Universidad del País Vasco Euskal Herriko Unibertsitatea

EKONOMIA ETA ENPRESA FAKULTATEA
FACULTAD DE ECONOMÍA Y EMPRESA

GRADO: Administración y Dirección de Empresas

Curso 2022/2023

NECESIDADES DE LAS EMPRESAS VASCAS EN MATERIA DE CIBERSEGURIDAD

Autor/a: González Bals Cabado, Kepa

Director/a: Saiz Santos, María

Bilbao, a 21 de junio de 2023

ÍNDICE

ÍNDICE DE GRÁFICAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE SIGLAS

APT Advanced Persistent Threat

BCSC Basque CyberSecurity Center

CCN Centro Criptológico Nacional

CLO Chief Legal Officer

CNI Centro Nacional de Inteligencia

CTO Chief Technology Officer

DDOS Distributed Denial of Service

DES Data Encryption Standard

EMPACT European Multidisciplinary Platform Against Criminal Threats

ENISA Empresa Nacional de Innovación Sociedad Anónima

EUSTAT Euskal Estadistika Erakundea

EUROSTAT Oficina Europea de Estadística

GPT Generative Pretrained Transformer

IA Inteligencia Artificial

IAM Identity and Access Management

IBM International Business Machines

ICT Information and Communication Technology

INCIBE Instituto Nacional de Ciberseguridad de España

INE Instituto Nacional de Estadística

NSA National Security Agency

ODS Objetivos de Desarrollo Sostenible

PWC PriceWaterhouseCoopers

PYME Pequeña y Mediana Empresa

RGPD Reglamento General de Protección de Datos

SIEM Security Information and Event Management

TIC Tecnologías de la Información y las Comunicaciones

UE Unión Europea

1. RESUMEN

El siguiente trabajo de investigación trata de responder a la pregunta que su propio título sugiere. La ciberseguridad es un tema que hoy en día está en boca de todos y tanto los individuos como las empresas lo reconocen como una prioridad, sin embargo, no es tan fácil identificar o plasmar la situación y definir los puntos de partida que existen para mejorarla.

Mediante revisión bibliográfica, estadística y el diseño de fuentes de datos propias el autor pretende mostrar a lo largo del documento las respuestas a los objetivos planteados, cuyos resultados aparecen en la parte final del trabajo. En el capítulo de introducción se exponen los antecedentes, metodología, estructura y objetivos mencionados.

Tras la introducción, el lector encuentra un capítulo dedicado a las megatendencias en el sector de la ciberseguridad. En este, se revisa la historia, tendencias en peligros y herramientas actuales e incluso se revisa la situación actual a nivel nacional e internacional en el sector. Es un capítulo más denso por su objetivo, pero muy importante para poner en contexto al lector antes de introducirse en el tema de la ciberseguridad de las empresas en Euskadi. Se identifican en él los comportamientos de los malwares y otras amenazas, primeros ataques cibernéticos y comparaciones, por ejemplo, del sector de la ciberseguridad entre los distintos países de la Unión Europea. Sitúa al sector como uno muy innovador y bien posicionado, pero todavía con muchos retos que afrontar.

Después, se encuentra el capítulo puente hacia la ciberseguridad de las empresas vascas, en forma de introducción al mundo de la ciberseguridad dentro de la empresa. En este capítulo se puede encontrar un ejemplo del porqué en este trabajo se eligen cuatro grandes bloques en forma de clasificación de los puntos de partida de las barreras y retos que las empresas encuentran para mejorar su ciberseguridad.

Finalmente, en el último capítulo previo a la presentación de las conclusiones detalladas se encuentra el denominado “El Caso Euskadi”. En este, se responde mediante el uso sobre todo de fuentes propias y bases de datos encontradas, a los subobjetivos de comparación del sector de la ciberseguridad vasco con el de su entorno e identificación de barreras y retos de las empresas vascas en ciberseguridad. Vienen dados por los bloques elegidos como distintos puntos de partida (Interno de las empresas, Legal, Político y Educativo o de Formación) y resultan, mediante la formación del

decálogo presentado en las conclusiones y resultados del proyecto, en la respuesta al objetivo principal del proyecto de investigación; la identificación de las necesidades de las empresas vascas en ciberseguridad.

Estas necesidades, para sorpresa del autor, se alejan de la mejora e innovaciones técnicas y tienen más relación con el factor humano y de decisiones de las personas, así como de las empresas vascas, objetivo de este estudio.

2. INTRODUCCIÓN

2.1. ANTECEDENTES

La ciberseguridad es hoy en día una necesidad de la que cada vez más se habla tanto por parte de los individuos como de las empresas. Son numerosos los casos de incidentes en materia cibernética de los que oímos hablar día tras día y por eso es que las empresas cada vez inciden más en este aspecto. La transformación digital de estas, acelerada por naturaleza, pero aún más por la explosión del teletrabajo, e-commerce y otras herramientas y negocios digitales, hace que todavía, en la mayoría de los casos, las empresas vayan por detrás de los delincuentes digitales.

"Nueve de cada 10 empresas tienen alguna medida de seguridad TIC implementada y ocho de cada 10 usan tecnologías de acceso remoto para su personal." (INE, 2022).

Euskadi, cuyo tejido empresarial está formado sobre todo por Pequeñas y Medianas Empresas (PyMEs) (Eustat, 2022), es uno de los referentes en la incorporación de herramientas digitales e innovadoras en sus empresas, situándose por detrás sólo de Cataluña en porcentaje de empresas que utilizan internet y web para su actividad, con un 83,1 por ciento sobre el total de las empresas del territorio (INE, 2022). Por un lado, el tamaño de las empresas, que hacen menos factibles las grandes inversiones en materia de ciberseguridad, y por otro la notable presencia de las empresas vascas en internet, hacen que la ciberseguridad en Euskadi sea una prioridad mayor.

En este contexto, se desarrolla el problema de identificar el origen de las necesidades que tienen las empresas vascas en materia de ciberseguridad, ya que, a pesar de su importancia, las vías que tienen las empresas para afrontar este reto son dispersas y poco accesibles en muchos casos. De esto mismo surge el interés personal del autor de este Trabajo de Investigación, que tras haber cursado la mención de Innovación Empresarial y haber realizado la estancia de prácticas en una start-up del entorno, en crecimiento e innovadora, ha percibido la falta de claridad que existe en las necesidades de seguridad cibernética y cómo abordarlas.

La materia a investigar va sin duda muy en línea con el plan de estudios y objetivos académicos del grado en Administración y Dirección de Empresas. Las necesidades de Seguridad se encuentran en el segundo escalón de la pirámide de Maslow, y hoy en día para las empresas, sobre todo las empresas vascas, las necesidades en ciberseguridad abarcan gran parte de estas necesidades, como se puede

Ilustración 1: Ciberseguridad en la Pirámide de Maslow

Fuente: Elaboración propia a partir de Maslow, 1943

ver en la Ilustración 1. Esto, como podemos ver, no solo está relacionado con las asignaturas del itinerario de Innovación empresarial sino también con numerosas asignaturas del grado, así como de la mayoría de las salidas profesionales de este. La ciberseguridad es un reto real y prioritario para cualquier empresa y toca a cualquier departamento o tarea dentro de estas. ¿Cómo almacena los datos personales de los empleados el departamento de Recursos Humanos?, ¿Cómo de expuestos tiene el departamento financiero los datos de caja y previsiones?, ¿Almacena de manera segura la dirección de la empresa sus posibles planes a implementar?

El derecho, la estadística, la econometría, la gestión del marketing y de la innovación, la dirección estratégica y financiera y otros muchos conocimientos adquiridos a lo largo del grado están directa o indirectamente relacionados con el objetivo de hacer de las compañías, entornos mucho más seguros frente a los peligros de la transformación digital.

En resumen, el proyecto de investigación tratará de unificar la información relativa a la ciberseguridad de las empresas vascas, con la intención de plasmar las necesidades que estas tienen en esta materia.

Además, cabe destacar que la mejora de la ciberseguridad de las empresas es un objetivo implícito en el objetivo número 9 de los Objetivos de Desarrollo Sostenible de las Naciones Unidas (ODS), que pretende “Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación”. Es evidente que la consecución de esta meta debe llevar consigo una base de seguridad digital sólida que permita estos avances de una forma segura y unificada.

Ilustración 2: ODS número nueve

Fuente: United Nations

2.2. OBJETIVOS

El objetivo de este trabajo de investigación es identificar las necesidades en materia de ciberseguridad de las empresas en Euskadi. En ningún caso pretende realizar sugerencias relativas a las cuestiones técnicas que implican la mejora de la ciberseguridad de las empresas, ya que estas se alejan de la rama de conocimiento de la Economía y la empresa.

Para la consecución de este objetivo se proponen una serie de subobjetivos necesarios para contextualizar el tema y hacerlo más comprensible y preciso:

I. Identificar las megatendencias mundiales actuales en materia de ciberseguridad.

II. Valorar los avances del País Vasco en lo relativo a la ciberseguridad y en comparación con su entorno.

III. Identificar las principales vulnerabilidades de las empresas vascas frente a peligros digitales.

IV. Definir los diferentes retos que tienen las empresas vascas y los diferentes ámbitos desde los que actuar.

Aunque pequeños detalles técnicos relativos a la cibernética deban ser mencionados para la consecución de la comprensión por parte del lector, la brecha teórico-práctica entre el mundo de la informática y la empresa limita el alcance de este trabajo, ciñéndolo al conocimiento e investigación económico-empresarial.

2.3. METODOLOGÍA

En cuanto a la metodología empleada para la realización de esta labor de investigación se pueden distinguir distintos pasos o bloques del proyecto (véase Ilustración 3).

En primer lugar, y al ser un tema apenas mencionado a lo largo del grado y con poca información accesible, sobre todo para lo limitado a Euskadi, se ha realizado una importante labor de investigación o revisión bibliográfica con el objetivo de filtrar las fuentes de información y destacar las que se han considerado óptimas para cada sección o rama del tema a investigar.

Asimismo, y tras haber filtrado estas fuentes se ha tratado de seleccionar la información que mejor contextualiza el objeto de estudio. En este punto ha sido muy importante no desviar la atención hacia la enorme cantidad de información relativa a la ciberseguridad a nivel mundial y tratar de acotarla solo a lo necesario para aportar al lector la visión necesaria para analizar el estudio en un contexto ya identificado y limitado previamente. Además, tras esta revisión bibliográfica se tratará de dar a entender al lector los diferentes puntos o sectores desde los cuales se pueden y deben tomar medidas que favorezcan la ciberseguridad de las empresas, en concreto las empresas vascas.

Después de esta revisión bibliográfica se ha llevado a cabo la labor de investigación empírica más relacionada con el objetivo final del trabajo. Con la información analizada previamente y tras haber elegido a la población de estudio como las empresas vascas, haciendo especial énfasis en las PyMEs y Start-ups, se ha escogido la muestra de empresas y entidades "objetivo" para la investigación. Para esta selección de fuentes de información y en busca de un diseño de entrevistas y encuestas óptimo, se ha tratado de encontrar contactos que puedan ser expertos o personas influyentes en cada uno de los distintos sectores o puntos de actuación que previamente se han identificado como principales para la búsqueda de la ciberseguridad empresarial en Euskadi (Véase apartado 6.1: diseño del trabajo de campo). Mediante las entrevistas conseguidas, tanto en formato escrito como telefónico, así como las encuestas realizadas, eventos a los que se ha asistido y otras fuentes de datos y respuestas a las preguntas planteadas se ha realizado un análisis de datos que ha resultado en el primer borrador de conclusiones o respuestas a los retos planteados para el proyecto (véase Ilustración 3).

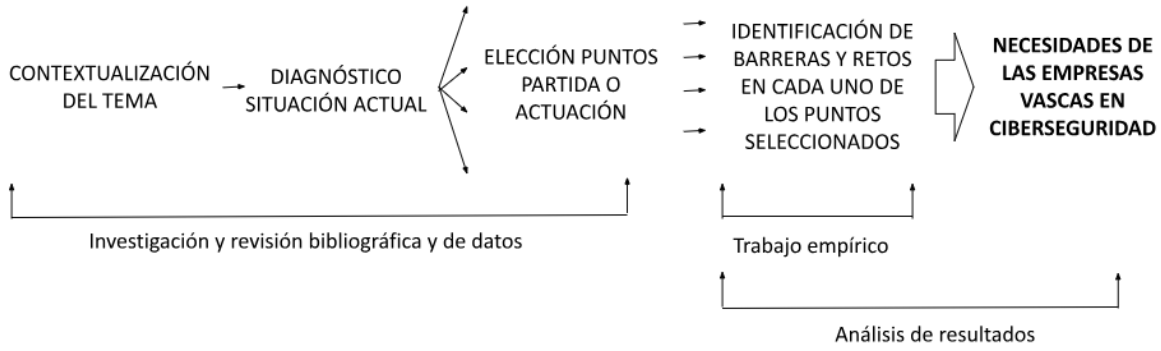


Ilustración 3: Metodología del proyecto

Fuente: Elaboración propia

Finalmente, y tras este análisis de datos se ha decidido dividir la estructura de la investigación en 4 principales fuentes de las necesidades de las empresas o ámbitos desde los que el autor considera que se debe empezar a actuar (Político, Jurídico, Empresarial y Educativo o de formación de las personas). Es por esto por lo que a lo largo del documento se utilizará este desglose continuamente, así como también a la hora de dar respuesta a los objetivos planteados.

Además, en cuanto a las consideraciones éticas, el autor asegura haber cumplido con la honestidad necesaria para la realización del documento. Para ello, se han citado todas las fuentes de forma correcta y se ha avisado y mencionado a todos los participantes de la investigación. Existen documentos firmados por el autor y cada participante con el permiso para la utilización de los datos recuperados gracias a todos ellos.

Los resultados obtenidos tendrán como base tanto la investigación bibliográfica como la empírica y no pretenden buscar soluciones a las necesidades identificadas, sino unificarlas para servir como punto de partida de la posible actuación.

2.4. ESTRUCTURA

En lo referente a la estructura que sigue el documento se puede identificar con la forma de "embudo", de forma que el autor persigue hacer entender al lector las megatendencias a nivel mundial relacionadas con la ciberseguridad en un principio, para luego acotar esta información a la población objetivo e ir incorporando nuevos datos a medida que se acerca a las conclusiones, donde se presenta el decálogo de necesidades como respuesta al objetivo principal del trabajo.

