticos, ataques de denegación de servicio, robo de datos, entre otros.

- Interrupción del servicio: Una brecha de seguridad puede tener un impacto negativo en la disponibilidad de servicios críticos, como sistemas de seguimiento de envíos, gestión de inventario, etc.

- Pérdida de confianza: Los clientes y proveedores pueden perder confianza en la capacidad de una empresa para proteger sus datos sensibles y operar de manera segura.

- Costes elevados: Las consecuencias económicas de un incidente de seguridad cibernética, como la respuesta a un ataque y la recuperación de datos, puede ser significativas y muy elevadas.

- Regulaciones cada vez más estrictas: Cada vez más regulaciones y requisitos de seguridad cibernética que las empresas de transporte y logística deben cumplir, lo que puede aumentar sus costes operativos.

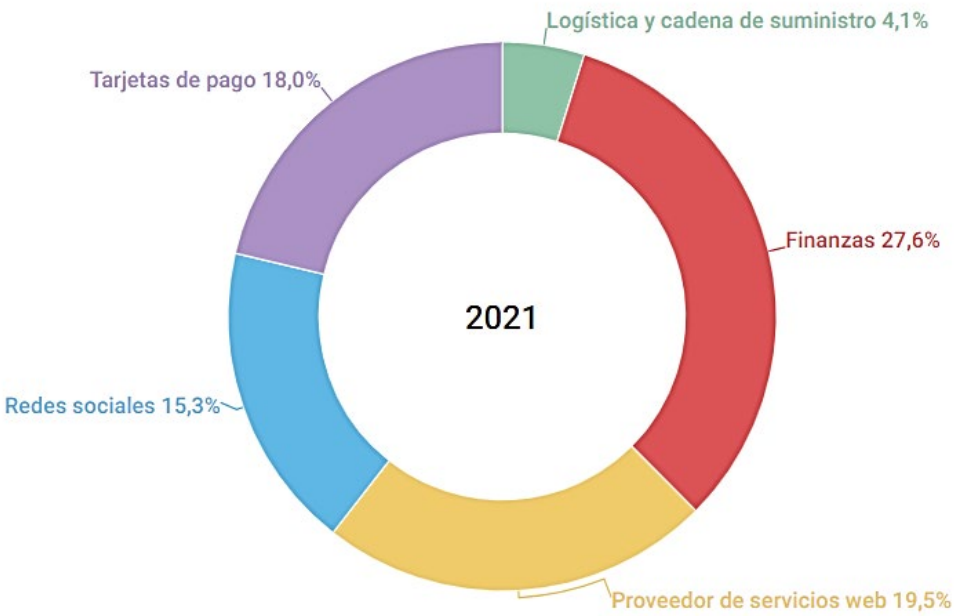
Por estas razones, es importante que las empresas en el sector del transporte y la logística tomen medidas proactivas para proteger sus sistemas y datos de las amenazas cibernéticas.

“Solo hay tres formas de reducir los ataques a través de la disuasión: Primero, invirtiendo en formación de ciberseguridad de todos los empleados. Segundo, mediante el aumento de la contratación de servicios de ciberseguridad y software de protección. Y, tercero, mediante la educación de los usuarios y clientes en ciberseguridad” (Liñán I. , 2023).

A continuación, encontramos, en el gráfico 1, una exposición sobre el porcentaje total de los ciberataques que se produjeron en el año 2021 en algunos de los diferentes sectores.

Como podemos observar uno de los sectores más afectado por este tipo de ataques es el sector financiero con un porcentaje del 27,6% del total, siendo el sector de la logística el de menor porcentaje con un 4,1%.

Gráfico 1: Porcentaje sobre el total de ciberataques por sector (2021)

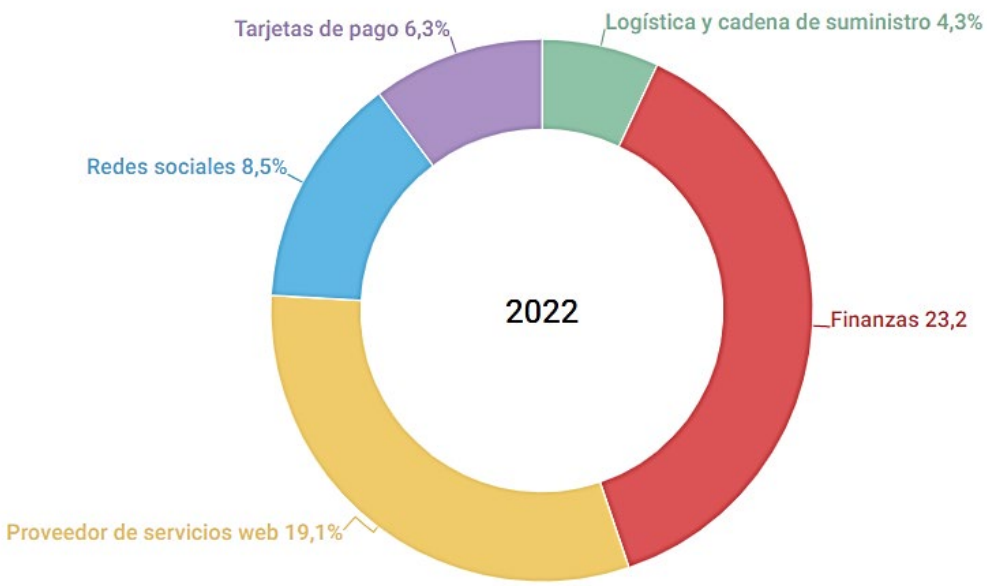


Fuente: el mercantil[1].

En el gráfico 2, que se expone a continuación, observamos cómo el sector de la logística ha visto incrementado el número de ataques en un 0,2%, pasando del 4,1% del año 2021 al 4,3% en el año 2022. El gráfico refleja a su vez el descenso del sector de las finanzas en un 4,4% en el año 2022, también podemos ver una disminución importante tanto en el sector de redes sociales como el de tarjetas de pago en un 6,8% y un 9% respectivamente. A su vez observamos que se han reducido del año 2021 al 2022 el porcentaje de ataques en el sector de proveedor de servicio web en un 0,4%. Por otro lado, cabe destacar que el único sector, de los que se exponen en los gráficos anteriores, que ha visto incrementado su porcentaje de ataques del año 2021 al año 2022 es el sector de la logística y cadena de suministro. Hay que remarcar que aun siendo el sector que ha visto incrementado el porcentaje de ataques del año 2021 al año 2022, sigue siendo el sector con menor porcentaje.

[1] https://acortar.link/9SKFxA

Gráfico 2: Porcentaje sobre el total de ciberataques por sector (2022)



Fuente: el mercantil[2].

"El sector español de logística y cadena de suministro dedica el 12,6% de su presupuesto anual a la ciberseguridad, siendo el país que más invierte en este tipo de tecnologías, 4 décimas por encima de la media de las compañías logísticas" (Cuadernos de Seguridad, 2019).

[2] https://acortar.link/9SKFxA

4.3. ¿Cómo implantar la ciberseguridad en el transporte y la logística?

En la actualidad, la ciberseguridad es un factor crítico para la gestión exitosa de la logística en las empresas, ya que su impacto en la competitividad es innegable. En un mundo cada vez mas digitalizado, las organizaciones deben asegurarse de que sus sistemas y datos estén protegidos de posibles ataques que puedan comprometer la integridad y confidencialidad de la información.

Es por ello que se ha convertido en un punto clave en la estrategia de digitalización de la logística de muchas compañías. La implantación de medidas de seguridad eficaces no solo garantiza el cumplimiento de las regulaciones en materia de privacidad y protección de datos, sino que también contribuye a la eficiencia en la gestión de la cadena de suministro.

En este sentido, la ciberseguridad se vuelve especialmente relevante para las empresas que manejan grandes volúmenes de información y procesos logísticos.

A pesar de que en materia de ciberseguridad existe continuamente riesgo, para implementar la ciberseguridad en el transporte y la logística, se debe tener en cuenta los siguientes pasos:

- Identificación de amenazas: En primer lugar, debemos evaluar los riesgos y amenazas cibernéticas específicas para el transporte y la logística.

- Planificación de la seguridad: Desarrollar un plan de seguridad cibernética que abarque la gestión de activos, acceso, autentificación y autorización, monitoreo y respaldo.

- Fortalecimiento de las defensas: Implementar medidas de seguridad técnicas, como *firewalls*, encriptación, detección y prevención de intrusiones y monitoreo de amenazas en tiempo real.

- Captación y sensibilización: Asegurarse de que todos los empleados estén capacitados en temas de ciberseguridad y sepan cómo detectar y responder a incidentes de seguridad.

- Pruebas y evaluaciones regulares: Las empresas deben realizar pruebas regulares de penetración y evaluaciones de seguridad para detectar vulnerabilidades y fortalecer la defensa.

- Monitoreo continuo y respaldo: Monitorear continuamente la actividad cibernética y tener un plan de respaldo para recuperarse de un ataque exitoso.

Estos pasos pueden ayudar a mitigar los riesgos cibernéticos y proteger el transporte y la logística contra posibles ataques cibernéticos.

El estudio realizado por la Agencia de la Unión Europea para la ciberseguridad (Enisa) “reporta que entre el 39% y el 62% de las empresas en Europa sufrieron ciberataques por parte de terceros y que los actores de la cadena logística fueron el segundo sector más atacado en 2021. Según la agencia europea, el sector pasó de reportar menos del 1% de intrusiones en 2020 al 17% al año siguiente” (Liñán I. , 2023).

5. INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE).

El Instituto Nacional de Ciberseguridad (INCIBE) es una entidad pública empresarial española encargada de promover y garantizar la seguridad en el uso de las tecnologías de la información y la comunicación (TIC) en el territorio nacional. Entre sus funciones destacan la formación y sensibilización en materia de ciberseguridad, la investigación y el desarrollo de soluciones y servicios de seguridad, y la asesoría y atención a incidentes de seguridad cibernética. Entre sus principales actividades podemos encontrar: la formación y sensibilización en materia de ciberseguridad, la investigación y el desarrollo de soluciones y servicios de seguridad, la asesoría y atención a incidentes de seguridad cibernética, y, por último, la colaboración con organizaciones y entidades en la prevención y respuesta a amenazas cibernéticas.