De esta forma y a grandes rasgos, el documento estaría formado, en primer lugar, por una contextualización en forma de megatendencias relativas a la ciberseguridad y las herramientas disponibles para mejorarla. Para ello, se destacarán los más importantes avances en esta materia, así como también la situación y deficiencias actuales.

Tras esta pequeña tarea de introducción en el tema a desarrollar, se tratará de trasladar al lector a un entorno más limitado, concretamente a Euskadi y las empresas, persiguiendo darle una imagen fiel del panorama actual en el que se encuentra el sector de la ciberseguridad en el País Vasco. Aquí se tratará de posicionar a Euskadi en comparación a su entorno en la materia en cuestión, así como de identificar las principales deficiencias que precederán a las posteriores necesidades atribuidas al territorio.

Habiendo situado al lector en el enorme mundo que forma todo lo relacionado con la ciberseguridad y colocado a Euskadi en este gran mapa mediante el uso de las mejores referencias e información encontradas, se empezará a segmentar el trabajo en cuatro grandes bloques: Entornos Político, Jurídico, Empresarial y Educativo o de formación de las personas. Se tratará de explicar, en cada uno de ellos, dónde nos encontramos y a dónde se pretende llegar para mejorar la ciberseguridad de las empresas vascas.

Estos dos últimos bloques explicados se pueden considerar la parte más interesante del trabajo de investigación para el lector. Es precisamente tras la lectura de ellos cuando se percibirán las respuestas a los objetivos del trabajo y cuando se hagan referencias a opiniones y datos reales extraídos a través las técnicas anteriormente explicadas. Por último, el autor tratará de plasmar las conclusiones de manera concisa en el siguiente apartado, que culminará con un decálogo que, de manera visual, enumerará las respuestas a los principales interrogantes surgidos al principio de la investigación.

2.5. DIVISIÓN DE CAPÍTULOS

La división de los capítulos en el caso de este proyecto de investigación es simple pero sencilla e intuitiva para el lector:

1. RESUMEN: Resumen previo a la lectura del documento. Tras la lectura de este resumen, el lector podrá identificar de manera clara y concisa el desarrollo del proyecto, pudiendo ver

destacadas las conclusiones a los retos o problemas planteados en el inicio. En este caso, el lector debería, tras la visión del resumen ser capaz de tener una primera idea de cuál es la parte del documento que responde a cada problemática. Además, se adjuntará un detalle de las siglas utilizadas en el documento.

2. INTRODUCCIÓN: En este capítulo se le da al lector la visión previa a la realización del análisis, planteando los antecedentes del proyecto como motivo o razón por la cual el tema a investigar ha sido elegido, los objetivos marcados y que deberían ser resueltos, la metodología utilizada para dar la imagen real de cuáles serán las fuentes y métodos con los que se consigue la información a analizar para la posterior redacción y por último la estructura del documento.
3. LA CIBERSEGURIDAD: Tratando de ser breve pero claro, este capítulo está destinado a tratar de conectar al lector con el mundo de la ciberseguridad. Con la utilización de solo los detalles técnicos necesarios, el lector debería poder entender la situación actual del sector en cuestión a través la lectura de un pequeño marco teórico, una puesta en escena de la historia y megatendencias actuales del sector, retos futuros de la ciberseguridad y situación en Europa y en España del mundo de la ciberseguridad. Estos dos últimos análisis de situación serán llevados a cabo gracias a la presentación de los datos estadísticos obtenidos en las distintas agencias oficiales.
4. EMPRESAS Y CIBERSEGURIDAD: Teniendo en cuenta que el capítulo anterior trata de la ciberseguridad en su totalidad, a través de la redacción de este siguiente, se tratará de acotar la información y utilizar lo aprendido por el lector para entender la situación del sector de la ciberseguridad en la red o mundo empresarial.
5. EL CASO EUSKADI: Similar al capítulo anterior, pero llevando el objetivo al siguiente nivel, en este último capítulo previo a las conclusiones se trata de finalmente acotar la información y rellenarla para la población elegida para el estudio: Las empresas vascas. En este apartado se hará uso de estadísticas, bibliografía, pero sobre todo fuentes de información creadas por el autor para realizar una aproximación casi total a la consecución de los objetivos planteados para el proyecto de investigación.
6. RESULTADOS: En este capítulo veremos en primer lugar la explicación metodológica del trabajo de campo realizado. Tras esta explicación se presentan los resultados obtenidos precisamente mediante este trabajo de investigación empírica cualitativa, precediendo a las conclusiones siguientes.

7. CONCLUSIONES: En las conclusiones analizaremos los resultados relacionándolos con los objetivos del proyecto de investigación En este capítulo se tiene acceso al decálogo que culmina la respuesta a estos objetivos y que precede a la presentación de las posibles líneas de investigación futura, abiertas para cualquier mejora o continuación del trabajo.
8. BIBLIOGRAFÍA: Presentación de las fuentes de información utilizadas para el análisis y redacción del documento.
9. ANEXO: Capítulo destinado al espacio para adjuntar los necesarios anexos de información como redacción escrita de las entrevistas.

3. LA CIBERSEGURIDAD

3.1. CIBERSEGURIDAD A GRANDES RASGOS

Cualquiera podría dar una explicación lógica acerca del significado del concepto de ciberseguridad porque el propio lenguaje ya lo hace a la perfección. No es más que el conjunto de técnicas y prácticas que hacen que la información y herramientas estén seguros frente a los posibles ataques cibernéticos o digitales. Este concepto implica la seguridad de cualquier individuo, empresa o ente que pueda poseer o guardar cualquier tipo de material susceptible de ser atacado por un delincuente por medio de las herramientas o armas digitales. Es importante remarcar que a pesar de que la mayoría de los dispositivos vulnerables tengan conexión a internet, el término engloba a cualquiera de ellos, incluyendo los aparatos y dispositivos no conectados.

La constante carrera de la ciberseguridad es perfectamente identificable como una carrera entre posibles ataques y defensas. Un símil fácilmente comparable, y que seguramente ayude a cualquiera a entender mejor este sector, es el de, por un lado, los ciber atacantes y la ciberseguridad, y por el otro, los virus o bacterias y la farmacología. Profesionales y expertos en la materia tratan siempre de adelantarse a los avances de estas formas de ataque, sin embargo, en la realidad, tanto en el sector farmacéutico como en el de la ciberseguridad, continuas reacciones a nuevas formas de ser atacados inducen a nuevas formas de defensa y protección.

Continuando con este símil que hemos utilizado en el párrafo anterior, podemos explicar, muy a grandes rasgos, el carácter y funcionamiento del tipo de ciberataque más clásico. Al virus que se instala en el organismo, en el sector cibernético se le llama “malware” y salvando las diferencias lógicas, el proceso que sigue es el mismo. El malware es programado para que, una vez instalado en el dispositivo de la víctima, cumpla determinados procesos que pueden variar entre extraer información, hacer caer una red, etc. Es cierto que, aunque en la mayoría de las situaciones en las que se habla de ciberseguridad y ciberataques se hable de este modo de ataque, incluida esta investigación, también se considera ataque digital cualquier otro intento de engaño, robo o acto de delincuencia llevado a cabo mediante cualquier dispositivo digital.

La principal herramienta en contra de los ciberataques se explica mejor volviendo al principio de todo este tema. Como ya se ha mencionado, este trabajo de investigación no pretende adentrarse

en el tan extenso y técnico mundo de la ciberseguridad. Es por esto por lo que nos conviene acordarnos de nuevo de que la cibernética y de manera implícita la ciberseguridad, trata, en resumen, de la información y la gestión de esta. Estos dos conceptos, lógicamente, son muy anteriores a la era digital y es por esto mismo que también la herramienta más útil que existe para la gestión de la información de forma segura proviene de muchos años atrás. A esta herramienta se le llama el "cifrado", y está muy relacionado con la criptografía, que consiste básicamente en guardar una información bajo un código o escritura que hace que esta sólo sea comprensible para aquellos que sepan o conozcan este código. Es sabido que esta técnica es utilizada por lo menos desde hace cuatro mil años, ya que existen recursos como recetas o historias que pretendían ser guardadas bajo un código que protegiera la propiedad intelectual de los autores.

Este proceso hoy en día se rige bajo un sistema llamado "protocolo". Un protocolo es un conjunto de reglas que cumple el programa que encripta y utiliza la información. En otras palabras, el programa, en función del protocolo utilizado, decidirá para quién estará encriptada la información y para quién no. Un protocolo conocido por todos hoy en día es el protocolo "https", el cuál asegura que lo que se haga o cambie en las páginas web que funcionen bajo él, no sea visible públicamente.

Asimismo, entre esta y otras muchas herramientas que son diseñadas para mejorar la ciberseguridad de los dispositivos, existe la que es seguramente la más conocida: el "antivirus". El software antivirus o "antimalware" funciona, sintiendo hacer referencia otra vez a la misma comparación y salvando las diferencias, como una vacuna. Estos softwares funcionan sobre todo a través de bases de datos que contienen información acerca de posibles amenazas para los dispositivos que les permiten identificarlas y bloquearlas en la medida de lo posible. La efectividad de estos, sobre todo en dispositivos personales que no guardan información especialmente susceptible de querer ser robada, es bastante alta, ya que los ataques que estos sufren son habitualmente derivados de malwares comunes o ya utilizados por muchos ciber-delincuentes (Oliveira, 2022).

3.2. HISTORIA DEL SECTOR DE LA CIBERSEGURIDAD

A pesar de que hayamos mencionado que independientemente de que un dispositivo esté o no conectado a la red puede ser atacado, en lo relativo a los orígenes de la ciberseguridad, el nacimiento del internet y la conexión en red es inmediatamente anterior a la creación de los cimientos de la ciberseguridad.

Fue durante la década de los años sesenta cuando las primeras redes de ordenadores fueron capaces de sostener los primeros tráficos de información entre dispositivos ordenadores a distancia. Esto ocurría en los Estados Unidos, donde uno de los trabajadores involucrados en ese mismo proyecto de tráfico de paquetes de datos a distancia (ARPNET) creó Creeper, el programa que auguraba los posibles peligros que esta nueva tecnología podría traer. Creeper era un programa que de manera autónoma desde el momento en el que este trabajador, Bob Thomas, lo lanzó, se propagaba entre dispositivos, alterando su funcionamiento e interrumpiendo para simplemente hacer aparecer un mensaje: "Soy Creeper. Atrápame si puedes". Otro compañero de este prestigioso equipo de investigadores, Ray Tomlinson, fue precisamente el que diseñó el primer software de seguridad que neutralizaba el experimento de su compañero y prevenía a los dispositivos de ser "contagiados". Creeper, y Reaper, el antimalware diseñado por Tomlinson, son el inicio del sector de la ciberseguridad (Hidalgo, 2021).

A la vez que el internet, el uso de este para fines delictivos crecía a pasos agigantados, y por eso, en la década de los setenta, en los Estados Unidos, como no, a manos de la conocida empresa tecnológica IBM y con la colaboración de la NSA se desarrolló el DES (Estándar de Cifrado de Datos). Este fue el comienzo de la aplicación del cifrado para la protección de los datos en la nube, o, en otras palabras, el primer protocolo. No era un protocolo especialmente robusto, sin embargo, fue adoptado y utilizado por gran parte de la comunidad hasta el principio del siguiente siglo.

Todo lo ocurrido hasta entonces no eran más que los primeros pasos del mundo de la cibernética. Fue en la década de los ochenta cuando las grandes empresas, instituciones y entidades, empezaron a hacer un uso diario de la tecnología de red. Esto se convirtió en una oportunidad para los ciber-delincuentes, que empezaron a desarrollar cada vez más y más potentes malwares que infectaran los dispositivos con fines lucrativos. Cada vez estos virus eran más parecidos a lo que hoy en día se conoce y, de hecho, en el dispositivo del prestigioso experto en ciberseguridad alemán Bernd Fix fue donde se desarrolló el primer antimalware con la forma con la que los conocemos hoy en día. El informático desarrolló el software que identificaba la infección del virus Vienna y lo destruía. El software de ciberseguridad se propagaba más rápido que el malware para el que había sido programado, lo que consiguió erradicar la cepa del en ese momento tan popular virus.

La ciberseguridad era ya una necesidad para cualquier individuo que hiciera uso de los dispositivos digitales y como no, la necesidad se convirtió en negocio. Las empresas dedicadas a

ciberseguridad empezaron a multiplicarse y fue a manos de estos que se crearon los primeros programas de ciberseguridad o antivirus. Empresas que todavía hoy siguen siendo líderes mundiales en el sector, empezaron a hacer negocio vendiendo estos programas que tan útiles se convertían a medida que los "hackers" encontraban nuevas bazas con las que atacar.

De la mano sobre todo de Microsoft, con productos como Windows 95 o Internet Explorer, el internet ya estaba en millones de casas en todo el mundo. Con ello, el número de ataques a la información que se traficaba en la red y, por ende, el sector de la ciberseguridad eran cada vez más protagonistas en el día a día ya no solo de las empresas e instituciones, sino también de los particulares. La facilidad en el envío de cualquier tipo de información a través de un simple correo electrónico y la poca educación digital que tenía la sociedad se convirtieron en los mayores alicientes de la delincuencia cibernética. Mails estándares con malwares adjuntos se enviaban continuamente y como siempre, la seguridad continuaba por detrás de los delincuentes y los programas de ciberseguridad no eran suficientemente fuertes para frenar este crecimiento de la delincuencia digital sobre todo porque su mayor arma no era otra que la "ingeniería social" o aprovechamiento del fallo humano.

Finalmente, a partir del inicio del nuevo milenio, el mundo de la ciberseguridad empezó a parecerse más a lo que hoy en día conocemos. Los programas antivirus gratuitos, las redes virtuales privadas, la educación digital… han ido poco a poco haciendo frente a los delincuentes de internet y haciendo cada vez más difícil la tarea de lucrarse con herramientas como malwares. Esto, finalmente, ha llevado al oscuro negocio del ciberataque un paso más allá. Durante la década de 2010 el negocio de la ciberseguridad ha tenido como objetivo y tarea la protección de la información personal e interna de cada dispositivo, familia, corporación… La amenaza ya no es tanta la de los malwares que provocan una brecha en una red o el mal funcionamiento de un dispositivo, sino la del robo de información personal de las personas, producto cuya cotización en los mercados paralelos es cada vez más alta. Esto último, es el motivo por el cual el sector de la ciberseguridad ha experimentado un tan notable auge en los últimos años. El impacto económico de un robo de datos para un país o empresa es cada vez más grande, y es por esto por lo que el dinero que estas mismas entidades están dispuestas a invertir en estar ciber-protegidas es cada vez mayor (Oliveira, 2022).

3.3. MEGATENDENCIAS EN CIBERSEGURIDAD

3.3.1. Los últimos días

A pesar de que el crecimiento de este sector sea por naturaleza acelerado, recientemente es cuando mayores cambios ha experimentado. Dos acontecimientos que a todos los sectores en mayor o menor medida han afectado, han sido especialmente notables en el sector de la cibernética y la ciberseguridad.

Por un lado, por culpa de la desgraciada guerra entre Ucrania y Rusia, hemos podido ver cómo ha llegado el momento en el que los ataques y amenazas más peligrosas entre los países se llevan a cabo a través de ataques cibernéticos consistentes en el pirateo de sistemas y robo de información confidencial. La Unión Europea ha hecho una de las mayores inversiones de ayuda al país invadido en un Equipo de Respuesta Cibernética Rápida, a la vista de los continuos ataques que la potencia rusa estaba realizando en contra de los sitios web oficiales y datos del estado ucraniano. Esto nos hace preguntarnos muchas cosas a las que seguramente no podamos responder, pero desde luego nos deja clara la importancia de los datos y la ciberseguridad hoy en día.

El otro de los acontecimientos que han marcado esta rápida aceleración del sector y sin duda el más significativo es la pandemia de la Covid-19. El ya popular teletrabajo encontró en el aislamiento de las familias la mejor palanca para llegar para quedarse. Desde 2020, muchas empresas han ofrecido a sus trabajadores la oportunidad de trabajar desde sus domicilios. Esto ha supuesto una gran oportunidad para los desarrolladores de herramientas de teletrabajo como los programas de conferencias, pero también un aliciente para la delincuencia cibernética. La conexión y tráfico de datos intra-empresariales se hacían desde dispositivos y redes familiares, los que habitualmente son mucho más vulnerables que los de las empresas sobre todo por la falta de inversión en medidas de ciberseguridad que hay en los ordenadores y redes domésticas. Asimismo, el auge del comercio digital ha supuesto también un crecimiento en las estafas durante las transacciones en internet (IBM, 2023).

3.3.2. Amenazas más comunes

Al igual que los virus mutan para siempre ir por delante de la industria médica y farmacéutica, los ciberatacantes, habitualmente expertos informáticos, consiguen estudiar las barreras que el sector de la ciberseguridad desarrolla para anteponerse a ellas y crear amenazas cibernéticas inmunes a las

defensas que pudieran desarrollarse. Aunque son miles las posibles armas con las que cuentan los delincuentes, a continuación, vamos a detallar las más comunes y habituales de la actualidad:

Programas maliciosos:

Los programas maliciosos son distintas formas de malware que consiguen provocar un acceso no autorizado a un sistema, así como dañarlo. Estos cada vez usan mejores técnicas para no ser detectados mediante las comunes herramientas de antivirus, entre otras. Uno de los factores importantes para ser cada vez más "sigilosos" es que ya no viajan en forma de archivo, lo que hace evitar sospechas y superar las barreras de detección que a veces, incluso la propia aplicación de email lleva instalado.

Ransomware:

A pesar de que el Ransomware sea un tipo de programa malicioso, es importante mencionarlo con exclusividad por la frecuencia con la que en los últimos años se han detectado ataques a manos de este tipo de programa. Concretamente, en 2022 un 17 por ciento de los ciberataques detectados se debían a uno de estos programas que se caracterizan principalmente por su forma de atacar, similar a la de un secuestro. El programa, una vez introducido en un dispositivo o red, bloquea sistemas, datos o archivos y amenaza a los propietarios con destruirlo o publicarlos en el caso de no recibir una compensación o rescate. Las empresas y gobiernos estatales o locales son el objetivo favorito de los delincuentes que utilizan este tipo de ataques, ya que por capacidad están peor protegidos y necesitan de sus datos y aplicaciones para el buen funcionamiento de las herramientas de los ciudadanos. La información privada o confidencial es también muy susceptible de ser atacada por medio de este tipo de malware.

Phishing/ingeniería social:

El Phishing o ingeniería social es una forma que se utiliza hoy en día en el sector de la cibernética y la ciberseguridad entre otros ámbitos, para denominar el uso de una técnica tan ancestral como el engaño. Muchos de los delincuentes cibernéticos basan su ataque en intentar engañar a un usuario para obtener información valiosa como pueden ser unas simples claves de pago para atacar económicamente a la víctima, una contraseña para obtener información con la que atacar o el acceso a un dispositivo o red para difundir un malware. Esta técnica basa su éxito en la vulnerabilidad humana

y es por esto que muchos organismos policiales y gubernamentales hacen tanto hincapié hoy en día en la protección de los datos personales.

Amenazas internas:

Al igual que la fórmula anterior, este tipo de ataque, también de los más comunes, tiene como pilar la vulnerabilidad y sobreconfianza humana. No siempre que somos ciberatacados lo somos a manos de un ciberdelincuente externo, de hecho, muchos de los problemas que tienen las empresas y los individuos en materia de ciberseguridad vienen tras brindar la confianza a una persona cerca como puede ser un empleado, stakeholders y cualquiera al que se le hayan concedido permisos de acceso sin suficiente control.

Ataques de denegación de servicio distribuido (DDoS):

No es tanto un ataque de robo de información sino un intento de "romper" o estropear una red gracias al lanzamiento de cantidades enormes de falsas solicitudes de tráfico, lo que colapsa la red y hace que el tráfico normal de la información no pueda llevarse a cabo. En otras palabras, el objetivo del delincuente en este caso no es tanto el de lucrarse de alguna forma si no el de perjudicar a los usuarios de una determinada red mediante el lanzamiento masivo de solicitudes.

Amenazas persistentes avanzadas (APT):

Otra de las técnicas que más se ven en los últimos días es la del espionaje cibernético o APT. Los delincuentes que usan esta técnica se introducen en una red o sistema sin alterar las redes ni los dispositivos, de modo que pasando desapercibidos, pero ya con acceso a la información interna, espían durante un periodo de tiempo de manera continúa extrayendo información relevante sin alterarla o intentar perjudicar la red o sistema.

Un ejemplo muy sonoro sobre este tipo de práctica ha sido el ataque a Solar Winds. En resumidas cuentas, Solar Winds ha sido la empresa que en un inicio fue la puerta de entrada a programas y códigos utilizados por miles de empresas y organizaciones en el mundo. Los delincuentes consiguieron quebrantar la ciberseguridad de esta empresa y acceder a códigos tan importantes como los de los softwares de Microsoft o archivos secretos de los Estados Unidos. Aunque podría ser comparable con otros miles de ataques, la importancia de los códigos a los que ha conseguido acceder,

así como el hecho de que la hipótesis más consistente sea que los atacantes fueran parte del gobierno ruso, hacen que este ataque, consistente en espionaje durante un periodo de tiempo todavía sin conocer, hay sido tan comentado en el sector y fuera de él.

Ataques de intermediario (man-in-the-middle):

Por último, podemos meter en el saco de los ciberataques más comunes el ataque de intermediario que, como el propio nombre indica, se trata de ataques en los que el ciberdelincuente consigue introducirse en medio de un intercambio de información entre dispositivos a través de una red no segura, accediendo a toda la información que viaje en ese flujo entre los dispositivos que se encuentren dentro de esa red. Las redes no seguras más comunes son habitualmente las públicas o de acceso fácil (Fortune Business Insights, 2022).

3.3.3. Principales herramientas de ciberseguridad

Después de haber comentado las amenazas más comunes a las que se enfrenta el sector de la ciberseguridad, es importante que el lector conozca las más importantes defensas con las que se cuenta hoy en día. A pesar de ser un sector en continua evolución, existen ciertas tendencias que seguramente continuarán siendo importantes bazas para prevenir o contrarrestar los ataques a manos de los hackers y delincuentes cibernéticos. Con ellas, las herramientas que los expertos en ciberseguridad más utilizan hoy en día son las siguientes:

La gestión de accesos e identidades (IAM)

Como su propio nombre indica, la conocida como IAM es la gestión de los accesos de los usuarios a una red o dispositivo. Esto, como puede intuir el lector incluye muchos procesos relacionados con los accesos. Entre los más importantes o conocidos podemos citar la obligación de las contraseñas seguras o la doble verificación a la hora de ingresar credenciales de accesos. Además, la IAM también se encarga de determinar que permisos o accesos se le conceden a cada usuario, dependiendo, por ejemplo, del rango o las tareas a realizar que tenga un empleado dentro de la empresa u organización. Con todo esto, se convierte en una herramienta muy importante para la investigación de la vida de un usuario, ya que al igual que se determinan los accesos que tiene cada uno de estos, se gestiona y vigila cómo y a dónde accede cada uno en cada momento.

Plataformas integrales

Se refieren a plataformas que tienen en cuenta todo tipo de casuísticas para así garantizar la seguridad de los datos internos. Gracias a estas plataformas, los gestores se aseguran de tener toda la visibilidad posible de los movimientos, entradas y salida que se hagan en la plataforma. Además, este tipo de plataformas cuentan con bases de datos que hacen mucho más fácil detectar las amenazas o vulnerabilidades a las que se pueden enfrentar en cada momento. También se encargan de cumplir con los reglamentos y normativas a los que deba hacerlo en el lugar y sector en el que se lleve a cabo la actividad de esa plataforma. Asimismo, y de manera obvia, garantiza el cifrado continuo de los datos y procesos.

Gestión de sucesos e información de seguridad (SIEM)

Es una de las herramientas más eficientes hoy en día. Su función ya ha sido mencionada anteriormente en este trabajo y es la de crear bases de datos que "aprendan" acerca del histórico de ciberataques recibidos por este u otro software para así detectar indicios que levanten sospechas de estar recibiendo un posible ataque. Las soluciones SIEM hoy en día llevan esta técnica aún más allá con la relativamente reciente incorporación de la IA (Inteligencia Artificial) que no solo basa sus diagnósticos en datos históricos de ciberataques, sino que también detecta patrones de comportamiento en la red potencialmente peligrosos. Además, estas soluciones ya son capaces de, de manera autónoma, dar respuesta a estos ciberataques, conduciendo al usuario a sitios cada vez más seguros en función de las sospechas que la inteligencia artificial detecte en el uso de la red (IBM, 2023).

Inteligencia artificial (IA)

A pesar de no poder denominarse una herramienta de ciberseguridad como tal, ya que su utilidad abarca prácticamente todos los ámbitos en la actualidad, la inteligencia artificial, como se ha mencionado en el anterior párrafo, se está incorporando cada vez más en todas las herramientas de ciberseguridad. Esta forma de tecnología, cada vez más accesible para todos con incorporaciones de softwares y programas que la integran como la tecnología GPT, basa su creciente éxito en la réplica del comportamiento humano con la incorporación de habilidades como el razonamiento, aprendizaje e incluso creatividad (Parlamento Europeo, 2021). Esto, como se puede intuir, es increíblemente beneficioso para el sector de la ciberseguridad que muchas veces encuentra sus mayores debilidades

en la brecha entre el factor humano con el que cuenta el atacante y no la máquina o software de ciberseguridad.

3.4. CIBERSEGURIDAD INTERNACIONAL, EUROPA

En una sociedad en la que el tráfico y almacenamiento de datos se lleva a cabo en su gran mayoría mediante herramientas digitales, la seguridad internacional no debe dejar pasar el momento de incorporar medidas relativas a las posibles amenazas digitales. Los países encuentran hoy en día sus mayores vulnerabilidades en la protección de su información. Es por ello por lo que las alianzas internacionales cada vez incorporan más medidas anti-ciberdelincuencia. La Unión Europea como es de esperar, no se queda atrás en este aspecto y desde el año 2016 cuenta con un Reglamento General de Protección de Datos (RGPD). Este reglamento está en continuo estudio y renovación y tiene como objetivo la protección de los datos personales de las personas físicas, implicando también a las empresas, organismos y sus formas de gestionar las bases de datos personales. La Unión Europea es la encargada de la designación de distintos organismos nacionales que lleven a cabo las labores de implantación y control de todas las medidas y leyes que todavía siguen entrando en vigor en el RGPD.

Entre las distintas medidas y herramientas que la Unión Europea ha incorporado recientemente podemos destacar algunas de ellas:

1. En marzo del año 2021 el Consejo Europeo sacó a la luz una nota de prensa acerca de las Conclusiones sobre la estrategia de Ciberseguridad. A través de esta nota de prensa, el Consejo dejó clara la senda que la Unión Europea iba a seguir en materia de ciberseguridad. Muy en línea con los ODS, la nota de prensa dejaba clara la importancia de la ciberseguridad en busca de una Europa resiliente, ecológica y digital. Entre las propuestas para el futuro anunciadas en esta nota de prensa destacan una Directiva actualizada para proteger mejor las redes y los sistemas de información y una nueva Directiva sobre la resiliencia de las entidades críticas.

2. Sistema de certificación de la ciberseguridad a escala de la UE. Se refiere a las certificaciones que la Unión Europea emite en busca de homogeneizar los productos, servicios y procesos existentes en los mercados y que muchas veces generan desconfianzas al usuario por la excesiva variedad ofertada en los distintos países.

3. La Agencia de la UE para la Ciberseguridad o Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) es simplemente una reforzada Agencia centralizada mucho más capacitada que la anterior para asistir a todos los países miembros ante posibles ciberataques.