Ilustración 2: Logo INCIBE

Fuente: Incibe

El Objetivo general del INCIBE es mejorar la seguridad de la información y de las infraestructuras críticas en el entorno digital en España.

“INCIBE trabaja para afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España” (INCIBE, 2016).

Por ello, el INCIBE se utiliza para:

- Mejorar la seguridad en el uso de las TIC en España: El INCIBE trabaja para aumentar la conciencia y la capacidad de las organizaciones y personas en materia de ciberseguridad.

- Prevenir y responder a incidentes de seguridad cibernéticas: El INCIBE brinda asesoramiento y apoyo a las organizaciones y personas en materia de ciberseguridad.

- Investigar y desarrollar soluciones de seguridad cibernética: El INCIBE lleva a cabo investigaciones y desarrolla soluciones de seguridad cibernética para mejorar la seguridad de las infraestructuras críticas en el entorno digital.

- Formación y capacitación en ciberseguridad: El INCIBE ofrece programas de formación y capacitación en ciberseguridad para mejorar la capacidad de las personas y las organizaciones en este ámbito.

- Fomentar la cooperación entre entidades en materia de ciberseguridad: El INCIBE fomenta la cooperación entre entidades gubernamentales, empresariales y de investigación en materia de ciberseguridad para mejorar la protección de las tecnologías de la información y la comunicación (TIC) en España.

El INCIBE-CERT es el Centro de Respuesta a Incidentes de Seguridad Cibernética del INCIBE. Es un centro de atención y respuesta a incidentes cibernéticos que trabaja para proteger a las organizaciones y ciudadanos españoles contra las amenazas cibernéticas. Este se encarga de analizar y responder a incidentes de seguridad cibernética, coordinando la respuesta con otras organizaciones nacionales e internacionales, y proporcionando asistencia técnica a las víctimas. Además, también trabaja en la prevención de incidentes cibernéticos a través de la sensibilización y la formación en ciberseguridad.

Algunas de las funciones y responsabilidades del INCIBE-CERT incluyen:

- Monitorear y analizar las amenazas cibernéticas en tiempo real.

- Proporcionar asesoramiento y recomendaciones para prevenir incidentes de seguridad cibernética.

- Coordinar la respuesta a incidentes de seguridad cibernética a nivel nacional e internacional.

- Investigar y analizar las brechas de seguridad y proporcionar informes y estadísticas sobre incidentes de seguridad cibernética.

- Ofrecer capacitación y formación en ciberseguridad a las organizaciones.

En resumen, el INCIBE-CERT es un componente clave de la estrategia nacional de ciberseguridad en España, trabajando para garantizar la seguridad y protección contra las amenazas cibernéticas.

Su misión es mejorar la seguridad en el uso de las tecnologías de la información y la comunicación (TIC) en España y proteger las infraestructuras críticas y los sistemas de información del país contra las amenazas cibernéticas. Para ello, el INCIBE trabaja en las siguientes áreas:

- Concienciación y capacitación: tiene como objetivo aumentar la conciencia y la capacidad de las organizaciones y personas en materia de ciberseguridad.

- Prevención y respuesta a incidentes: brinda asesoramiento y apoyo a las organizaciones en la prevención y respuesta a incidentes de seguridad cibernética.

- Investigación y desarrollo: lleva a cabo investigaciones y desarrolla soluciones de seguridad cibernética para mejorar la seguridad de las infraestructuras críticas en el entorno digital.

- Cooperación: fomenta la cooperación entre entidades gubernamentales, empresariales y de investigación en materia de ciberseguridad para mejorar la protección de las tecnologías de la información y la comunicación (TIC) en España.

En cuanto a su visión, el INCIBE trata de ser un referente en ciberseguridad a nivel nacional e internacional, contribuyendo a crear un entorno seguro en el uso de las TIC en España.

Para alcanzar esta visión, trabaja en estrecha colaboración con entidades gubernamentales, empresariales y de investigación, aplicando soluciones innovadoras y eficaces para prevenir y responder a las amenazas cibernéticas, también busca sensibilizar a la sociedad sobre la importancia de la ciberseguridad y promover la formación y el conocimiento en materia de seguridad en el entorno digital. Se podría decir que su visión es ser un líder en ciberseguridad en España, contribuyendo a la creación de un entorno digital seguro para las personas, las organizaciones y las infraestructuras críticas.

Por lo que respecta a sus valores, que son fijados por el Consejo de Administración, estos valores orientan su trabajo y comportamiento, y reflejan su compromiso con la misión y visión de la organización. Estos valores incluyen:

1. Vocación de servicio público: el compromiso con el bienestar y la seguridad de la sociedad española.

2. Espíritu neutral y colaborativo: el compromiso de la entidad INCIBE con la colaboración y la neutralidad en su trabajo.

3. Proactividad y flexibilidad: la capacidad para anticiparse a los cambios y adaptarse rápidamente a las nuevas demandas y desafíos.

4. Excelencia: el compromiso con el desempeño de alta calidad en todo lo que hace.

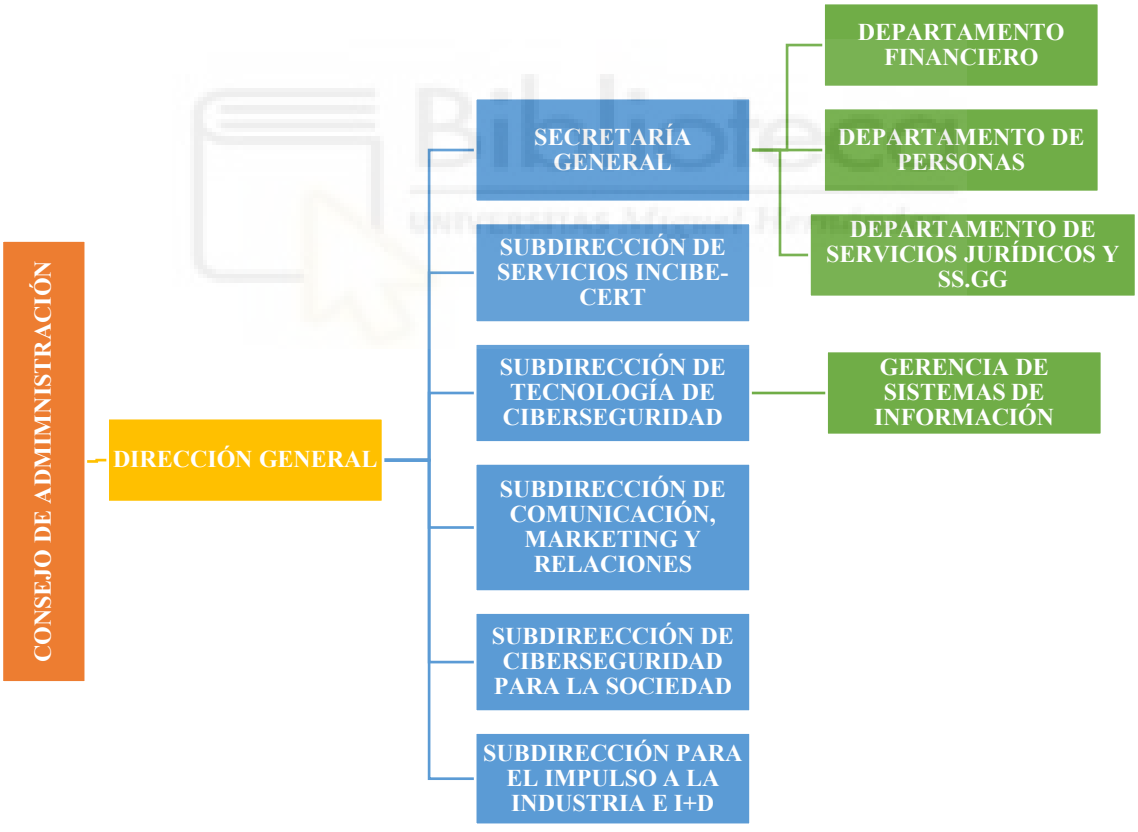
5. Innovación: la dedicación a la innovación y la búsqueda de soluciones innovadoras para los desafíos de la ciberseguridad.

6. Desempeño nacional e internacional: la transparencia y responsabilidad en el desempeño de las tareas y funciones de INCIBE.

7. Colaboración nacional e internacional: la importancia de la colaboración y coordinación con organizaciones nacionales e internacionales para lograr los objetivos de la organización.

En cuanto a la estructura jerárquica, la encontramos plasmada en el siguiente organigrama.

Figura 1: Organigrama INCIBE.



Fuente: elaboración propia[3].

[3] https://www.incibe.es/que-es-incibe/organigrama

En primer lugar, tenemos el consejo de administración, el cual está compuesto por diez consejeros, de los cuales seis son vocales. El consejo de administración se encuentra presidido por Dª. Carme Artigas Brugal, que a su vez es secretaria de Estado de Digitalización e Inteligencia Artificial, Vicepresidencia Primera del Gobierno y Ministerio de Asuntos Económicos y Transformación Digital. Por otra parte, tenemos a D. Alberto Martínez Lacambra que es el vicepresidente del INCIBE y además director general de la Entidad Pública Empresarial Red.es.

En segundo lugar, tenemos al director general, que es Félix Barrio Juárez "experto Universitario en Dirección y Gestión de la Información y Tecnologías por la Universidad de Alcalá y doctor por la Universidad de Salamanca. Asimismo, es gerente de Ciberseguridad CISM por ISACA. Ha sido miembro del Board of Directors de la European Cyber Security Organization (ECSO), y presidente del Subcomité de Tecnologías de Ciberseguridad-UNE" (INCIBE, 2020).

En tercer lugar, tenemos a la secretaria general y a sus diferentes subdirecciones. El cargo de la secretaría general lo ostenta Carla Redondo Galbarriatu, "es Licenciada en Derecho y Diplomada en Ciencias Económicas por la Universidad de Deusto y tiene más de 7 años de experiencia en la materia. Forma parte del Cuerpo Superior de la Administración Civiles del Estado y ha desempeñado funciones para el Ministerio de Defensa, como Técnico Superior en la Subdirección de Personal Militar" (INCIBE, 2022).