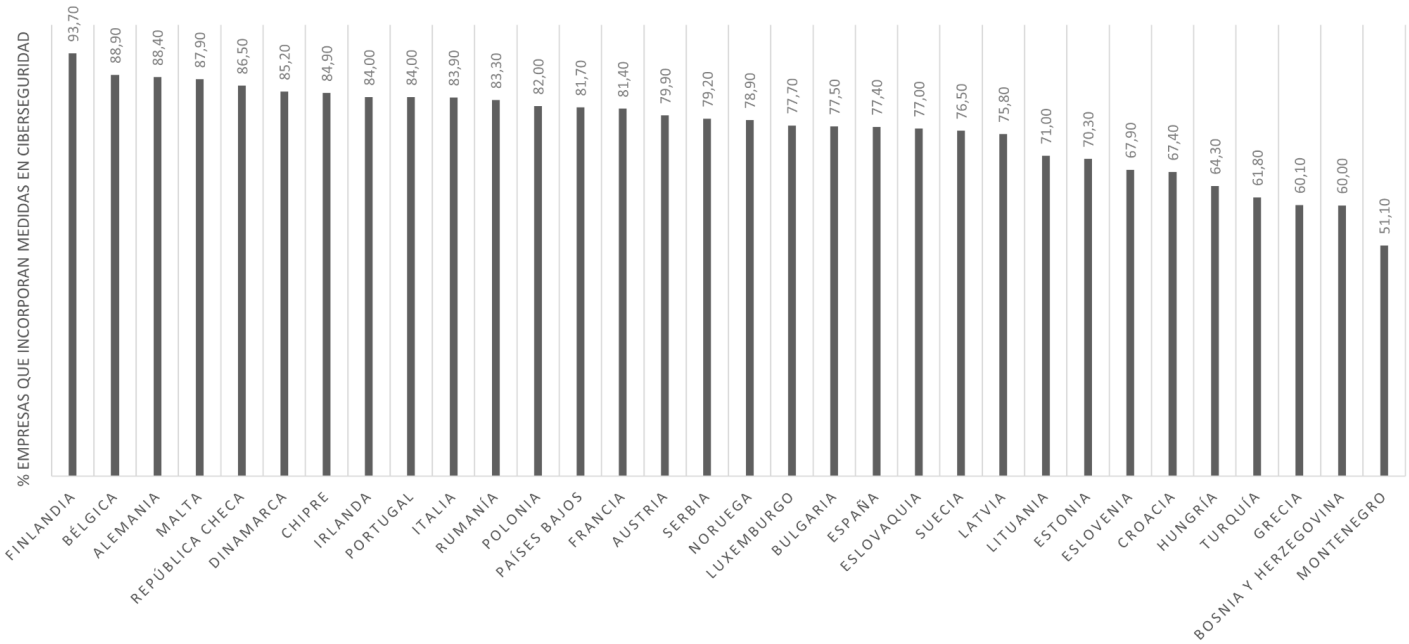
4. Creación del Centro Europeo de Ciberdelincuencia, dedicado a apoyar a los países miembros a investigar y desmantelar redes de delincuencia cibernética sobre sobre todo dedicadas a ataques que verdaderamente dañen a las víctimas, como puede ser la explotación sexual de menores en línea. La herramienta principal de este Centro Europeo de Ciberdelincuencia es la plataforma multidisciplinar europea contra las amenazas delictivas (EMPACT).

Además de todas estas novedades se encuentran otros diversos caminos relacionados con el sector de la ciberseguridad en los que la Unión Europea está invirtiendo mucho. Entre ellos se encuentra la inversión en cifrado, justicia y acción policial digital, conservación de datos e impulso de la ciberdemocracia entre otros muchos objetos de inversión. Tanta es la importancia de la ciberseguridad para los organismos europeos que el Plan Estratégico Europa Digital (2021-2027) se detalla una inversión de 1.600 millones de euros en ciberseguridad, ciberseguridad desarrollada a través de los objetivos que hemos detallado anteriormente, así como de organismos internacionales que favorecen la consecución de los anteriormente mencionados. Un importante ejemplo de estos organismos recientemente desarrollados o mejorados es el Centro Europeo de Ciberdelincuencia, dentro de la Europol, el organismo policial internacional europeo (Consejo de la Unión Europea, 2023).

3.4.1. Ciberseguridad en las empresas europeas

Habiendo visto resumidos los distintos avances logrados en este sector en la Unión Europea, es importante mencionar además la situación que las empresas europeas perciben en lo relativo a su ciberseguridad. Estas compañías se sienten cada vez más respaldadas por las herramientas y regulaciones que la UE incorpora, como las arriba mencionadas. No hay que olvidar que fuera de los organismos públicos europeos existen cada vez más empresas dedicadas a ofrecer servicios de ciberseguridad, así como el sector asegurador, que cada vez experimenta una mayor demanda en pólizas preventivas de siniestros digitales. Concretamente, en Europa existen más de 60.000 empresas de ciberseguridad y más de 660 centros especializados en el sector (Consejo de la Unión Europea, 2023).

Como en el resto de los sectores, los distintos países que componen la Unión Europea no reman al unísono en lo relativo al buen hacer en ciberseguridad de las empresas. Este "buen hacer" es medible de muy distintas maneras. Según los últimos estudios estadísticos realizados en 2023 por Eurostat, la Oficina Estadística de la Unión Europea, acerca del porcentaje de empresas que incorporan medidas de protección cibernética, se puede considerar que una empresa cumple esta característica si se encarga de que se cumplan siempre las medidas de autenticación de las contraseñas utilizadas por todos los usuarios, tanto internos como externos, de la compañía. Tratando estos datos, obtenemos los siguientes resultados sobre el porcentaje de las empresas de más de diez trabajadores de cada país que cumplen con esta característica:



Gráfica 1:Porcentaje de empresas que incorporan medidas de ciberseguridad en los países de la Unión Europea en 2022

Fuente: Elaboración propia, datos de encuesta Ciberseguridad en empresas (Eurostat).

Tal y como puede observarse en la Gráfica 1, los datos son relativamente buenos en la mayoría de los casos, sin embargo, el gráfico no refleja una realidad del todo consistente teniendo en cuenta la seguridad de las empresas. La medida que considera Eurostat a la hora de realizar el estudio ha sido probablemente elegida por la facilidad de su medición, es decir, es un dato que cierra la encuesta en dos posibilidades, lo que facilita su análisis. Para llevar esta investigación al siguiente nivel y tratar de reflejar de manera más realista la situación de las empresas de los países europeos habría que hacer un estudio mucho más detallado de una serie de variables más específicas pero que, en definitiva, dificultarían mucho la extracción de datos para esta muestra de tan grande tamaño.

A pesar de esto, estos datos sí son válidos para reflejar la diferencia entre países en materia de ciberseguridad. Aunque el cumplimiento de la autenticación de contraseñas no sea suficiente para calificar como correcta la ciberseguridad de una empresa es evidente que es una norma que una empresa que trabaja su seguridad cibernética cumple en la mayor parte de los casos. En base a esto, y habiendo ordenado los resultados del estudio de mayor a menor, podemos observar cómo países como Finlandia, Bélgica y Alemania cuentan con un tejido empresarial digitalmente más seguro que los demás, siendo Grecia, Bosnia y Herzegovina y Montenegro aquellos con las empresas digitalmente menos seguras. A pesar de no ser variables directamente proporcionales, el lector, tras ver estos resultados puede lógicamente percibir como el nivel de vida, economía e innovación, favorece la ciberseguridad de las empresas.

3.5. LOS CAMINOS HACIA UNA SOCIEDAD CIBERSEGURA

Anteriormente hemos analizado, de manera muy superficial la situación pasada y actual del sector de la ciberseguridad, pero antes de focalizar el tema en el mundo de la empresa es importante que el lector entienda los siguientes pasos de la sociedad en materia de ciberseguridad. A pesar de que no todo el planeta vaya alineado en cuanto a lo que respecta a estos objetivos, sí se pueden identificar ciertas sendas que muchos de los países y organismos internacionales desean seguir en este aspecto. Los derechos humanos y la calidad de vida de las personas juegan un papel importante en este camino ya que cada vez más, la seguridad digital es un derecho del que las personas en todo el mundo hacen uso día tras día.

En línea con lo mencionado sobre la parte más personal de la ciberseguridad, uno de los caminos que el sector claramente ha empezado es el de la protección de datos personales. En el apartado anterior se mencionaban algunas medidas y normativas aplicadas para la protección de datos personales, como puede ser el RGPD, sin embargo, las autoridades admiten que este es todavía un gran reto y objetivo que resolver por lo que los esfuerzos seguirán siendo grandes en este aspecto.

Las autoridades regulatorias además promueven no solo planes de prevención sino también importantes avances en la normativa penalizadora para todo tipo de ciberataques o malos usos de los dispositivos e información digital. Con todo esto además se incorporarán mayores medidas de seguridad en todos los tipos de transacciones cibernéticas, desde compraventas hasta meros flujos de información entre dispositivos remotos.

Las empresas han ido poco a poco incorporando sistemas y dispositivos digitales durante años. Los empleados se han formado con los años y son ahora expertos en el uso de múltiples herramientas digitales distintas pero esta diversidad de plataformas se ha convertido en un enemigo en lo que se refiere a ciberseguridad. A raíz de la reciente explotación del teletrabajo y acceso remoto a la información empresarial, se han creado brechas de seguridad, las cuales han sido, en muchos casos, objetivo de los ciberdelincuentes. Es por esto por lo que la senda que ahora han tomado las empresas es la de reducir en la medida de lo posible el número de plataformas o programas utilizados por los empleados, para así centralizar la información y los procesos, creando un entorno cibernéticamente más seguro.

A partir de este 2023, las empresas están tomando el riesgo de ciberataque como uno de los tres principales riesgos de la empresa. Es por esto que se prevé que, en los próximos años, sobre todo en las grandes empresas se designen cargos de altos directivos encargados únicamente de labores y control de ciberseguridad empresarial. Esto es muy importante no solo en el aspecto de la información sino también en el económico ya que, de media, las empresas pierden, según la encuesta recientemente realizada por la consultoría Price Waterhouse Cooper (PWC) en este 2023, 2,17 millones de euros al año por culpa de incidentes de ciberseguridad.

3.6. LA SITUACIÓN DEL SECTOR EN ESPAÑA

Para culminar este apartado relativo a la situación de la ciberseguridad es importante explicar la situación que vive este sector en España. Para ello, es vital mencionar la importancia del Instituto Nacional de Ciberseguridad (INCIBE). INCIBE es una entidad dependiente del estado encargada de la investigación y oferta de servicios en busca de construir ciberseguridad nacional e internacional en España. La entidad realiza diagnósticos anuales y accesibles para todos que detallan de manera muy precisa las principales métricas y casuísticas de la ciberseguridad anual en el último año. Esta se convierte en una herramienta muy útil para situar al lector de este trabajo de investigación en cuanto a la situación que el Estado atraviesa en este aspecto.

En el último informe de situación de INCIBE (2023), relativo al diagnóstico del año 2022, se confirman ciertas tendencias que el lector ha podido identificar a lo largo del documento. El número de ataques o casos de incidencias sigue en aumento, también en España. Según los registros, se han registrado un 8,8 % más de incidentes en España, de los cuales, en torno a un 40 % se han considerado

de peligrosidad alta, muy alta o crítica. Esta peligrosidad se estima en función de la gravedad de las consecuencias o posibles consecuencias que un ataque puede tener.

Un dato especialmente destacable para el objeto de este proyecto que el informe de INCIBE nos ofrece es el relativo a los ataques a las empresas. Del total de ciberataques gestionados en España, un 52 % ha sido sufrido por las empresas. Lo más destacable de esto es que tras los análisis de cada uno de los casos, se ha detectado que, en 9 de cada 10 ciberataques sufridos por las empresas, el origen no es otro que la vulnerabilidad de los sistemas de información internos. Esto significa que en la no actualización o la mala configuración de los sistemas informáticos de las empresas, los ciberdelincuentes encuentran su más importante y fácil vía de actuación.

Es importante mencionar que el sector académico es una importante diana para los atacantes de internet. Las patentes, estudios y otro tipo de información vulnerable y atractiva para ser robada es la mayor fuente de valor de las redes universitarias. Por eso, es un gran reto para ellas optimizar sus sistemas de información en busca de proteger su propiedad intelectual, así como la de los alumnos, profesores y otros profesionales que componen este sector. Desde la UPV-EHU sin ir más lejos y también durante el año 2022 hemos podido ver cómo por culpa de ataques como estos incluso los alumnos hemos tenido la obligación de cambiar todos nuestros datos de accesos a las redes internas. Sin embargo, estos son casos puntuales y de especial importancia, pero desde la Universidad informan de que estos ataques son recurrentes y diarios. A pesar de que los objetivos del trabajo están principalmente orientados al sector empresarial, sin duda y como veremos más adelante las conclusiones serán en muchos casos válidas para sectores como el académico o la propia ciberseguridad de las personas físicas.

Ya hemos dado a conocer que las empresas son el principal objetivo de los ataques por parte de los delincuentes digitales. A pesar de esto, resulta importante mencionar como dentro del mundo de la empresa existen ciertos sectores especialmente vulnerables o atractivos para los delincuentes digitales. Los sectores de la energía, el agua, el transporte y el sector financiero y tributario son el objetivo de nada menos que el 90,1 % de los ataques que reciben las empresas. Es lógico pensar que estos sectores abarcan gran parte del conjunto de ciberataques a empresas porque también forman la mayoría del tejido empresarial, pero este no es el único detonante para ser los más atacados. Sectores como estos son atractivos para los delincuentes digitales por un lado por las grandes cantidades de dinero que en ellos circula, lo que puede ser atractivo para generar una brecha que en

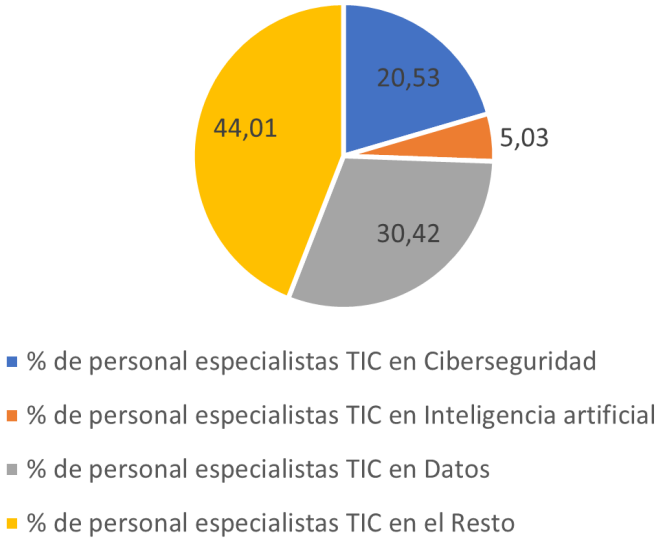
términos económicos no sea tan importante para las empresas, pero sí lo sea para los atacantes y por el otro, porque en muchos casos son sectores alejados de la innovación tecnológica en la actividad principal, lo que hace también no tener tan presente el reto de la ciberseguridad. Lógicamente esta tónica está cambiando y para las empresas de estos sectores, como de la mayoría, la ciberseguridad es uno de los retos más sonoros e importantes.

3.6.1. Estadísticas relevantes, TIC y Ciberseguridad en España

Además, el documento de INCIBE ofrece el mapa de la ciberseguridad en el que se detalla el número total de dispositivos vulnerables (puntos de conexión a internet en los que se ha detectado una posible vulnerabilidad o facilidad para un potencial ataque digital) detectados divididos por provincias. En relación con esto y en línea con los objetivos del proyecto de investigación es importante mencionar que las provincias vascas se encuentran por detrás; es decir, con menos puntos vulnerables, que provincias como Madrid, Barcelona, Valencia o Sevilla.

Además de INCIBE como principal agencia nacional de ciberseguridad, como siempre podemos encontrar datos estadísticos relevantes a este tema en el INE. Anualmente, el Instituto Nacional de Estadística realiza durante el primer trimestre una encuesta relativa al uso de las TIC en las empresas. De esta encuesta es de donde el autor ha podido sacar algunos datos que pudieran ser relevantes para la contextualización más cuantitativa del sector de la ciberseguridad en España.

Al haber utilizado datos estadísticos de empresas con más de diez empleados para el estudio de la situación europea, el autor ha considerado oportuna la elección de la población contraria en el caso de España. En este caso, tras analizar los resultados de la encuesta, se ha decidido formar conjuntos determinados para su representación en gráficas, tratando de sintetizar la información obtenida.

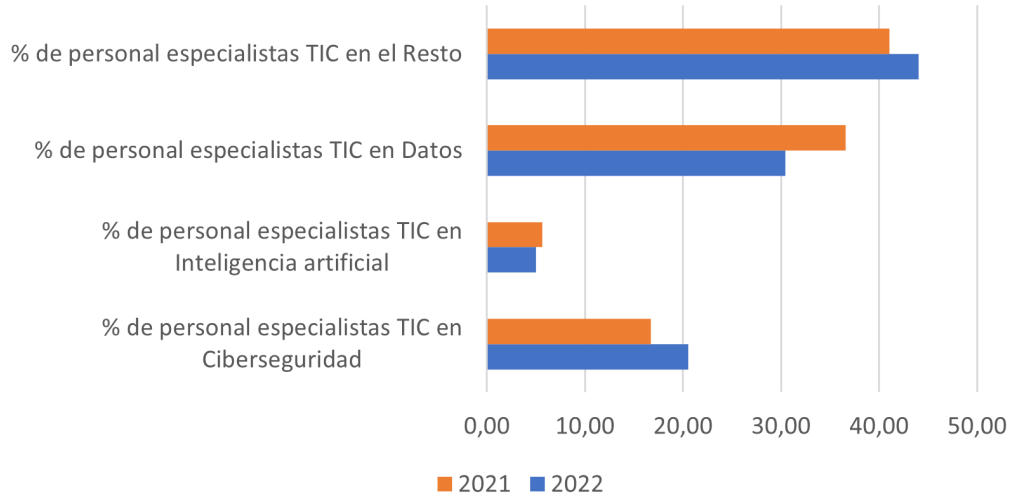


Gráfica 2: Porcentaje de especialistas TIC de cada rama en las empresas españolas 2022

Fuente: Elaboración propia, datos de encuesta uso de las TIC empresas españolas (INE, 2022).

En primer lugar, y como primera extracción, mostramos la Gráfica 2 relativa a la encuesta más reciente (INE, 2022). Es interesante percibir cómo, aunque exista un pensamiento extendido en la sociedad de que los datos son el empleo de moda, las empresas emplean a 2 expertos en ciberseguridad por cada tres que emplean en Data.

El análisis resulta aún más interesante esta extracción con un análisis de evolución de datos 2021-2022.

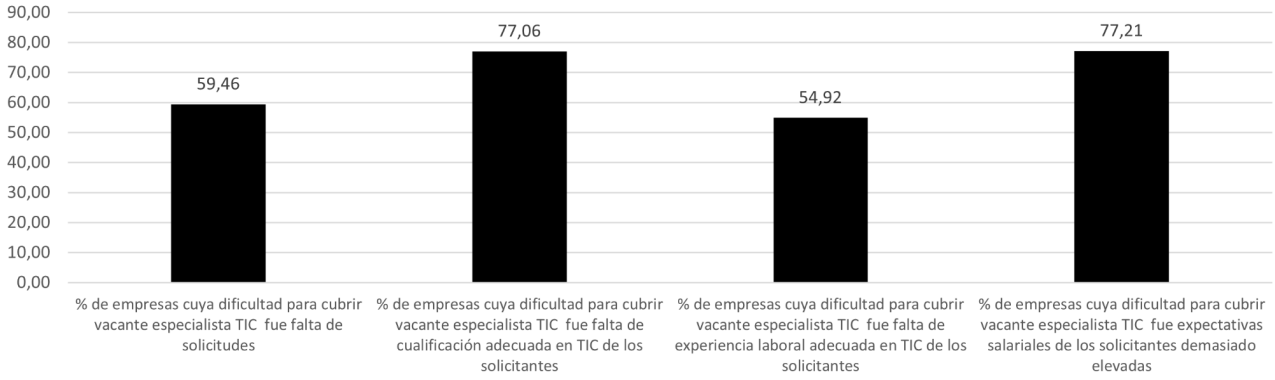


Gráfica 3: Porcentaje de especialistas TIC de cada rama en las empresas españolas 2022 comparado con 2021.

Fuente: Elaboración propia, datos de encuesta uso de las TIC empresas españolas (INE, 2021 y 2022).

Como podemos observar en la Gráfica 3 la necesidad de especialistas en ciberseguridad se incrementa en las empresas españolas en el año 2022. Junto con ellos, los especialistas TIC en empleos distintos a los contemplados también experimentan un aumento dentro de las empresas. Estos incrementos se compensan con el decremento del porcentaje de especialistas en Datos, cuyo reciente "boom" empieza a verse mermado.

En muchos casos, la búsqueda de perfiles especialistas en TIC, incluidos los de ciberseguridad, no depende exclusivamente de la demanda de las empresas. En esta encuesta, las empresas también respondieron a esta consulta y los resultados revelan una realidad muy llamativa en la Gráfica 4.



Gráfica 4: Porcentaje de origen de la dificultad de encontrar especialistas TIC en las empresas españolas 2022.

Fuente: Elaboración propia, datos de encuesta uso de las TIC empresas españolas (INE, 2022).

Como podemos comprobar, la encuesta revela que los problemas a los que se enfrentan las empresas a la hora de buscar perfiles especializados en TIC son principalmente la insuficiente cualificación de los solicitantes y sobre todo las elevadas expectativas salariales de estos. También son problemas para más de la mitad de las empresas encuestadas y que hayan tenido problemas para cubrir estas vacantes la falta de solicitudes y la falta de experiencia de los solicitantes. Con estos resultados podemos concluir que a pesar de ser hoy en día uno de los perfiles para el que más personas trabajan en conseguir, todavía el mercado laboral sigue ofreciendo pocas personas cualificadas y suficientemente experimentadas en el sector, lo que dificulta y encarece los procesos de selección.

Por último, como datos a resaltar de la encuesta además de los recién mencionados, son destacables los resultados de que solo el 3% de las empresas españolas de menos de diez trabajadores proporcionan formación en TIC a sus empleados y que solo en el 25,85% de ellas es el personal interno el que realiza las labores TIC.

4. EMPRESAS Y CIBERSEGURIDAD

El lector, tras la lectura del documento hasta este punto podría ser capaz de, inspirándose al menos en lo que podemos denominar este "marco teórico" y reunión de datos, realizar un diagnóstico muy general de la situación que atraviesa y ha atravesado el mundo y las empresas en lo relativo a la defensa contra potenciales ciberataques. Sin embargo, como introducción a la verdadera resolución de los objetivos planteados al inicio de este proyecto de investigación, consideramos conveniente resumir en distintos puntos todo lo estudiado hasta este punto. Diagnosticar la situación actual del sector sin centrarse tanto en los objetivos del trabajo nos ayudará a encontrar similitudes y diferencias entre el panorama internacional y el vasco, que es en definitiva la relativamente pequeña población objetivo-escogida. Por esto, se alejará la mirada del mundo tan técnico y complejo que es la ciberseguridad para tratar de sintetizar todo lo aprendido de una forma más "llana", enumerando una serie de ideas que introduzcan al lector a la lectura del apartado más importante o llamativa del proyecto:

1. Cualquier tipo de información interna o privada de las empresas es susceptible de ser robada o atacada por los delincuentes cibernéticos. Por muy insignificante que parezca, cualquier dato es valioso para ser utilizado en contra de la empresa o incluso para acceder de forma más fácil a otros datos que pudieran ser más delicados o importantes para la empresa.

2. Desde el punto de vista internacional o nacional, es innegable que existen progresos en la regulación o normativa en contra de los ciberataques o incluso a favor de la prevención de estos en las empresas. Sin embargo, la ley todavía sigue muy por detrás en este sentido y las empresas se ven en muchas ocasiones poco protegidas por los organismos públicos legislativos ante potenciales daños sufridos por ataques digitales.

3. Muchas empresas no le dan la suficiente importancia a este problema, lo que hace que, de manera demasiado frecuente, estas sean atacadas por pequeñas negligencias o malos usos de sus plataformas y herramientas digitales. Todavía, la ciberseguridad se percibe en muchos casos como un reto futuro y muchas compañías no son conscientes de datos tan abrumadores como que las PyMEs españolas reciben de media treinta mil ciberataques diarios (CEO ASSECO, 2023).

4. Los dirigentes políticos no invierten suficiente tiempo en el estudio y cuidado del sector de la seguridad y lo ponen por el momento por detrás de otros muchos sectores cuando en la realidad, hoy en día, los datos nos confirman que es un problema real para las empresas y la producción de los países. Su labor es pobre no solo en la acción sino también en la concienciación de las personas y compañías, algo que es primordial para preparar a la sociedad contra este peligro real.

5. El error o falta de precaución humana es en muchos casos la vía de ataque de los delincuentes cibernéticos. Si la empresa quiere desarrollar un entorno digital seguro, de nada le va a servir invertir en herramientas o primas de seguros de ciberseguridad si antes no ha concienciado a sus empleados en las más básicas técnicas y procedimientos preventivos de ciberataques. Esto, como es lógico es un problema para las empresas, sin embargo, también es un reto de la sociedad educar a los habitantes en la ciberseguridad.

Estos puntos dividen claramen5e las necesidades de las empresas en ciberseguridad en cuatro grandes bloques: Político, Jurídico, Empresarial y Educativo o de formación de las personas. A partir de este punto, se atacarán los objetivos del proyecto desde esta perspectiva.

5. EL CASO EUSKADI

Tras haber valorado la situación de la ciberseguridad de las empresas tanto en Europa como en España, es momento de realizar el mismo ejercicio con Euskadi para después, y con la ayuda de las conclusiones obtenidas del análisis de las bases de datos tanto recogidas en la nube como obtenidas personalmente por el autor, tratar de llegar a la consecución de los objetivos inicialmente planteados. Para ello, en un inicio se hará más uso de las estadísticas ya existentes recogidas para realizar el ejercicio de contextualización de la situación del sector en Euskadi, y después, mayor hincapié en las bases de datos creadas personalmente para, enfocar el resultado hacia el objeto del proyecto. Es importante destacar que al igual que sucede en otros ámbitos y sectores de actividad, Euskadi está bien posicionada en lo referente a la ciberseguridad e innovación relacionada con ella. Existen ejemplos para sostenerlo como la reciente noticia de la creación de la "cybertzaintza" o policía en contra de la delincuencia digital (El Correo, 2023).

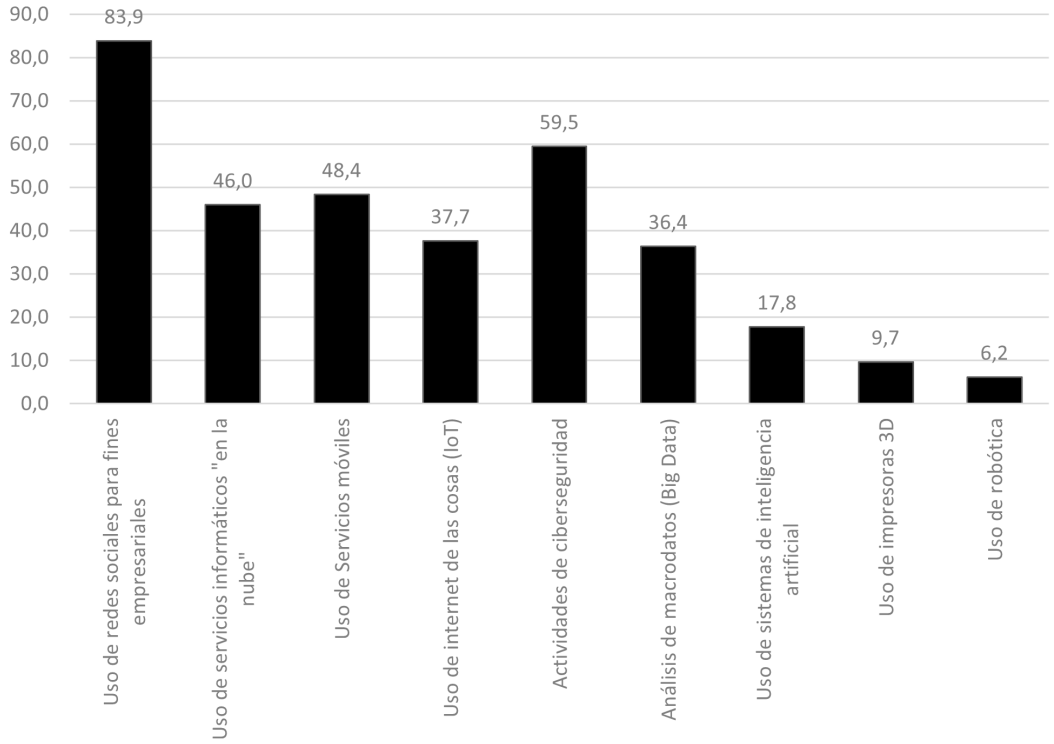
En línea con lo comentado anteriormente, la labor e iniciativa de Basque Cybersecurity Center (BCSC) es muy importante en este aspecto. La agencia, puntera a nivel estatal e incluso europeo en labores de ciberseguridad realiza importantes proyectos e iniciativas para la mejora de la ciberseguridad, sobre todo de las empresas. Entre otras muchas iniciativas importantes, se destaca el Informe Anual de Ciberseguridad, cuya última actualización ha sido extraída por el autor para su análisis y utilización en este punto del proyecto.