Por último, de la secretaría general dependen tres departamentos, el financiero, de personas y el de servicios jurídicos y SS.GG.

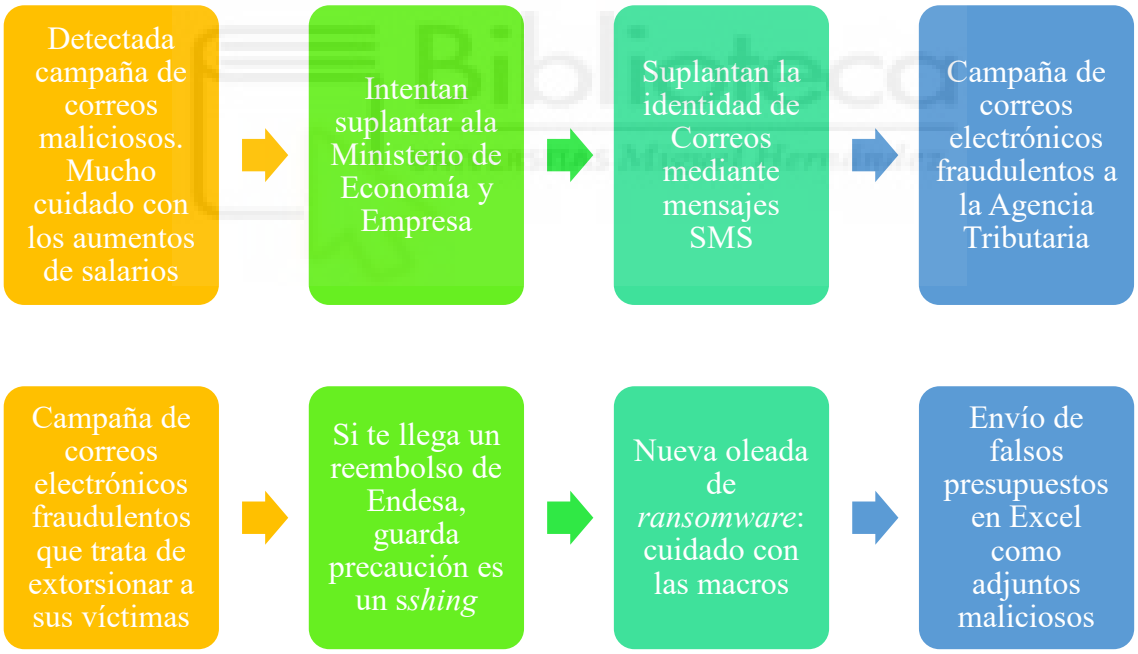
La tecnología que utilizan las diferentes empresas del sector depende en su mayor parte de su propia actividad, por tanto, las empresas están expuestas a distintos riesgos en función de su sector. Por ello SECtoriza2 aproxima pautas y recomendaciones concretas para sectores determinados y que así las empresas puedan anticiparse.

SECtoriza2 es una solución de ciberseguridad especifica para el sector logístico. Este sector es un componente crítico de la economía global, encargado de la entrega

eficiente y oportuna de bienes y servicios. Con el uso creciente de la tecnología en la industria, es importante garantizar la seguridad de los datos y la información sensibles para evitar posibles violaciones de seguridad y proteger la integridad de la información y los sistemas de la empresa. SECtoriza2 se enfoca en brindar una protección completa para el sector logístico, para asegurar la continuidad del negocio y mantener la confianza de los clientes.

Las principales amenazas que afectan a las asociaciones tienen su origen en el correo electrónico. El siguiente recopilatorio de avisos de seguridad se trata de ejemplos de ataques más comunes que sufre el sector de la logística:

Figura 2: Avisos de seguridad.



Fuente: elaboración propia[4].

[4] https://www.incibe.es/sites/default/files/contenidos/SECtoriza2/logistica.pdf

6. CIBERATAQUES MÁS HABITUALES EN EL SECTOR.

Un ciberataque es un intento malintencionado de dañar, alterar, robar o acceder ilegalmente a un sistema informático o a la información que se encuentra almacenada en él. Los ciberataques pueden ser perpetrados por individuos, grupos o incluso gobiernos, y pueden tener como objetivo una amplia variedad de objetivos, incluyendo:

- Robo de información confidencial: En el cual los atacantes pueden tratar de obtener acceso a información confidencial, como contraseñas, información de cuentas bancarias o de tarjetas de crédito, propiedad intelectual o secretos comerciales.

- Interrupción de servicios: Para este tipo de ciberataque, los atacantes pueden intentar interrumpir o paralizar servicios críticos de una organización o gobierno, como por ejemplo sistemas de energía, servicios de emergencia, servicios financieros, entre otros.

- Manipulación de datos: Los atacantes pueden alterar o destruir datos almacenados en sistemas informáticos, lo que puede tener consecuencias graves, como la pérdida de datos críticos o la alteración de información en sistemas de control.

- Suplantación de identidad o *phishing*: Los ciberdelincuentes pueden utilizar técnicas de *phishing* o *malware* para obtener acceso a información confidencial o para suplantar la identidad de una persona o empresa.

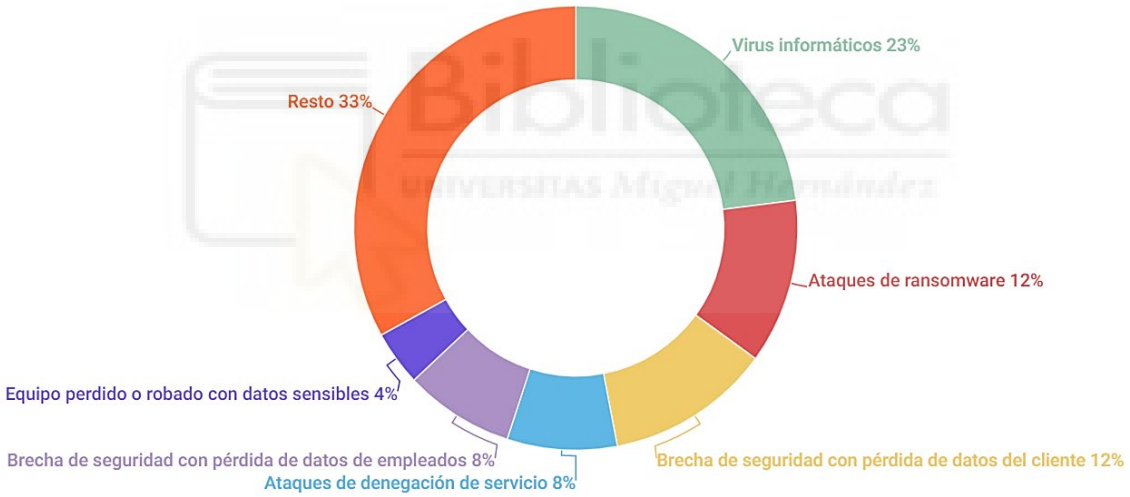
- *Malware*: Los ciberatacantes pueden usar *malware* (software malicioso) para infectar sistemas informáticos con el objetivo de dañar, controlar o robar información.

En resumen, cualquier acción que tenga como objetivo causar daño, alterar o robar información de un sistema informático se puede considerar un ciberataque.

En general, es importante que las empresas del sector de la logística y el transporte implementen medidas de seguridad efectivas para prevenir los virus informáticos y otros tipos de ciberataques. Esto incluye mantener los sistemas de software y hardware actualizados, utilizar programas antivirus y firewalls, realizar copias de seguridad regularmente y educar a los empleados sobre las prácticas seguras de seguridad cibernética.

"Se estima que, más del 8% de las empresas del sector de la logística y el transporte se han visto afectadas por este tipo de ciberataques" (UNO logística, 2020)

Gráfico 3: Tipos de ataques informáticos a las empresas españolas de logística y transporte (2019).



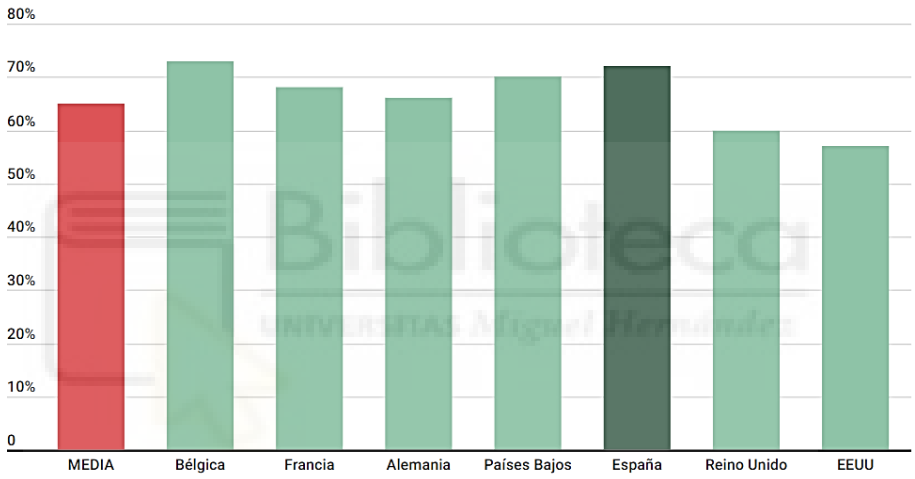
Fuente: El mercantil[5]

En el gráfico anterior, se exponen los tipos de ataques informáticos que se han producido en las empresas españolas dedicadas al sector de la logística y el transporte. Debemos destacar que el ataque más habitual es el que se produce mediante virus informático, que se trata de un tipo de programa malicioso (*malware*) que tiene la capacidad de replicarse a sí mismo y propagarse a otros archivos y

[5] https://acortar.link/aQD71i

sistemas informáticos sin el conocimiento o el consentimiento del usuario, este tipo de ataque representa un 23% del total. En segunda posición encontramos dos tipos de ataques, los ataques de *Ransomware* y los ataques de brecha de seguridad con pérdida de datos de los clientes, ambos con un 12%. En tercer lugar, tenemos, tanto ataques de denegación de servicio como brecha de seguridad con pérdida de datos de empleados, los dos ataques con un 8%. Y en último lugar, el equipo perdido o robado con datos sensibles, el cual representa un 4% del total.