5.1. SITUACIÓN DE LA CIBERSEGURIDAD EN LAS EMPRESAS VASCAS

Tal y como se ha hecho con el caso de la situación europea y española, para realizar conclusiones y contextualizar el panorama del sector de la ciberseguridad en Euskadi se han obtenido los datos más recientes del Instituto Vasco de Estadística o EUSTAT. Al ser esta vez una población todavía más pequeña, el número de encuestas y datos fiables disponibles en la nube son todavía más reducidos; sin embargo, tras analizar y extraer ciertas comparables se puede plasmar una imagen representativa que se detalla a continuación.

Para empezar, es sabido por todos, pero no por ello no se debe mencionar que Euskadi es hoy en día una sociedad muy innovadora y puntera en lo referente a la digitalización de empresas. El gasto de las empresas vascas en innovación supera los 3.000 millones de euros anuales y es que además de

la propia identidad innovadora del tejido empresarial vasco, un 30,4% de las empresas que realizan tareas de digitalización y desarrollo en Euskadi reciben financiación pública para estas labores. Esto genera resultados óptimos para las empresas que apoyan este tipo de prácticas, las cuales llevan a que los productos innovadores generen de media el 36% de la cifra de negocios en sus compañías (EUSTAT, 2022). La diferencia entre las variables utilizadas para la creación del siguiente gráfico con las que el INE usa para valorar el uso de las TIC en las empresas españolas dificulta la comparación entre la situación de ambas poblaciones. En este caso, se verá reflejada la importancia de las TIC en Euskadi mediante la representación de su utilización diaria no en las empresas privadas, sino en la Administración pública.



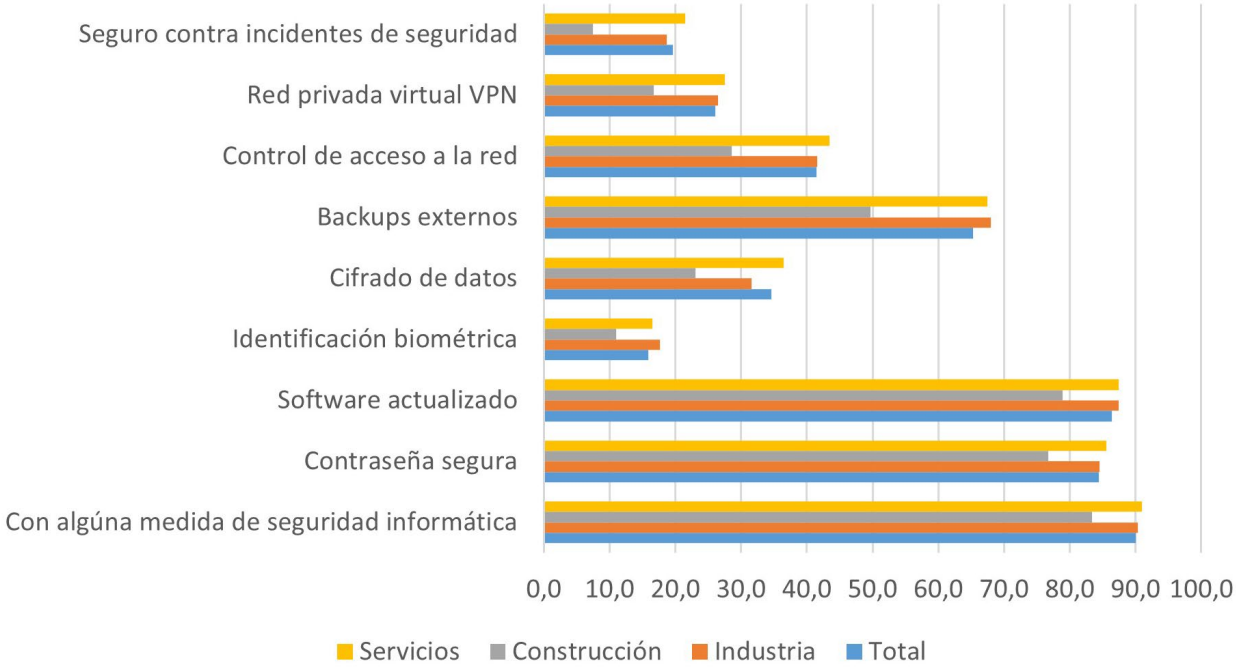
Gráfica 5: Porcentaje de establecimientos de la Administración Pública Vasca que hacen diferentes usos de las herramientas TIC.

Fuente: Elaboración propia, Fuentes de datos: Eustat. Encuesta sobre la sociedad de la información en la administración (2022).

En la Gráfica 5 se puede observar cómo incluso en el sector público, para Euskadi la tecnología es hoy en día un pilar fundamental. Además, como dato destacable, podemos mencionar el gran protagonismo de las actividades de ciberseguridad que realiza la Administración pública. Como ya se ha mencionado anteriormente en este documento, entidades públicas como la Universidad del País

Vasco afirman recibir ataques diarios de potenciales delincuentes digitales. Casos como este, hacen que cada vez más en los organismos públicos vascos se lleven a cabo importantes tareas de prevención.

Los datos anteriormente mencionados resultan importantes para visualizar la importancia de las TIC y la Industria 4.0 en Euskadi. Sin embargo, Eustat ofrece datos muy curiosos y representativos con relación al objeto de este proyecto de investigación. Con el tratamiento de estos datos se ha logrado representar en la Gráfica 6 una realidad muy interesante.



Gráfica 6: Porcentaje de empresas de los diferentes sectores de actividad que incorporan las distintas medidas de ciberseguridad.

Fuente: Elaboración propia, Fuentes de datos: Eustat. Encuesta sobre la sociedad de la información. Empresas (2022).

De estos datos podemos extraer diferentes conclusiones importantes y que ayudan al lector a seguir formando un diagnóstico propio e inicial de la situación del sector de la ciberseguridad en Euskadi. En primer lugar, podemos observar que en total un 90 % de las empresas vascas incorporan alguna medida de ciberseguridad, llegando a ser un 91 % en el caso de las empresas del sector servicios (véase Gráfica 6).

Por otro lado, es importante destacar el hecho de que claramente y con mucha diferencia con en el resto de los sectores, la construcción es el ámbito en el que menos medidas de ciberseguridad se incorporan. No es la primera vez que vemos algo similar en este trabajo de investigación. En el análisis

de las megatendencias del sector de la ciberseguridad descubrimos que hay ciertos sectores especialmente vulnerables a ser atacados por delincuentes digitales. En el caso de la construcción podemos concluir con lo contrario. Así como la energía (industria) o el sector financiero (servicios) son especialmente vulnerables e incorporan más medidas de ciberseguridad, la construcción no está tan necesitada de esto. Esto es porque la construcción es probablemente el ámbito en el que menos tráfico de datos se lleva a cabo de manera digital. Ni en la operativa ni tampoco demasiado en el Back-office el flujo de información digital está presente en la actividad de las compañías constructoras.

Una variable interesante por analizar en este caso por su similitud con otra utilizada en este documento es el uso de la contraseña segura. El lector quizás haya sido capaz de identificar que el uso de la contraseña segura es la misma variable de análisis que Eurostat utiliza para reflejar el porcentaje de empresas de cada país que incorporan alguna medida de ciberseguridad. Esta relación resulta muy útil para introducir a Euskadi en la población utilizada para la realización de la Gráfica 1 del documento. Este gráfico, ya explicado anteriormente arrojaba resultados como el de que en España un 77,4 % de las empresas utilizan contraseñas seguras. Comparando esto con el resultado de los análisis proporcionados por Eustat, podemos ver como Euskadi sube la media del estado en lo relativo a medidas de ciberseguridad (84,4 % teniendo en cuenta sólo la implementación de contraseñas seguras en las empresas), situándose a la altura de países punteros en este sentido como son los casos de Chipre, Irlanda o Portugal, tres de los diez mejor posicionados en la Unión Europea en este sentido.

Por último, otra variable a destacar de este último análisis es la incorporación de pólizas de seguros de ciberseguridad en las empresas vascas. Como podemos observar, no es algo con especial protagonismo en el año 2022; sin embargo, tras hablar con la correduría de seguros Asebrok, aseguran que el crecimiento de estas incorporaciones sobre todo en las grandes empresas crece a pasos agigantados, llegando a pagar precios muy elevados por este tipo de pólizas ya que, en muchos casos, cubren riesgos especialmente delicados para las compañías.

6. ESTUDIO EMPÍRICO

6.1. Diseño de trabajo de campo

Habiendo situado a Euskadi y sus empresas en el mapa en lo que se refiere a resultados estadísticos acerca de su ciberseguridad, mediante las fuentes de datos creadas personalmente (entrevistas y/o encuestas) vamos a tratar de, a continuación, realizar una valoración de la situación vasca en cada una de las ramas de acción o bloques de los que ya se ha hablado anteriormente en el documento: Político, Jurídico, Empresarial y Educativo o de formación de las personas. Estos bloques, a pesar de que se hayan comentado en los anteriores apartados del proyecto de investigación, no han sido seleccionados de manera aleatoria. A medida que hemos ido observando las megatendencias del sector hemos encontrado que precisamente estos cuatro son los puntos u orígenes desde los cuales, las empresas encuentran vulnerabilidades para mejorar su ciberseguridad.

Las fuentes serán creadas personalmente por dos principales motivos; las encontradas en la nube son escasas y además son notablemente subjetivas por estar escritas por compañías u organismos dedicados, en el día a día, precisamente a la actividad que están valorando. Por eso, para encontrar valoraciones mejor fundadas, la información finalmente utilizada para la consecución del siguiente apartado del trabajo de investigación ha sido la recabada mediante (véase Ilustración 4):

1. Entrevistas en profundidad realizadas a cuatro expertos en el sector, referentes en los 4 bloques de contenido resultantes del análisis bibliográfico: político, jurídico, empresarial y educativo.
2. Una encuesta realizada por dieciséis participantes relacionados con el mundo de la empresa en distintos ámbitos, con la intención de conocer la visión general de estos y valorar las sensaciones que desde dentro se tienen acerca de la ciberseguridad de las empresas.

Una vez finalizado el análisis de resultados y el diagnóstico final, el proyecto de investigación debería posibilitar una primera identificación de las respuestas o soluciones a los objetivos planteados inicialmente.

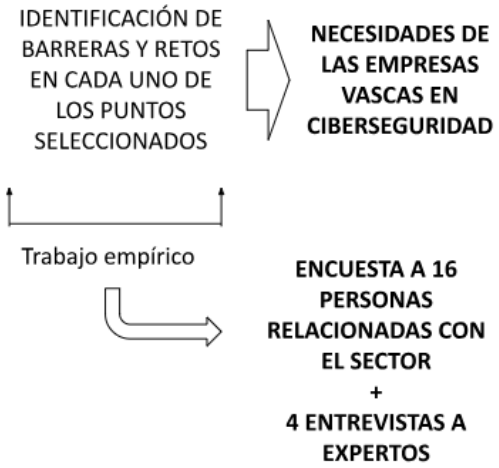


Ilustración 4: Metodología diseño de trabajo de campo

Fuente: Elaboración propia a partir de Ilustración 3

Los expertos seleccionados para las cuatro entrevistas realizadas han sido los siguientes, cada uno de ellos ha sido seleccionado de manera específica por su más estrecha relación con uno de los cuatro bloques ya mencionados. Además, todos han accedido a que sus nombres, experiencia y respuestas puedan ser mencionados en este documento.

Jose Gargallo: Licenciado en Computer Science & Engineer y con amplia experiencia en equipos tecnológicos de diferentes empresas a lo largo de su carrera. Actual CTO de Líbere Hospitality - All Iron Group y recientemente nominado a mejor CTO de España. Se ha tratado de enfocar las preguntas hacia el sector de la empresa y su perspectiva interna. Se adjunta la entrevista en el Anexo.

Lorena Pérez: Su perfil ha sido seleccionado por su carrera profesional en el sector del derecho relacionado con la cibernética y la docencia de asignaturas de regulación cibernética de diferentes universidades como Carlos III de Madrid, CUNEF y otras. Fue Investigadora Académica de la Cátedra Genoma Humano y Derecho en la UPV-EHU y actualmente es la Chief Legal Officer de la empresa Stocken Capital además de profesora de máster y mentora en distintas universidades. Como se puede comprender, su opinión tiene especial valor para el análisis de la situación del ámbito del derecho. Entrevista telefónica no grabada.

Leyre Madariaga: El perfil encaja a la perfección con el objetivo de valorar la situación política en la que se encuentra Euskadi de cara a apoyar a las empresas en la mejora de su ciberseguridad. Leyre lleva más de diez años trabajando para el Gobierno Vasco en continuo contacto con las empresas y tratando en muchas ocasiones con temas relacionados con la innovación y la protección cibernética de estas. Actualmente desarrolla su trabajo de Directora de Transformación Digital y Emprendimiento en Eusko Jaurlaritza - Gobierno Vasco. Se adjunta la entrevista en el Anexo.

Javier Allende: Javier ha desarrollado toda su carrera en importantes puestos siempre relacionados con la seguridad de las empresas, sobre todo la seguridad cibernética. Además, actualmente, además de su puesto en Auditor de Seguridad de Sistemas de Información es docente de máster en ciberseguridad. Esto, además de su experiencia académica en la Universidad de Deusto como estudiante de Ingeniería y Máster en Seguridad de la Información han derivado en que su opinión sea especialmente valorada para el análisis de la influencia del sector académico en la mejora de la ciberseguridad de las empresas vascas. Se adjunta la entrevista en el Anexo.

Estas cuatro entrevistas, junto con la encuesta "general" ya mencionada anteriormente resultan en los próximos cuatro análisis o presentaciones de situación.

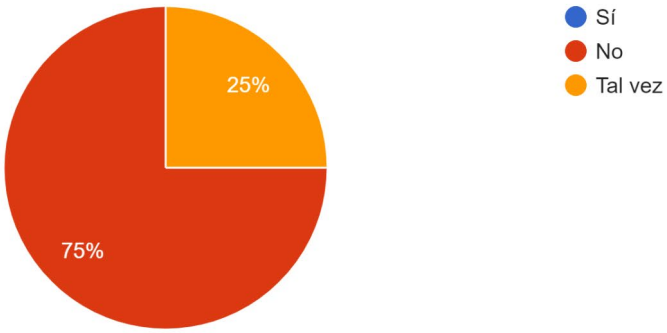
6.2. Resultados

6.2.1. Ámbito político y ciberseguridad en Euskadi

¿Está la política vasca y española haciendo lo posible para la mejora de la ciberseguridad de las empresas?

La política es un sector que el autor ha considerado importante de valorar para el objeto del proyecto por distintos motivos. El buen hacer de las empresas vascas es también motivado por la gestión de los gobiernos a lo largo de los años, pero, en el tema de la ciberseguridad, la importancia que realmente tiene para las empresas hoy en día a veces no se ve reflejada en la actividad diaria.

Si analizamos lo que las personas encuestadas, relacionadas con la empresa, perciben del apoyo de las fuerzas políticas en Euskadi podemos observar varios datos llamativos representados en la Gráfica 7.



Gráfica 7: Respuesta a la pregunta "¿Crees que los organismos y partidos políticos llevan a cabo suficientes iniciativas para proteger a las empresas de potenciales ciberataques?"

Fuente: Elaboración propia, Fuentes de datos: Encuesta de Ciberseguridad en las empresas vascas, elaboración propia. (2023)

En primer lugar, observamos que un 75 % de los encuestados crees que la labor política en busca de la mejora de la ciberseguridad de las empresas vasca no es suficiente y ninguno cree que lo es. En otras palabras, de los dieciséis encuestados relacionados de diferentes formas con alguna empresa de Euskadi, tres cuartas partes la percibe la labor política en este aspecto como nula y el resto la desconoce completamente.

La mitad de los individuos desconocen si las acciones políticas favorecen a la ciberseguridad de las empresas y es precisamente en línea con este resultado lo que proponen como posibles mejoras del sector político en este aspecto: Visualización. Los trabajadores creen que el deber del sector político en busca de la ciberseguridad de las empresas debe ser sobre todo exponer el problema y las herramientas con las que las empresas vascas cuentan para llegar a ser más ciberseguras. Entre las respuestas, es destacable la de la persona que dice que la principal mejora a la que la política debería aspirar es "Circulares y formación gratuita. Dar más conocimiento a través del BCSC. Poca gente lo conoce y pueden hacer mucho.". Esta respuesta, es avalada en gran medida por el Informe Anual de Actividad del BCSC con datos tan llamativos como los siguientes (BCSC, 2023):

- En las 12 jornadas realizadas con empresas las personas alcanzadas han sido 170, menos de 15 por evento.

- En 130 eventos de sensibilización se han alcanzado 2.684 personas, lo que también resulta una cifra sorprendentemente pequeña.

Tanto los expertos entrevistados como los encuestados han coincidido en que la visualización de las herramientas disponibles es una medida necesaria para abordar el problema de la ciberseguridad de las empresas, sin embargo, la mayoría coincide en que uno de los principales objetivos del sector político en este aspecto debería ser la sensibilización de las personas y la red empresarial vasca.

La opinión de Leyre Madariaga al ser preguntada por esto va muy en línea con lo anteriormente mencionado y es que define la transversalidad como uno de los principales retos que las personas dedicadas a la política deberían tener. Este concepto de la transversalidad es algo abstracto, pero se refiere en definitiva a la introducción del concepto y problema de la ciberseguridad en la sociedad, para después poder ser abordado con una sociedad vasca más sensibilizada.

"El mayor reto es entender la transversalidad de la transformación digital. Afecta a todos lo ámbitos de la sociedad y de la empresa. Desde lo público, a veces nos cuesta gestionar esa transversalidad." (Madariaga, 2023)

Leyre además percibe que la ciberseguridad de las empresas vascas es en general, mejor que la del resto de España y le da a la labor política en Euskadi un nueve sobre diez en lo relativo a las acciones de mejora de la ciberseguridad de las empresas. Ella ve este tema como una prioridad directamente relacionada con la competitividad de las empresas y por ende de Euskadi.

6.2.2. Ámbito jurídico y ciberseguridad en Euskadi

A pesar de que también contamos con la opinión de Lorena Pérez para hablar sobre la situación de la Ley en lo referido a ciberseguridad, el autor cree oportuno en el caso de la ley realizar un diagnóstico de situación previo a la puesta en escena de la opinión de la experta y los encuestados.

A lo largo del documento se puede percibir el gran volumen de trabajo que queda por hacer para buscar la ciberseguridad de las empresas desde todos los ámbitos, incluido el derecho. Sin embargo, que quede mucho por hacer, como también se ha mencionado en el proyecto, no significa que sea poco lo que actualmente hay. El sector legislativo europeo y español está haciendo mucho a favor de la ciberseguridad de las personas y empresas.

Ejemplo de este buen hacer que el sector legislativo está llevando a cabo en este tema tenemos el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, aprobado durante esta legislatura y publicado por resolución de 28 de abril de 2022. A continuación, veremos una serie de aspectos destacables de este reciente Real Decreto-ley y por el que ha sido elegido como ejemplo. Además, se relacionarán los distintos artículos de este mismo con las opiniones recogidas.

De las opiniones de los encuestados es destacable la homogeneidad de estas. En la mayoría de los casos, las personas, en este caso relacionadas con empresas, desconocen la existencia de leyes o normativas relacionadas con la ciberseguridad o incluso creen que no existen. El 25 por ciento considera que la ley sí protege a las empresas de potenciales ciberataques. En las respuestas a la pregunta "Menciona a rasgos generales los posibles cambios que las leyes o normativas pudieran percibir para favorecer la ciberseguridad de las empresas." se leen varias que proponen el diseño de leyes que controlen la ciberseguridad y sancionen al ciberdelincuente, otros afirman no tener ideas al respecto.

"La creación de leyes específicas de ciberseguridad es una medida necesaria para la mejora de la ciberseguridad de las empresas" (Encuesta Ciberseguridad en las empresas vascas, 2023).

Tras este inciso, es muy interesante ver cómo efectivamente en el propio decreto recientemente mencionado se cumplen con las solicitudes o ideas de mejora de los encuestados. El decreto ley establece requisitos de seguridad específicos para la quinta generación de la tecnología, pero sucede y completa los anteriores ya existentes.

La mayoría de la sociedad considera libre su uso y tratamiento de los dispositivos pero como el propio Artículo 11 de este Decreto dice: "Los sujetos previstos en el artículo 4 deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G, con base en lo establecido en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones." (Real Decreto-ley 7-2022, 2022). Como usuario de un dispositivo, cualquier individuo tiene deberes que cumplir por ley. Además, se especifican artículos relativos al uso corporativo de los dispositivos y redes, así como el uso por parte de la administración pública en el Artículo 15 y 17.

Como demostración de que la labor en ciberseguridad del sector legislativo no es algo del último año podemos encontrar numerosos Decretos-Ley y Órdenes que avalan esta afirmación. Por ejemplo, podemos analizar la orden PRA/33/2018 publicada en el BOE y en vigor desde el 24 de enero de 2018 para regular el Consejo Nacional de Ciberseguridad y que afirma en su primer acuerdo que se modifica el marco regulador del Consejo Nacional de Ciberseguridad aprobado por Acuerdo del Consejo de Seguridad Nacional en su reunión del día 5 de diciembre de 2013.

En resumen, las leyes y normativas existen y a pesar de que esto no signifique que todas las necesidades que la ley puede ofrecer estén cubiertas, como dice Lorena Pérez, no se puede decir que el sector jurídico no respalde la ciberseguridad de las empresas españolas o vascas.

Contrastando las opiniones de los expertos encontramos también ideas como la posible obligación de auditoría de ciberseguridad a las empresas, sin embargo, Jose Gargallo, CTO y experto en tecnología de empresas, considera que no sería una medida demasiado eficiente por el posible "trampeo" o negocio subyacente que esto podría generar.

Tras este análisis podemos concluir con este apartado afirmando que leyes y avances en estas existen pero que incluso a las personas participantes de empresas les resultan desconocidas. Además, el carácter persuasivo de estas normativas es inexistente y apenas se emplean recursos en asegurar el cumplimiento de ellas.

6.2.3. Empresas y ciberseguridad en Euskadi

Las empresas necesitan apoyo para mejorar su ciberseguridad, pero ¿están haciendo lo correcto para ello?

Es fácil externalizar el problema, pensar que todas las barreras se encuentran en el exterior y que las empresas de manera interna están haciendo lo correcto para llegar a ser más ciberseguras. Ninguna de las personas encuestadas cree que lo más importante para la búsqueda de la ciberseguridad de las empresas sean las labores internas de las compañías, sin embargo, solo tres de ellas creen que las labores realizadas por las empresas sean buenas o muy buenas.

Muchas de las opiniones tanto de los expertos como de los encuestados son relacionadas con la concienciación interna de los empleados. Las personas dentro de la empresa todavía perciben el

problema de la ciberseguridad como algo “lejano”. El impacto de los ciberataques generalmente no es fácil de visualizar por los trabajadores.

“El objetivo de las empresas para mejorar su panorama interno de ciberseguridad debe ser concienciar de que realmente existe y de que son vulnerables en cualquier momento.” (Encuesta Ciberseguridad en las empresas vascas, 2023).

Jose Gargallo, CTO de Líbere Hospitality - All Iron Group y recientemente nominado a mejor CTO de España es crítico con la labor de las empresas. En primer lugar, Jose cree que la ciberseguridad en las empresas vascas es peor en general que en el entorno nacional e internacional pero además es importante destacar que formando parte del departamento de IT de una start-up tecnológica vasca valora con un tres sobre diez la labor interna de las empresas en materia de ciberseguridad.

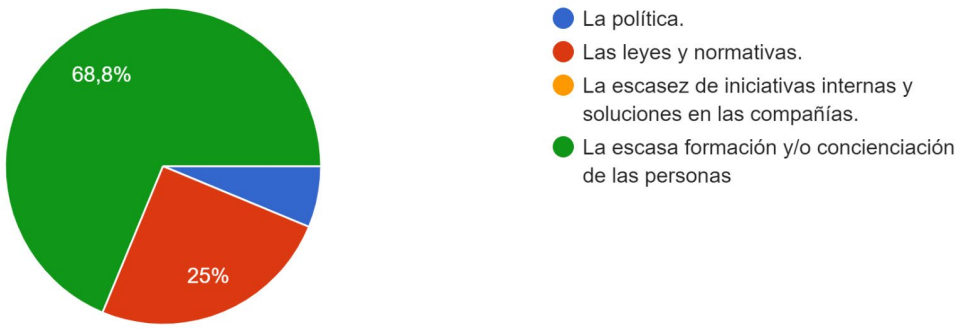
Jose coincide con la opinión anteriormente mencionada de que la prioridad de las empresas debe ser la concienciación interna de los empleados acerca del riesgo que supone no estar preparados para potenciales ciberataques. Cree que tras este primer paso se podrían llevar a cabo otras medidas como incorporación de servicios para la búsqueda de la ciberseguridad.

“...de ahí que: primero concienciación, luego acciones por voluntad propia cuando la empresa le vea el valor.” (Gargallo, 2023).

6.2.4. Formación en ciberseguridad en Euskadi.

¿Cómo afecta la formación previa al trabajo de las personas en la ciberseguridad de sus empresas?

Sabemos, a grandes rasgos, lo que significa el concepto de la ciberseguridad y posiblemente alguna vez hayamos percibido algún peligro digital gracias a mensajes que hemos escuchado durante nuestra educación y/o formación, sin embargo, a la hora de la verdad es una realidad que la preparación que actualmente los trabajadores tienen para ser eficientes y seguros durante el uso de sus herramientas digitales es mínima. La encuesta realizada lo demuestra, y es que el 68,8 % de los encuestados cree que la mayor barrera que las empresas encuentran para la mejora de su ciberseguridad es precisamente la escasa formación de las personas.



Gráfica 8: Respuesta a la pregunta "¿Cuál elegirías como la MAYOR barrera que encuentran las empresas vascas para mejorar su ciberseguridad?"

Fuente: Elaboración propia, Fuentes de datos: Encuesta de Ciberseguridad en las empresas vascas, elaboración propia. (2023)

Ninguno de los encuestados ha valorado la labor de la formación en la búsqueda de la mejora de la ciberseguridad de las empresas vascas como positiva, como vemos reflejado en la Gráfica 8. Por el contrario, Javier Allende, auditor de sistemas de ciberseguridad y profesor de máster en ciberseguridad valora la formación actual como positiva y considera que esta mejora debe consistir principalmente en la mejora de los procesos internos de las empresas.

"Ya que existe la asignatura Informática en muchos centros en vez de enseñar programas que no siempre necesarios para la vida laboral, podría destinarse cierto horario lectivo para el aprendizaje de ciberseguridad tanto de empresas y como de particulares" (Encuesta Ciberseguridad en las empresas vascas, 2023).

Contrastando esta opinión con la del resto de expertos y la encuesta general, vemos que, por el contrario, la mayoría, incluyendo a los expertos de Gobierno Vasco y departamentos tecnológicos ven necesidades primordiales de las empresas vascas en la formación de las personas. Reuniendo todas estas opiniones y analizándolas se pueden identificar percepciones relacionadas la falta de formación en el ámbito necesaria para cualquier perfil profesional, así como la falta de educación digital relacionada con ciberseguridad. Muchos destacan la importancia de, además, formación previa al trabajo, pero ofrecida por la propia empresa empleadora, esto último quizás relacionado con las posibles mejoras internas de las empresas.

"Formación temprana en colegios, continuación de la formación en universidades, muestra de las consecuencias reales… Hay mucha gente que dice "a mí me da igual, yo no tengo nada que esconder". Pero como dijo Edward Snowden en una entrevista: "No consiste en tener algo que esconder, sino en tener algo que proteger"(Encuesta Ciberseguridad en las empresas vascas, 2023).

7. CONCLUSIONES

7.1. CONCLUSIONES

Llegado este punto del documento resulta interesante volver a los objetivos planteados inicialmente.