Gráfico 4: Empresas que han sufrido ataques cibernéticos en su cadena de suministro (2019).



Fuente: El mercantil[6]

Por lo que respecta al gráfico 4, representa el porcentaje de empresas que han sido atacadas cibernéticamente en los diferentes países. Como podemos observar, el 72% de las empresas españolas se han visto afectadas, esto sitúa a los ataques producidos a empresas españolas, 5 puntos por encima de la media que surge de analizar los países expuestos en el gráfico. Al igual que España, Bélgica es otro de los países más afectados con un 72%, seguido de Países Bajos con un 70%, Francia con un 68%, Alemania con un 66%, Reino Unido un 60% y, por último, con el menor porcentaje, Estados Unidos, con un porcentaje del 57%. “El coste medio de los

[6] https://acortar.link/aQD71i

ciberincidentes a empresas de logística y transporte de los países objeto del estudio de Hiscox ascendió a 530.000 dólares en 2019, muy por encima de los 157.000 dólares registrados en 2018" (Liñán J. C., 2019).

En los siguientes apartados pasaremos a explicar en profundidad los ciberataques que son más comunes en el sector de la logística y del transporte.

6.1. Virus informático.

En primer lugar, nos encontramos con los virus informáticos que se trata de un tipo de programa malicioso (*malware*) que tiene la capacidad de replicarse a sí mismo y propagarse a otros archivos y sistemas informáticos sin el conocimiento o el consentimiento del usuario. Los virus informáticos suelen ser diseñados para causar daño o alterar el funcionamiento normal de un sistema informático.

Los virus informáticos pueden infectar cualquier tipo de archivo ejecutable, incluyendo documentos de texto, imágenes y programas. Una vez que un archivo se infecta con un virus, el virus puede propagarse a otros archivos del sistema y a otros sistemas conectados a la red.

"Se estima que, más del 20% de las empresas del sector de la logística y el transporte, han sido infectadas por algún tipo de virus informático en los últimos meses de 2020" (UNO logística, 2020).

Algunos ejemplos de los efectos dañinos que pueden causar los virus informáticos incluyen:

- Borrar o corromper archivos y datos importantes del usuario.

- Ralentizar el rendimiento del sistema, ya que los virus a menudo consumen recursos del sistema mientras se ejecutan.

- Capturar información confidencial, como contraseñas, información bancaria y otra información personal.

- Explotar vulnerabilidades de seguridad para permitir que otros tipos de *malware*, como troyanos o *ransomware*, ingresen al sistema.

Existen varios tipos de virus informáticos, cada uno diseñado para cumplir diferentes objetivos maliciosos. Los virus pueden ser propagados a través de

descargas de Internet, correos electrónicos, dispositivos USB infectados y redes compartidas. Por esta razón, es importante contar con medidas de seguridad actualizadas, como programas antivirus y firewalls, para protegerse contra los virus informáticos y otros tipos de *malware*. Existen dos tipos de softwares maliciosos que son los más habituales, en primer lugar, tenemos el troyano, este se oculta dentro de otro programa legítimo para engañar al usuario y así poder ejecutar acciones maliciosas en su sistema sin su conocimiento, una vez que se ejecuta el troyano en el sistema de la víctima, puede abrir una puerta trasera en el sistema para que los atacantes puedan acceder a él remotamente. Para protegerse contra los troyanos, es importante tener instalado un programa antivirus actualizado y no descargar o abrir archivos adjuntos de fuentes desconocidas. En segundo lugar, destaca el gusano, se propaga a través de redes de computadoras y sistemas en línea. A diferencia de otros tipos de *malware*, los gusanos no necesitan la interacción del usuario para propagarse. En su lugar, explotan vulnerabilidades en el sistema operativo, software y otros sistemas conectados en la red para replicarse a sí mismos y propagarse a otros sistemas. Los gusanos pueden ser muy peligrosos, ya que una vez que se propagan en un sistema, pueden sobrecargar los sistemas, robar información y causar daños en los sistemas infectados. Además, como los gusanos se propagan automáticamente, pueden infectar rápidamente una gran cantidad de sistemas en poco tiempo.

El sector de la logística y el transporte puede ser un objetivo para los ciberataques, incluyendo los ataques de virus informáticos. Sin embargo, la cantidad de ataques que se producen en este sector en particular puede variar significativamente dependiendo de muchos factores, como el tamaño de la empresa, los sistemas informáticos que se utilizan, el nivel de seguridad implementado, entre otros. Algunas formas en que los virus informáticos pueden afectar el sector de la logística y el transporte incluyen, tanto la interrupción del flujo de trabajo, el robo de datos confidenciales y la alteración de datos en el caso de seguimiento de envíos y la información de inventario, lo que puede resultar en errores y retrasos en la entrega.

6.2. Ransomware.

El ciberataque *ransomware* es un tipo de ataque cibernético en el que los atacantes utilizan *malware* para cifrar los archivos del usuario o de la empresa y luego exigen un rescate para recuperar el acceso a los datos cifrados. Los ataques *ransomware* se han vuelto cada vez más comunes en los últimos años y pueden ser muy dañinos para las empresas y los individuos afectados.

Los atacantes suelen propagar el *ransomware* mediante correos electrónicos de *phishing*, descargas maliciosas, kits de explotación y otras tácticas. Una vez que se ejecuta el *ransomware* en el sistema de la víctima, cifra los archivos del usuario o de la empresa y los mantiene secuestrados hasta que se pague un rescate. Los atacantes pueden exigir el pago en moneda digital, como Bitcoin, para evitar ser rastreados.

A menudo, los atacantes amenazan con destruir o publicar información confidencial si no se paga el rescate. El pago del rescate no garantiza necesariamente que los archivos se descifren, y en algunos casos, los atacantes pueden exigir un pago adicional después de recibir el primer pago.

Para protegerse contra los ataques de *ransomware*, las empresas y los individuos deben tomar medidas preventivas, como mantener el software actualizado, utilizar herramientas de seguridad como firewalls y programas antivirus, implementar la autenticación de dos factores, realizar copias de seguridad de los datos importantes con regularidad y capacitar a los empleados sobre cómo identificar y evitar los correos electrónicos de *phishing*. En caso de un ataque de *ransomware*, es importante no pagar el rescate y en su lugar buscar ayuda de un experto en seguridad informática o un proveedor de servicios de recuperación de datos.

Los ataques de *ransomware* son cada vez más frecuentes en el sector de la logística y el transporte. Los atacantes a menudo apuntan a empresas de este sector porque suelen tener sistemas de información críticos y grandes flotas de

vehículos, lo que los hace especialmente vulnerables a los ataques de *ransomware*.

Además, la pandemia de COVID-19 ha aumentado aún más el riesgo de ataques de *ransomware* en el sector de la logística y el transporte, ya que muchas empresas han tenido que adaptarse a nuevas formas de trabajo y adoptar tecnologías de trabajo remoto que pueden no estar completamente aseguradas.

Los ataques de *ransomware* pueden ser especialmente dañinos para las empresas de logística y transporte, ya que pueden interrumpir la cadena de suministro y detener la entrega de productos, lo que puede tener un gran impacto en los clientes y en la economía en general.

Para protegerse contra los ataques de *ransomware*, las empresas de logística y transporte deben asegurarse de tener políticas de seguridad adecuadas en su lugar y utilizar soluciones de seguridad de tecnología de la información (TI) robustas, como firewalls, programas antivirus, software de detección de intrusiones y copias de seguridad regulares. También es importante educar a los empleados sobre las mejores prácticas de seguridad, ya que "el error o fallo humano está presente en más del 85% de estos ciberataques" (UNO logística, 2020) y tener un plan de respuesta en caso de un ataque de *ransomware*.

"Más del 10% de las empresas del sector de la logística y el transporte han sufrido un ciberataque de *Ransomware* o una brecha de ciberseguridad con importantes pérdidas de datos de clientes en el último año" (UNO logística, 2020).

6.3. *Phishing* o suplantación de identidad.

El ciberataque de *phishing*, también conocido como suplantación de identidad, es una técnica de ataque cibernético en la que los atacantes intentan engañar a los usuarios para que revelen información personal, financiera o de otra índole, a menudo haciéndose pasar por una entidad de confianza o familiar para la víctima.

El *phishing* es comúnmente llevado a cabo a través de correos electrónicos de aspecto legítimo, que parecen ser enviados por una empresa legítima, un servicio en línea, una institución financiera u otra organización. Los correos electrónicos pueden incluir enlaces a sitios web falsificados o descargas de archivos maliciosos. Si un usuario hace clic en el enlace o descarga el archivo, el *malware* puede infectar su dispositivo o se le puede solicitar que revele información personal o financiera.

También existe una variante de *phishing* llamada "*spear phishing*", que es un ataque más dirigido y personalizado en el que los atacantes utilizan información específica sobre la víctima, como su nombre, cargo, correo electrónico y otros datos, para hacer que el mensaje de *phishing* parezca más legítimo y creíble.

Para protegerse contra los ataques de *phishing*, es importante ser cauteloso al hacer clic en enlaces o descargar archivos de fuentes desconocidas o sospechosas. Los usuarios deben verificar la autenticidad de los correos electrónicos y otros mensajes antes de hacer clic en cualquier enlace o descargar cualquier archivo. Las empresas pueden ayudar a proteger a sus empleados mediante la implementación de políticas de seguridad, la formación en mejores prácticas de seguridad y la utilización de herramientas de seguridad de tecnología de la información (TI), como filtros de correo electrónico y soluciones antivirus y antimalware.

En el caso del sector de la logística y el transporte son comunes este tipo de ataques, al igual que en muchos otros sectores. Los atacantes a menudo utilizan correos electrónicos de *phishing* para engañar a los empleados de empresas de

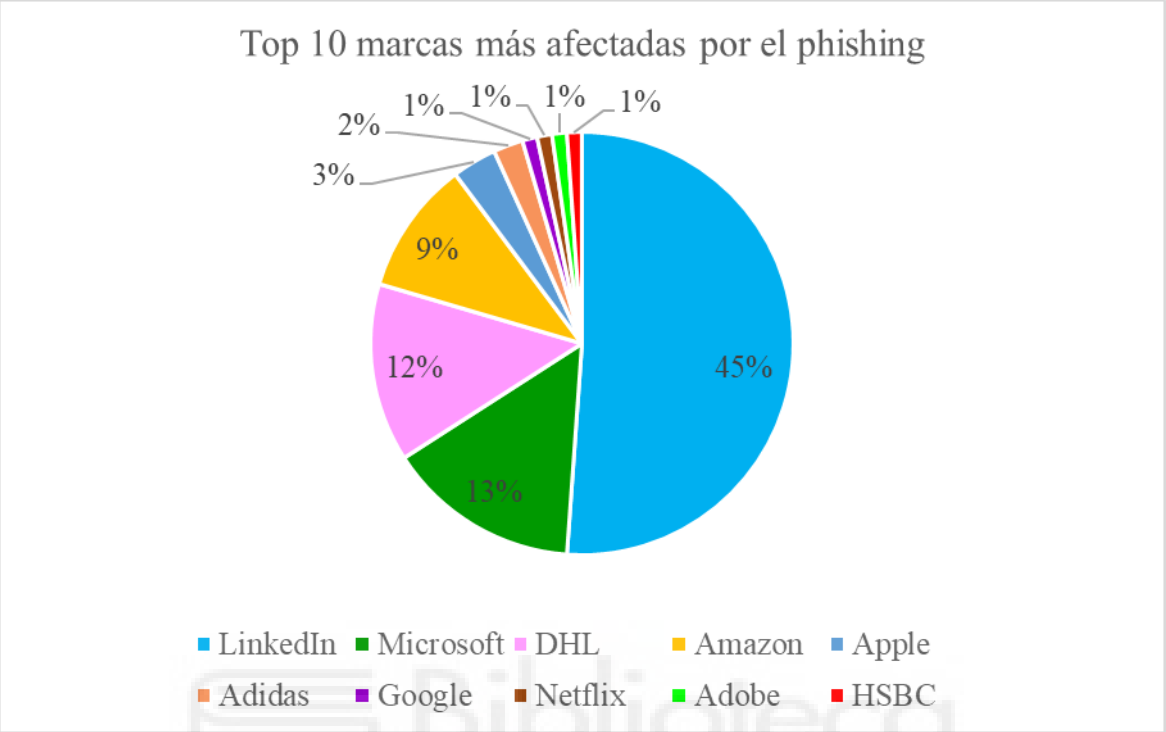
logística y transporte para que proporcionen información confidencial o hagan clic en enlaces maliciosos, lo que puede poner en peligro la seguridad de la empresa.

Además, el sector de la logística y el transporte es especialmente vulnerable a los ataques de *phishing* debido a la naturaleza de su trabajo. Por ejemplo, los atacantes pueden hacerse pasar por empresas de transporte para obtener información sobre envíos, rutas de transporte y detalles de entrega.

Para protegerse contra los ataques de *phishing*, las empresas de logística y transporte deben educar a sus empleados sobre las mejores prácticas de seguridad. También es importante que las empresas implementen medidas de seguridad como la autentificación de múltiples factores, la utilización de filtros de correo electrónico y el monitoreo de la actividad de la red para detectar actividades sospechosas.

Las primeras diez marcas más afectadas por el phishing según los últimos datos de Check Point son: LinkedIn, Microsoft, DHL, Amazon, Apple, Adidas, Google, Netflix, Adobe y Hong Kong and Shanghai Banking Corporation Limited (HSBC) (Red Seguridad, 2022).

Gráfico 5: Top 10 marcas afectadas por el *Phishing* (2022).



Fuente: elaboración propia[7].

[7] https://acortar.link/14V7q6

6.4. Denegación de servicio o *Denial of Service* (DoS).

El ciberataque de denegación de servicio (DoS, por sus siglas en inglés *Denial of Service*) es un ataque informático que tiene como objetivo sobrecargar un servidor, red o sitio web con tráfico malintencionado para que se vuelva inaccesible para los usuarios legítimos.

En un ataque DoS, el atacante envía una gran cantidad de solicitudes al servidor o sitio web, lo que lo sobrecarga y lo hace incapaz de responder a las solicitudes legítimas de los usuarios. Esto puede causar una interrupción en el servicio o incluso una caída completa del sitio web o servicio.

Existen diferentes técnicas utilizadas en los ataques DoS, incluyendo el envío de paquetes de datos malformados, el envío de una gran cantidad de solicitudes de acceso simultáneas, el uso de *bots* (programas informáticos automatizados) para enviar solicitudes, y otros métodos diseñados para sobrecargar el servidor objetivo.

Los ataques DoS son considerados como una amenaza importante para las empresas, organizaciones y servicios en línea, ya que pueden causar pérdidas financieras, daños a la reputación y pérdida de datos. Para protegerse contra los ataques DoS, se recomienda implementar medidas de seguridad, como el monitoreo constante de la red, la configuración adecuada de los servidores y el uso de soluciones de seguridad de red.

En la industria de la logística y el transporte, los ataques DoS pueden tener graves consecuencias. Por ejemplo, un ataque DoS a un sitio web de una empresa de logística o de transporte podría impedir que los clientes accedan a información importante sobre sus envíos, lo que puede generar frustración y pérdida de confianza en la empresa.

Además, si un ataque DoS afecta a los sistemas de seguimiento de envíos, la empresa podría perder la capacidad de rastrear y monitorear la ubicación de sus envíos en tiempo real, lo que podría causar retrasos y costos adicionales.

Como podemos observar en el gráfico 3 de “Tipos de ataques informáticos a las empresas españolas de logística y transporte”, un 8% de los ataques que se producen en este sector son de denegación de servicio (DoS).

Para mitigar los riesgos asociados a los ataques DoS, las empresas del sector de la logística y el transporte pueden implementar medidas de seguridad adecuadas, como el uso de soluciones de seguridad de red y la monitorización constante de los sistemas y redes para detectar y prevenir los ataques. También es importante que las empresas tengan planes de contingencia en caso de que se produzca un ataque DoS para minimizar los daños y reducir el tiempo de inactividad.

7. PRINCIPALES CONSECUENCIAS DE LOS CIBERATAQUES EN EL SECTOR.

El sector del transporte y la logística es fundamental para la economía global, ya que es responsable de la movilización de bienes y servicios en todo el mundo. Sin embargo, la digitalización de este sector ha aumentado la vulnerabilidad respecto a los ciberataques, que pueden tener graves consecuencias en términos de seguridad, confidencialidad y operaciones.

Uno de los principales efectos de los ciberataques en el sector del transporte y la logística es la interrupción de las operaciones. La interrupción de los sistemas de transporte y logística puede afectar a la capacidad de las empresas para llevar a cabo entregas a tiempo, procesar pagos, rastrear inventario y comunicarse con los clientes. Esto puede causar retrasos en las operaciones, lo que a su vez puede afectar la productividad y reducir la eficiencia del negocio.

Además, los ciberataques pueden comprometer la integridad de los datos de las empresas de transporte y logística. Esto puede resultar en la pérdida o robo de información confidencial, como la información de los clientes, los planes de entrega y los detalles de las operaciones comerciales. La pérdida de datos puede ser costosa y potencialmente perjudicial para la reputación de la empresa. La exposición de información confidencial puede poner en riesgo la privacidad y la seguridad de los clientes, lo que puede llevar a la pérdida de confianza de los mismos y, en última instancia, a la pérdida de ingresos.

Otro efecto negativo de los ciberataques en el sector del transporte y la logística es el daño a la reputación. Si la información confidencial de los clientes se ve comprometida, la empresa puede perder la confianza de sus clientes. Además, si los sistemas de la empresa están comprometidos, puede parecer que la empresa no tiene los controles de seguridad adecuados en su lugar. Esto puede afectar a la capacidad de la empresa para atraer nuevos clientes y retener a los clientes ya existentes.

Los ciberataques también pueden ser costosos para las empresas de transporte y logística. El coste de mitigar los efectos del ciberataque, recuperar datos perdidos y

mejorar la seguridad de los sistemas puede ser muy alto. Además, las empresas pueden enfrentar multas y sanciones por no cumplir con los requisitos de seguridad. Esto puede afectar la rentabilidad de la empresa y su capacidad para invertir en su crecimiento futuro.

Por otra parte, los ciberataques pueden llevar a problemas legales para las empresas de transporte y logística. Las empresas pueden ser responsables legalmente si no han tomado las medidas adecuadas para proteger los datos de los clientes. Las empresas también pueden enfrentar acciones legales de los clientes afectados por el ciberataque. Las empresas pueden estar sujetas a demandas de los clientes afectados, lo que puede ser costoso y perjudicial para la imagen de la empresa.

Los ciberataques también pueden tener un impacto en la cadena de suministro. Si una empresa es víctima de un ciberataque, puede ser necesario detener la producción o la entrega hasta que se resuelva el problema. Esto puede tener un impacto negativo en otros negocios que dependen de la empresa de transporte y logística para la entrega de bienes y servicios. Además, los ciberataques pueden afectar la disponibilidad de los bienes en el mercado, lo que puede afectar los precios y la competencia en el mercado.

También es importante que las empresas de logística y transporte tengan un plan de respuesta a incidentes cibernéticos en su lugar. Esto significa que deben estar preparadas para responder rápidamente en caso de un ciberataque, incluyendo la identificación y el aislamiento del incidente, la recuperación de los datos perdidos y la comunicación efectiva con los clientes y otras partes interesadas.

Otra medida importante para mejorar la seguridad cibernética en el sector de la logística y el transporte es la colaboración y compartir información entre las empresas. Esto puede incluir la colaboración en el desarrollo de soluciones de seguridad cibernética y la creación de una red de alerta temprana para compartir información sobre posibles amenazas.

Por otra parte, es importante que las empresas de logística y transporte consideren la seguridad cibernética como parte de su estrategia de negocio y no sólo como una

preocupación técnica. Esto significa que deben tener un enfoque proactivo para la seguridad cibernética, identificando y evaluando constantemente los riesgos y tomando medidas para reducirlos.

En resumen, los ciberataques en el sector de la logística y el transporte pueden tener graves consecuencias en términos de seguridad, confidencialidad y operaciones. Pueden interrumpir las operaciones, comprometer la integridad de los datos, dañar la reputación de la empresa y ser costosos tanto en términos financieros como legales. Es crucial que las empresas del sector de la logística y el transporte tomen medidas adecuadas de seguridad cibernética para proteger sus datos y sistemas y garantizar la integridad de la información crítica.

7.1. Pérdida de datos o información esencial para la realización de la actividad diaria.

El sector de la logística y el transporte maneja una gran cantidad de datos y ha experimentado una intensa digitalización en los últimos años. Esto hace que estas empresas sean vulnerables a los ataques cibernéticos, y la pérdida de datos o información crucial puede acarrear graves consecuencias tanto para las propias empresas como para sus clientes.

Cuando se produce la pérdida de información esencial en el sector de la logística y el transporte, pueden producirse errores en los envíos, lo que se traduce en retrasos en las entregas, pérdida de mercancías y daños a la reputación de la empresa. Además, el cruce de datos o información también puede tener consecuencias graves, como el robo de información confidencial de la empresa, como datos de clientes, información financiera y estrategias de negocio.

Los ciberataques también pueden ser utilizados para manipular los datos de envío, lo que puede dar lugar a la entrega de mercancías a destinos equivocados o la pérdida de mercancías. Esto puede ser especialmente grave en la cadena de suministro global, donde el seguimiento y la trazabilidad son esenciales para garantizar la entrega de los productos en el tiempo y lugar adecuados.

Por lo tanto, es crucial que las empresas del sector de la logística y el transporte tomen medidas adecuadas de seguridad cibernética para proteger sus datos y sistemas y garantizar la integridad de la información crítica. Esto incluye la implementación de protocolos de seguridad de la información, el cifrado de datos sensibles, la realización de pruebas de penetración y la formación de los empleados en seguridad cibernética.

7.2. Pérdida económica por gastos derivados del ciberataque.

Cuando ocurre un ciberataque en el sector de la logística y el transporte, a menudo se producen gastos significativos relacionados con la restauración y limpieza de los sistemas afectados, la contratación de expertos en seguridad informática y, en algunos casos, el pago de un rescate económico en caso de ciberextorsión.

Estos costes pueden ser extremadamente altos y resultar difíciles de asumir para muchas empresas del sector. Como resultado, la pérdida económica derivada de los ciberataques puede ser muy significativa y tener un impacto negativo en la rentabilidad y estabilidad financiera de las empresas afectadas.

Además de los costes directos mencionados anteriormente, los ciberataques en el sector de la logística y el transporte también pueden provocar una serie de costes indirectos. Por ejemplo, el tiempo de inactividad de los sistemas y la interrupción de la actividad empresarial pueden generar pérdidas de ingresos y retrasos en las entregas, lo que puede afectar la satisfacción del cliente y la reputación de la empresa. También pueden surgir costes adicionales relacionados con la implantación de medidas de seguridad adicionales para prevenir futuros ciberataques y la recuperación de datos perdidos o dañados durante el ataque. En resumen, la pérdida económica derivada de los ciberataques puede ser significativa y tener un efecto duradero en la estabilidad financiera de las empresas del sector de la logística y el transporte.

7.3. Pérdida de beneficios por paralización de la actividad.

La paralización de la actividad como resultado de un ciberataque en el sector de la logística y el transporte puede generar una pérdida de beneficios significativa. La interrupción en los sistemas operativos y la imposibilidad de acceder a la información y datos relevantes afecta a la realización de la actividad logística de manera eficiente y eficaz. Esta consecuencia suele ser una de las más comunes y a su vez una de las que más daño pueden ocasionar a las empresas de este sector.

En particular, los sistemas de gestión de flotas y los softwares de seguimiento de envíos son los más vulnerables y críticos para el sector. Las empresas del sector pueden experimentar importantes retrasos en las entregas, y las incidencias con los clientes pueden afectar la reputación y la fidelidad de estos últimos. Además, la paralización de la actividad puede llevar a la pérdida de contratos y clientes a largo plazo, lo que conlleva una disminución significativa de la rentabilidad y el crecimiento empresarial.

A parte de los retrasos en las entregas y las incidencias con los clientes, la paralización de la actividad también puede tener un impacto negativo en la cadena de suministro. Las empresas pueden enfrentar dificultades para recibir y enviar productos, lo que puede generar interrupciones en la cadena de producción y la distribución de bienes. Esto puede aumentar los costes de almacenamiento y transporte, lo que afecta a la rentabilidad de las empresas del sector. Por otra parte, la recuperación de los sistemas afectados puede ser un proceso largo y costoso, lo que puede resultar en una pérdida adicional de beneficios a corto y medio plazo.

En resumen, la paralización de la actividad como consecuencia de un ciberataque puede tener graves implicaciones económicas y operativas para las empresas del sector de la logística y el transporte.

7.4. Pérdida económica por reclamaciones de terceros (Responsabilidad Civil).

Las empresas del sector de la logística y el transporte pueden enfrentarse a una pérdida económica importante por reclamaciones de terceros relacionadas con la Responsabilidad Civil.

El manejo de información personal y sensible de clientes y proveedores hace que estas empresas sean especialmente vulnerables a las brechas de seguridad y fugas de información. En este sentido, el Reglamento General de Protección de Datos (RGPD) establece medidas de seguridad que deben ser implementadas para proteger la privacidad de los datos de los usuarios y establece sanciones elevadas en caso de incumplimiento.

Respecto al Reglamento General de Protección de Datos (RGPD), se trata de una normativa de la Unión Europea que establece las reglas sobre la protección de datos personales y la privacidad de los ciudadanos europeos. El RGPD se aplica desde mayo de 2018 y se aplica a todas las empresas que procesan datos personales de ciudadanos de la UE, independientemente de su ubicación geográfica. El objetivo principal del RGPD es fortalecer la protección de los datos personales y aumentar la responsabilidad de las empresas y organizaciones que los procesan.

En 2019, “las multas por incumplimiento de la normativa llegaron a ser de hasta el 4% de los ingresos anuales de la empresa en los casos más graves” (UNO logística, 2020).

En consecuencia, las empresas que no cumplen con las normativas de seguridad pueden verse expuestas a reclamaciones y demandas por parte de terceros que pueden tener un impacto económico significativo. En España, “según datos oficiales de la Agencia Española de Protección de Datos (AEPD), en los primeros seis meses de 2022, la cuantía por multas en España alcanzaba los 20,5 millones de euros. Desde el año 2018, la agencia ha impuesto multas por un total de 55 millones de euros y el incremento anual de 2020 a 2021 asciende a 337%” (EQS Group, 2022).

Además, la pérdida económica por reclamaciones de terceros no se limita solo a sanciones y multas impuestas por los organismos reguladores. En caso de una violación de seguridad y fuga de información, los clientes y proveedores afectados pueden reclamar daños y perjuicios a la empresa responsable, lo que puede resultar en demandas civiles y pérdidas económicas adicionales. Asimismo, estas reclamaciones pueden afectar a la reputación y la confianza de los clientes en la empresa, lo que puede resultar en una disminución de los ingresos y beneficios a largo plazo. Por lo tanto, es esencial para las empresas del sector de la logística y el transporte implementar medidas de seguridad adecuadas y cumplir con las normativas establecidas para evitar brechas de seguridad y posibles reclamaciones.

La existencia de la Agencia Española de Protección de Datos (AEPD) es esencial para garantizar la privacidad y seguridad de los datos personales de los ciudadanos españoles, así como para fomentar la confianza en el uso de servicios y tecnologías que requieren el tratamiento de dicha información. La labor de la AEPD contribuye a proteger la intimidad de las personas, evitando que sus datos sean utilizados de forma indebida o con fines ilícitos, y promoviendo un uso responsable y ético de la información personal en el ámbito público y privado. Fue creada en el año 1992 y su principal función es garantizar que se cumpla la normativa en materia de protección de datos en el país.

La AEPD se encarga de supervisar y controlar el tratamiento de datos personales por parte de empresas, organismos públicos y cualquier entidad que maneje información de carácter personal. También se encarga de recibir y atender las denuncias relacionadas con el incumplimiento de la normativa de protección de datos y de imponer sanciones en caso de que se detecten infracciones.

Además, la AEPD también tiene la función de informar a la ciudadanía sobre sus derechos en materia de protección de datos y de ofrecer orientación y asesoramiento a las empresas y entidades sobre cómo cumplir con la normativa de protección de datos de manera efectiva.

Respecto al Reglamento General de Protección de Datos (RGPD) establece una serie de obligaciones para las empresas y organismos públicos que manejan datos personales, así como una serie de derechos para los ciudadanos en cuanto a la gestión y control de sus datos. La AEPD, como autoridad competente en España, se encarga de velar por el cumplimiento del RGPD, de investigar y sancionar las infracciones, y de asesorar a empresas y ciudadanos en cuanto a la aplicación de esta normativa.

7.5. Pérdida de reputación e imagen de la empresa.

Es verdad que la pérdida de reputación e imagen de una empresa tanto en el sector del transporte y la positiva como en los distintos sectores existentes en la industria, es una consecuencia económica complicada de medir. La reputación y la imagen de las empresas son vitales para poder alcanzar un nivel óptimo de éxito y obtener un buen renombre en la industria, por ello estas pueden ser perjudicadas por diversos factores ciberataques que pueden afectar negativamente la reputación de una empresa, tales como la pérdida de información de sus clientes, la divulgación de datos confidenciales al público, el secuestro de la página web o las cuentas en redes sociales, entre otros.

En primer lugar, la pérdida de información de clientes puede ser muy perjudicial para la imagen de una empresa. Si los clientes confían en una empresa para mantener sus datos seguros y esta no lo hace, esto puede provocar una gran pérdida de confianza y credibilidad. Por otra parte, si se filtra públicamente información confidencial, esto puede tener un impacto aún mayor en la reputación de la empresa.

En segundo lugar, el secuestro de la página web o las redes sociales también puede dañar seriamente la imagen de una empresa. Si los clientes o el público en general no pueden acceder a los servicios o información de la empresa, esto puede causar una gran frustración y enfado. Además, si la empresa no logra recuperar el control de sus canales digitales a tiempo, puede haber una pérdida de confianza y credibilidad, ya que los clientes pueden sentir que la empresa no tiene la capacidad de proteger adecuadamente sus canales digitales y, por ende, sus datos. Es importante que las empresas del sector de la logística y el transporte tomen medidas proactivas para proteger su reputación y su imagen ante estos tipos de amenazas.

En este caso tenemos como ejemplo la empresa estadounidense Forward Air de transporte aéreo y terrestre, la cual sufrió un ataque el 15 de diciembre de 2020, la empresa comunicaba un incidente que afectaba a sus sistemas informáticos, desde el exterior se observaba que algo no funcionaba óptimamente ya su

página web no operaba correctamente. Este ataque afectó tanto a la empresa, que pidió a sus trabajadores que desconectaran todos los equipos informáticos de la sede, esta desconexión interrumpía las diversas operaciones, que se vieron interrumpidas durante varios días, ya que con los equipos informáticos apagados sus diferentes importaciones y exportaciones no podían atravesar las aduanas.

Estaba claro que el coste del ataque junto con la paralización de su actividad iba a acarrear un coste millonario, exactamente de 7,5 millones de dólares aproximadamente.

8. LA VULNERABILIDAD DE LAS PYMES ANTE LOS CIBERATAQUES.

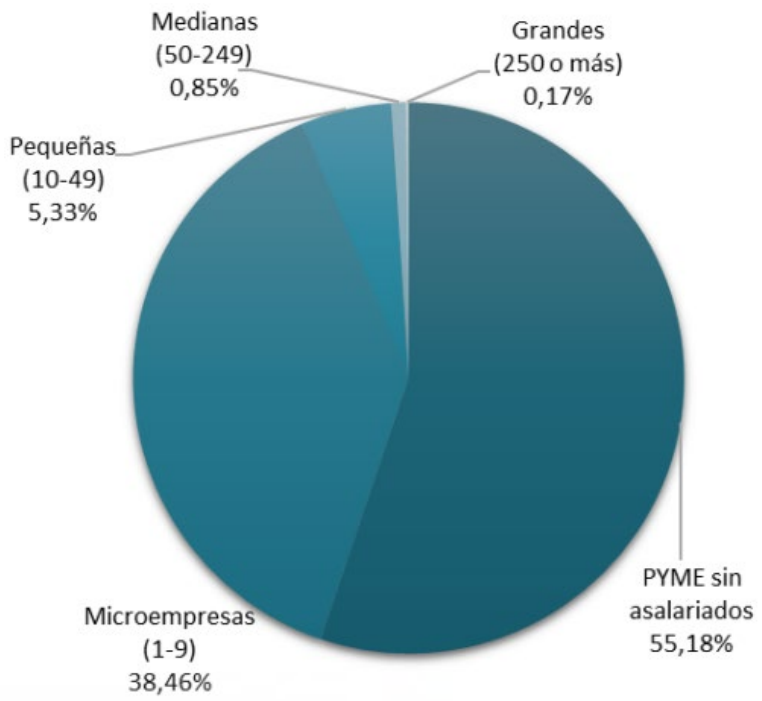
Para introducir este punto comenzaremos definiendo qué son las pequeñas y medianas empresas (PYMES), se trata de la empresa que tenga menos de 250 empleados y además sus ingresos anuales sean menores a 50 millones de euros, y/o que su balance general sea igual o inferior a 43 millones de euros. Además, dentro de la categoría de las PYMES encontramos tres subcategorías de tipos de empresas en función de su tamaño:

- Las microempresas formadas por menos de 10 empleados
- Las pequeñas empresas las cuales tienen menos de 50 empleados
- Las medianas empresas con menos de 250 empleados.

Las pequeñas y medianas empresas (PYMES) son las que principalmente mantienen la economía del estado español, estas representan más del 95% del tejido empresarial. “Las pymes suponen el 65% del PIB de nuestro país y generan el 75% de los puestos de trabajo. Por tanto, nuestras pymes son fundamentales para nuestro sistema económico” (Hervás, 2022).

La frecuente pérdida de información a causa de ciberataques es una realidad alarmante que causa graves consecuencias económicas. Un informe publicado por Zurich Seguros revela que las pequeñas y medianas empresas pueden sufrir pérdidas económicas de hasta 50.000 euros anuales solo por ataques informáticos. Esta problemática es aún más agravante en España, donde las empresas reciben un promedio de 66 ciberataques al año. Los ciberataques continúan siendo una de las mayores amenazas para las empresas del país.

Gráfico 6: Distribución de empresas por tamaño (enero 2022).

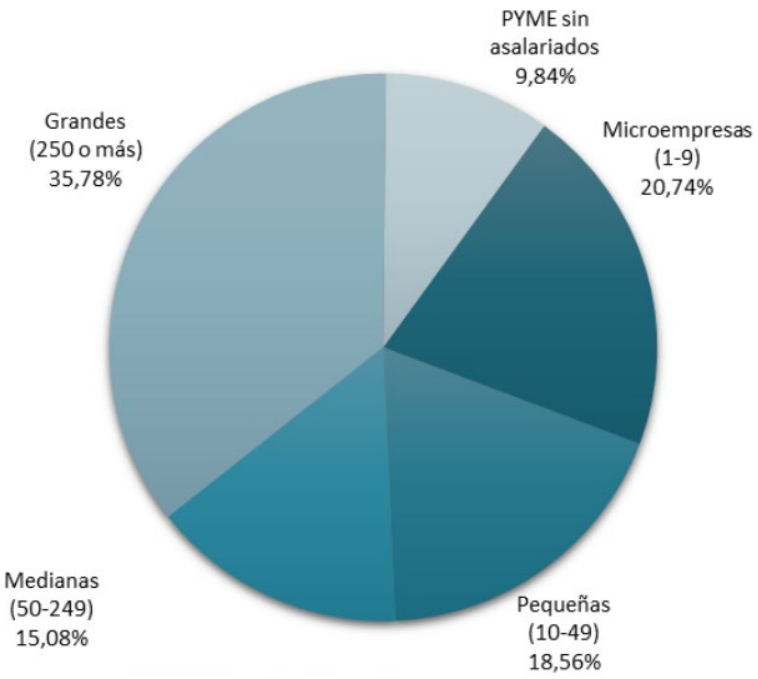


Fuente: ipyme.org[8]

El gráfico 6 nos representa la distribución de las empresas según su tamaño, en el cual se observa claramente, con más del 50%, destacan las PYMES sin asalariados, las cuales están centradas en empresas creadas recientemente por personas físicas. En segundo lugar, detrás de las PYMES sin asalariados, con un 38,46% tenemos las microempresas, se trata de empresas que tienen menos de diez trabajadores y su volumen de negocio anual no supera los dos millones de euros. En tercer lugar, tenemos las pequeñas empresas con un 5,33%, como hemos dicho anteriormente las pequeñas empresas son aquellas que tienen menos de 50 empleados y además un volumen de negocios anual no supera los diez millones de euros. En cuarto lugar, las medianas con un 0,85% y en último lugar las grandes con un 0,17%. Por ello del gráfico podemos obtener que el gran tejido empresarial de España está formado por PYMES sin asalariados.

[8] http://www.ipyme.org/Publicaciones/CifrasPYME-enero2022.pdf

Gráfico 7: Distribución del empleo por tamaño (enero 2022).

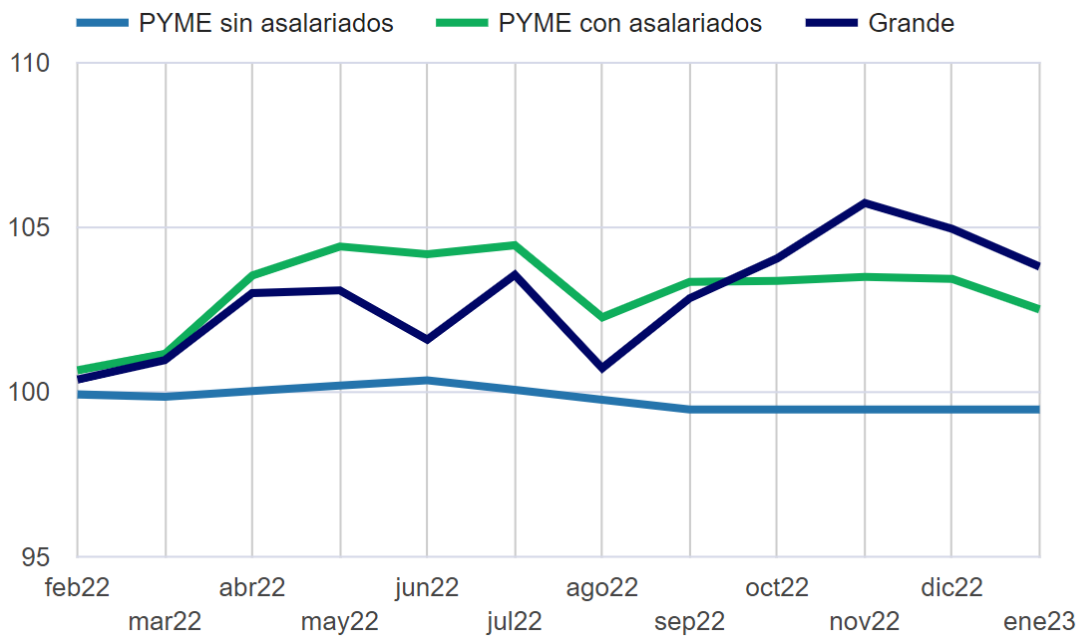


Fuente: ipyme.org[9]

En el gráfico 7 podemos observar la distribución del empleo según su tamaño, en primer lugar, tenemos el empleo de las grandes empresas, las cuales ostentan un 35,78% del empleo. En segundo lugar, observamos el 20,74% de las microempresas, seguidas en tercer lugar de las pequeñas empresas con un 18,56%. En cuarto lugar, se posicionan las medianas empresas con un 15,08%. Y por último las PYMES son asalariados con un 9,84%

[9] http://www.ipyme.org/Publicaciones/CifrasPYME-enero2022.pdf

Gráfico 8:Evolución del empleo por tamaño. Cifras PYMES. Datos enero 2023.



Fuente: Ministerio de industria, comercio y turismo[10].

En febrero, el número de pequeñas y medianas empresas (PYMES) con asalariados aumentó en un 0,26% con respecto al mes anterior, lo que equivale a un total de 3.362 empresas adicionales, elevando el número total a 1.311.222. El número de grandes empresas también aumentó en un 0,61% (32 empresas adicionales), llegando a un total de 5.305 empresas. En conjunto, esto dio lugar a un total de 1.316.527 empresas con asalariados, lo que representa un aumento del 0,26% y 3.394 empresas adicionales.

En cuanto al empleo, las PYMES con asalariados emplearon a un total de 9.212.939 trabajadores en febrero, lo que significa una oscilación del 0,76% y 69.716 trabajadores adicionales. Las grandes empresas emplearon a un total de 6.134.601 trabajadores, lo que representa un aumento del 0,61%, es decir, 37.474 empleados adicionales. En total, todas las empresas con asalariados emplearon a 15.347.540 trabajadores, lo que equivale a un aumento del 0,70% y 107.190 trabajadores adicionales.

[10] https://industria.gob.es/es-es/estadisticas/paginas/estadisticas-y-publicaciones-sobre-pyme.aspx

El segmento de PYMES con asalariados de tamaño mediano, es decir, de 50 a 249 empleados, experimentó el mayor crecimiento tanto en términos de número de empresas con un 1,52% como de empleo con un 1,55%.

Aproximadamente a nivel mundial más del 60% de las pequeñas y medianas empresas (PYMES) se han visto afectadas por ciberataques. “Antes de la pandemia, las pymes englobaban el 97% de empresas en España, un porcentaje que marca el predominio de las microempresas, que constituían el 94% de las empresas del sector privado a enero del 2020 con un total de 3.417.000 compañías” (GD Empresa, 2022).

La vulnerabilidad de las pequeñas y medianas empresas (PYMES) españolas en el sector del transporte y la logística ante los ciberataques es un tema de gran importancia en la actualidad. A medida que estas empresas se vuelven más tecnológicas y digitales, también las vuelve más vulnerables a los ciberataques. Además, las PYMES son las más afectadas por estos ataques debido a su falta de recursos, medidas de seguridad adecuadas y la falta de conciencia sobre los riesgos de ciberseguridad y la falta de medidas de seguridad efectivas. Muchas veces esta falta de recursos, medidas y la falta de conciencia se debe a sus presupuestos limitados, a esto lo podemos añadir que no suelen contar con personal especializado en esta materia, además, muchas veces carecen de herramientas de protección, motivo por el cual acentúa su vulnerabilidad ante estas amenazas. La mayoría de estas empresas no están al tanto de las diversas amenazas cibernéticas y por ello no pueden tomar medidas de seguridad efectivas que les permitan protegerse.

Para abordar estas vulnerabilidades, las PYMES del sector necesitan implementar medidas que sean efectivas, como puede ser el uso de software y la realización de copias de seguridad de forma regular. También es importante que las empresas capaciten a su personal sobre los diversos riesgos de la ciberseguridad y establecer políticas claras de seguridad. Por otra parte, las PYMES pueden no ser conscientes de que también son un objetivo para los ciberdelincuentes, y que su tamaño no las hace inmunes a estos ataques. El sector del transporte y la logística maneja grandes cantidades de datos confidenciales, esto las convierte en un objetivo muy atractivo.

Ampliando las medidas mencionadas anteriormente, las PYMES deberías incluir algunas de estas medidas para prevenir ataques:

- Deben realizar actualizaciones regulares de software y sistemas operativos, estos son esenciales para proteger los sistemas de las PYMES contra vulnerabilidades conocidas.

- Las PYMES deben asegurarse de que las contraseñas utilizadas para acceder a sistemas y redes sean fuertes y difíciles de adivinar.

- Limitando el acceso a información confidencial las PYMES pueden reducir el riesgo de exposición a ciberataques, por ello es importante que solo el personal autorizado tenga acceso a dicha información.

- El uso de herramientas de seguridad en línea para protegerse contra las amenazas puede ayudar a las empresas a reducir el riesgo de ataques. Como herramientas pueden utilizar antivirus, firewalls y herramientas de detección de intrusiones.

- Y, por último, las empresas deben realizar copias de seguridad de forma regular de sus datos más importantes, por tanto, en caso de ciberataque podrían recuperar los datos guardados.

Como se ha ido mencionando a lo largo de este apartado, los ciberataques en el sector son constantes, ya que se realizan transacciones en línea o tienen información importante, como pueden ser datos de envíos, entregas, rutas, clientes y proveedores. Por tanto, un ciberataque exitoso puede tener graves consecuencias, como la pérdida de información crítica, el robo de identidad, el fraude y la interrupción de las operaciones comerciales, además pueden sufrir daños financieros y de reputación. Por ello es crucial que las PYMES busquen asesoramiento y apoyo especializado en este ámbito.

En resumen, la ciberseguridad es una preocupación cada vez más importante para las PYMES de los diferentes sectores, y sobre todo del sector del transporte y la

logística. La falta de recursos financieros y técnicos, la falta de conciencia sobre los riesgos de la ciberseguridad y la falta de medidas de seguridad efectivas, hacen que estas empresas sean especialmente vulnerables a los ciberataques. Para protegerse, las PYMES deben implementar medidas de seguridad efectivas, capacitar a su personal y obtener un buen asesoramiento y apoyo especializado. Implementando estas medidas y mediante un buen asesoramiento, las empresas pueden reducir significativamente su vulnerabilidad a los ciberataques y proteger sus datos y sistemas.

9. CONCLUSIONES.

Como conclusiones extraídas de este Trabajo de Fin de Grado, podemos asegurar que la ciberseguridad se ha convertido en un tema cada vez más relevante en el sector del transporte y la logística debido al aumento en la dependencia de la tecnología y la digitalización de los procesos.

La falta de medidas de ciberseguridad puede tener un impacto devastador en las empresas de transporte y logística, como la pérdida de datos esenciales para la realización de la actividad diaria, la paralización de la actividad empresarial y la pérdida económicas, entre otros. Por tanto, para implantar la ciberseguridad en el sector, se pueden seguir diversas medidas, incluyendo la concienciación de los trabajadores, la implementación de medidas de protección física y lógica y la realización de auditorías de seguridad periódicas. En este sentido, el Instituto Nacional de Ciberseguridad (INCIBE) proporciona recursos y herramientas útiles para las empresas que quieran mejorar su ciberseguridad.

Podemos concluir que los ataques más habituales que hemos tratado a lo largo del trabajo son los virus informáticos, ransomware, phishing o suplantación de identidad y denegación de servicio. Es necesario que las empresas estén preparadas para hacer frente a estos ciberataques, lo que implica contar con un plan de contingencia y respuesta.

10. BIBLIOGRAFÍA.

Controla Plus. (22 de febrero de 2022). Obtenido de https://www.controla-plus.com/blog/ciberseguridad-transporte-logistica/#Impacto_de_la_ciberseguridad_en_el_transporte_y_la_logistica

Cuadernos de Seguridad. (30 de diciembre de 2019). Obtenido de España, país que más invierte en ciberseguridad en el sector logístico y de transporte: https://cuadernosdeseguridad.com/2019/12/espana-logistica-ciberseguridad/

EQS Group. (24 de Noviembre de 2022). Obtenido de Multas por incumplimiento en España según el RGPD: https://www.eqs.com/es/compliance-blog/multas-por-incumplimiento/#:~:text=Seg%C3%BAn%20datos%20oficiales%20de%20la,a%202021%20asciende%20a%20337%25.

GD Empresa. (25 de Julio de 2022). Obtenido de ¿Cuántas pymes hay en España? Datos y Porcentajes: https://gdempresa.gesdocument.com/noticias/la-evolucion-de-las-pymes#:~:text=Porcentaje%20de%20pymes%20en%20Espa%C3%B1a,total%20de%203.417.000%20compa%C3%B1%C3%ADas.

González, R. (30 de enero de 2023). *Cinco Días*. Obtenido de https://cincodias.elpais.com/cincodias/2023/01/25/pyme/1674679646_587962.html

Hervás, L. V. (27 de Junio de 2022). *Cinco Días*. Obtenido de ¿Cómo son las pymes en España? | Pyme | Cinco Días: https://cincodias.elpais.com/cincodias/2022/06/24/pyme/1656070303_778210.html

INCIBE. (27 de enero de 2016). Obtenido de https://www.incibe.es/que-es-incibe

INCIBE. (15 de Julio de 2020). Obtenido de INCIBE: https://www.incibe.es/summer-bootcamp/sbc2020/ponentes/felixbarrio

INCIBE. (2022 de Octubre de 2022). Obtenido de INCIBE: https://www.incibe.es/enise/ponentes/carla-redondo-galbarriatu

Liñán, I. (10 de Enero de 2023). *El Mercantil*. Obtenido de El Mercantil: https://elmercantil.com/2023/01/10/la-ciberseguridad-alienta-a-las-empresas-

logisticas-a-afinar-el-comportamiento-del-empleado/#:~:text=Este%20estudio%20reporta%20que%20entre,al%2017%25%20al%20a%C3%B1o%20siguiente.

Liñán, J. C. (10 de Septiembre de 2019). *El Mercantil*. Obtenido de El Mercantil: https://elmercantil.com/2019/09/10/el-sector-logistico-espanol-incrementa-sus-inversiones-en-ciberseguridad/

Red Seguridad. (9 de Agosto de 2022). Obtenido de Top 10 de empresas más suplantadas por los cibercriminales: https://www.redseguridad.com/actualidad/ciberseguridad/phishing-este-es-el-top-10-de-empresas-mas-suplantadas-por-los-cibercriminales_20220809.html

UNO logística. (20 de junio de 2020). Obtenido de https://www.unologistica.org/ciberriesgo-la-logistica-transporte/