En primer lugar, a través de la recogida de referencias bibliográficas fiables y completas del sector se ha conseguido plasmar de la manera más sintetizada posible la situación actual del sector de la ciberseguridad en forma de megatendencias, referida tanto a las amenazas más comunes como a las herramientas disponibles para hacerles frente. En el tercer apartado del tercer capítulo del documento, La Ciberseguridad, se puede encontrar el listado de lo anteriormente mencionado, complementado además con información relativa al pasado y futuro del sector, así como la valoración de este en el territorio internacional y nacional. Las megatendencias en el sector a modo de resumen son el reciente y explosivo nacimiento de soluciones empresariales en ciberseguridad, la insistencia de los ciberdelincuentes en confiar en los métodos más arcaicos de engaño para conseguir sus objetivos y el exponencial crecimiento de puntos de "peligro" por la rutinaria presencia del teletrabajo y nuevas herramientas digitales como la IA.

Una conclusión de esta revisión de datos para la presentación de las megatendencias y como ya se menciona en el apartado 3.4.1 del proyecto de investigación es que las recogidas de datos para la realización de los estudios estadísticos en el uso de ciberseguridad son a veces muy pobres. En este apartado vimos como Eurostat hacía uso de la variable "utilización de contraseñas seguras" para medir la medida en la que una empresa hace uso de medidas de ciberseguridad. Esto no es la realidad, ya que el cumplimiento de esta medida no implica en absoluto ser una empresa cibersegura.

Este informe de situación internacional y nacional mencionado en el anterior párrafo es idóneo para, junto con el capítulo cuarto, que introduce a las empresas en la ecuación de manera directa, situar al lector antes de analizar los siguientes objetivos, acotados ya al territorio vasco. Para precisamente responder o llegar a las metas o subobjetivos II, III y IV se forma el capítulo quinto. Euskadi está muy bien posicionada frente a su entorno como así avalan los resultados y datos estadísticos explicados en el primer apartado del capítulo El Caso Euskadi, situando al territorio junto a los países europeos punteros en la utilización de medidas de ciberseguridad. Resulta curioso percibir

cómo a pesar de esto, las personas encuestadas y/o entrevistadas no tienen la percepción de estar más protegidas o preparadas que las del entorno, sin embargo, como es comentado en el capítulo, esta conclusión casa a la perfección con un resultado primordial del proyecto, que nos indica que la ciberseguridad y herramientas son por lo menos suficientes, pero inútiles sin cultura y visibilidad del problema.

Esto último va muy en relación con la siguiente cuestión planteada en los objetivos del trabajo. Con el previo análisis bibliográfico y ya situando a Euskadi en el mapa de la ciberseguridad nos ha costado mucho encontrar vulnerabilidades en la falta de herramientas, innovación o calidad del entorno técnico. Todos estos factores son buenos y es esta, finalmente, la conclusión más importante de este Trabajo de Fin de Grado y la que precede a la respuesta del subobjetivo (IV) y al objetivo general del trabajo; las vulnerabilidades en ciberseguridad de las empresas vascas se encuentran en resumen en los factores más humanos de las empresas.

Con lo mencionado anteriormente y en respuesta al subobjetivo IV, identificamos, partiendo de los puntos de partida o bloques seleccionados, los siguientes retos que deben afrontar las empresas vascas para mejorar su ciberseguridad.

7.2. DECÁLOGO DE LOS RETOS DE LAS EMPRESAS VASCAS EN CIBERSEGURIDAD

El siguiente decálogo se puede considerar como resultado sintetizado del proyecto, y se presenta dividido en los cuatro bloques de actuación elegidos:

<u>Político</u>

1. Prioridad de la ciberseguridad de las empresas en los programas e iniciativas, al menos proporcional a su potencial impacto económico.
2. Inversión en campañas de sensibilización del problema tanto para empresas como para personas.
3. Visibilización de las herramientas disponibles para la mejora de la ciberseguridad en la gestión empresarial.

Jurídico

4. Difusión sobre legislación y asistencia acerca de las leyes vigentes relativas a ciberseguridad y su cumplimiento.
5. Un mayor estudio y seguimiento de incidencias concretas.

Empresa

6. Protocolos de concienciación interna del impacto del buen-hacer y de las posibles consecuencias negativas de no llevarlo a cabo.
7. Una mayor inversión tanto de tiempo como de presupuesto en la incorporación de medidas de ciberseguridad, como política de personas en las organizaciones.
8. Implementación de periodos de formación de ciberseguridad específica del sector en el que opera la empresa, ya que, aunque los métodos son comunes, existen especificaciones en cada uno de ellos.

Educativo

9. Enseñanza de nociones básicas de ciberseguridad independientemente del perfil académico.
10. Contacto con la ciberseguridad en la educación tan temprano como la persona se introduzca en el uso de redes y dispositivos digitales.

7.3. LÍNEAS DE INVESTIGACIÓN FUTURA

Finalmente, el resultado ha sido sorprendente para el autor, que en un principio pensaba que las necesidades estarían más relacionadas con la falta de inversión, recursos o innovación y no tan en línea a cuestiones humanas o de decisión de las personas. Aun así, el resultado final es atractivo y muy útil de cara a visualizar el objeto del trabajo. El resultado además abre puertas e invita a ser continuado, quizás en una línea más técnica inalcanzable para este proyecto por su alcance y rama de conocimiento. Es deseo del autor que esta invitación sea aceptada por juristas, docentes, políticas y políticos o expertos y expertas en ciberseguridad capaces de identificar las soluciones posibles y concretas a estas necesidades de las empresas vascas en ciberseguridad.

Como broche final y para finalizar el cuerpo del documento se adjunta una cita de una conversación mantenida en tono amistoso durante la realización del trabajo, para tomarla como idea de valoración de medidas en ciberseguridad en las empresas:

"...Pues yo trabajaba en XXX y de manera esporádica recibía correos del tipo de: "Te escribo desde el departamento financiero por un problema con tu nómina, por favor, rellena los datos bancarios que adjunto en el siguiente enlace para poder gestionar y tramitar el pago lo antes posible", pinchabas en ese enlace y te llevaba a un sermón del encargado de ciberseguridad diciéndote: Has caído en esta tonta trampa de ciberdelincuencia, ahora pulsa este enlace y apúntate al curso de formación interna sobre métodos de ciberseguridad!"..."

8. BIBLIOGRAFÍA

Basque CyberSecurity Center (BCSC). (2023). Informe anual de actividad 2022. https://www.ciberseguridad.eus/sites/default/files/2023-05/BCSC_Memoria_2022_es%20%281%29.pdf

Basque CyberSecurity Center (BCSC). Situación de la ciberseguridad en Euskadi - 4 o trimestre de 2022. (2023). Recuperado de https://www.ciberseguridad.eus/empresa-segura/utilidades-empresa/guias-estudios-informes/situacion-de-la-ciberseguridad-en-euskadi-4-trimestre-2022

CCN. (2023). Integrantes del Centro Nacional de Inteligencia. Centro Nacional de Inteligencia, Ministerio de Defensa, Gobierno de España. Recuperado de: https://rns.ccn-cert.cni.es/es/integrantes-rns/listado-completo-de-integrantes

Consejo de la Unión Europea. (2023). Ciberseguridad: cómo combate la UE las amenazas cibernéticas. Recuperado de: https://www.consilium.europa.eu/es/policies/cybersecurity/

Eurostat, Statistics Explained. (2022). ICT security in enterprises. Recuperado de: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises

Eustat. (2022). El número de empresas en la C.A. de Euskadi disminuyó un 0,9% y el empleo aumentó un 0,2% en 2022 [Nota de prensa]. Recuperado de: https://www.eustat.eus/elementos/El-numero-de-empresas-en-la-CA-de-Euskadi-disminuyo-un-0,9-y-el-empleo-aumento-un-0,2-en-2022/not0020453_c.html#:~:text=En%20la%20C.A.%20de%20Euskadi%20operaban%20151.088%20empresas%20de%20los,seg%C3%BAn%20datos%20elaborados%20por%20Eustat.

Eustat. (2022). El gasto de las empresas en innovación aumenta un 8,7% en 2021 y supera por primera vez los 3.000 millones de euros en la C.A. de Euskadi [Comunicado de prensa]. https://www.eustat.eus/elementos/el-gasto-de-las-empresas-en-innovacion-aumenta-un-87-en-2021-y-supera-por-primera-vez-los-3000-millones-de-euros-en-la-ca-de-euskadi-/not0020530_c.html

Fortune Business Insights. (2023). Cybersecurity market, key market insights. Recuperado de: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

Guadilla, D. (2023). El Gobierno vasco crea la Cyberzaintza para combatir las amenazas digitales. El Correo. https://www.elcorreo.com/politica/gobierno-vasco-crea-cyberzaintza-combatir-amenazas-digitales-20230606172523-nt.html

Hidalgo, M. (2021). "Atrápame si puedes": el inocente primer virus informático de la historia cumple 50 años. *El País*. https://elpais.com/tecnologia/2021-05-20/atrapame-si-puedes-el-inocente-primer-virus-informatico-de-la-historia-cumple-50-anos.html

IBM. (2023). IBM Security X-Force Threat Intelligence Index 2023. IBM Reports Recuperado de: https://www.ibm.com/reports/threat-intelligence

Instituto Nacional de Ciberseguridad. (2022). Encuesta sobre el uso de TIC y del comercio electrónico en las empresas Año 2021 – Primer trimestre de 2022 [Nota de prensa]. Recuperado de: https://www.ine.es/prensa/tic_e_2021_2022.pdf

Instituto Nacional de Ciberseguridad. (2022). Especialistas y perfiles tic, INE. Recuperado de: https://www.ine.es/jaxiT3/Datos.htm?tpx=53964#!tabs-tabla

Instituto Nacional de Ciberseguridad. (2023). Balance de Ciberseguridad 2022. Recuperado de: https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf

La Moncloa. (2022). El Congreso convalida por amplia mayoría la Ley de Ciberseguridad 5G [Prensa/Actualidad/Asuntos Económicos y Transformación Digital]. Recuperado de: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2022/280422-ley_seguridad.aspx

Moore, S. (2019). Las 7 principales tendencias en ciberseguridad para 2022. Gartner, Insights, Tecnología de la Información. Recuperado de: https://www.gartner.es/es/articulos/las-7-principales-tendencias-en-ciberseguridad-para-2022

Oliveira, L. (2022). La historia de la ciberseguridad. Blog Experiencia de NordVPN. Recuperado de: https://nordvpn.com/es/blog/historia-ciberseguridad/

Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad. Boletín Oficial del Estado, 20, de 23 de enero de 2018. https://www.boe.es/buscar/act.php?id=BOE-A-2018-799&p=20180123&tn=2

Parlamento Europeo. (26 de marzo de 2021). ¿Qué es la inteligencia artificial y cómo se usa? Noticias Parlamento Europeo. Recuperado de https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa?at_campaign=20234-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=DSA&at_goal=TR_G&at_audience=&at_topic=Artificial_Intelligence&gclid=Cj0KCQjwi46iBhDyARIsAE3nVraq2_3k3_mfN60phbsWWljWp8PobH6ZsKfcduezH3Pnde49yzAZD3caAq5_EALw_wcB

Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación. Boletín Oficial del Estado, 76, de 30 de marzo de 2022.

Reglamento general de protección de datos [RGPD]. Reglamento (UE) 2016/679. 25 de mayo de 2018 (Unión Europea).

Solano, M. (2021). Ciberseguridad internacional: ¿de qué se trata?. EAE Programas - Blog Internacinalización. https://www.eaeprogramas.es/blog/internacionalizacion/ciberseguridad-internacional-de-que-se-trata

The Cocktail Analysis. (2022). Panorama actual de la Ciberseguridad en España. La ciberseguridad en España. Una perspectiva desde las Pymes, sociedad civil y administración pública. Google Reports. Recuperado de: https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

9. ANEXOS

ANEXO 1 - Artículos 15 y 17 del Real Decreto-ley 7/2022

Artículo 15. Gestión de seguridad por los usuarios corporativos 5G.

1. Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación deberán garantizar la instalación, despliegue y explotación seguros de redes privadas 5G y prestación segura de servicios 5G en autoprestación mediante la aplicación de técnicas y procedimientos de operación y supervisión que garanticen la seguridad de las redes y servicios 5G.

2. Los usuarios corporativos 5G mencionados deberán aportar al Ministerio de Asuntos Económicos y Transformación Digital una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos, cuando sean requeridos para ello.

Artículo 17. Gestión de seguridad por las Administraciones públicas.

1. Las administraciones públicas deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G.

2. En particular, las administraciones públicas que quieran llevar a cabo la instalación, despliegue y explotación de redes 5G, ya sean públicas o privadas, o la prestación de servicios 5G, disponibles al público o en autoprestación, no podrán, por razones de seguridad nacional, utilizar equipos, productos y servicios proporcionados por suministradores de alto riesgo o riesgo medio.

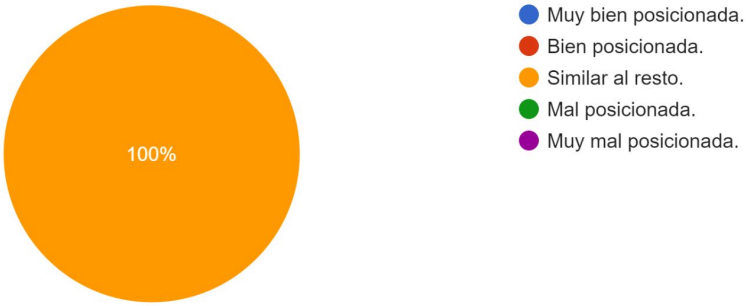
ANEXO 2 - Entrevistas a expertos

Entrevista Jose Gargallo - CTO Líbere Hospitality

1- ¿Crees que la Ciberseguridad debería ser una de las prioridades de las empresas hoy en día? ¿Por qué?

Totalmente, es una realidad que la mayoría de crímenes son ya digitales, mirar hacia otro lado es no querer o no entender el riesgo

2- ¿Cómo dirías que se encuentra Euskadi en comparación con el resto del Estado en lo que respecta a la ciberseguridad de las empresas?



3- ¿Crees que se podrían realizar acciones políticas que favorezcan la mejora de la ciberseguridad de las empresas vascas? ¿Qué reto debería proponerse el sector político para ello?

No me hagas hablar de política, jaja. Siempre se orienta todo a ayudas y demás, y no creo que sea la forma de dar un salto de calidad real.

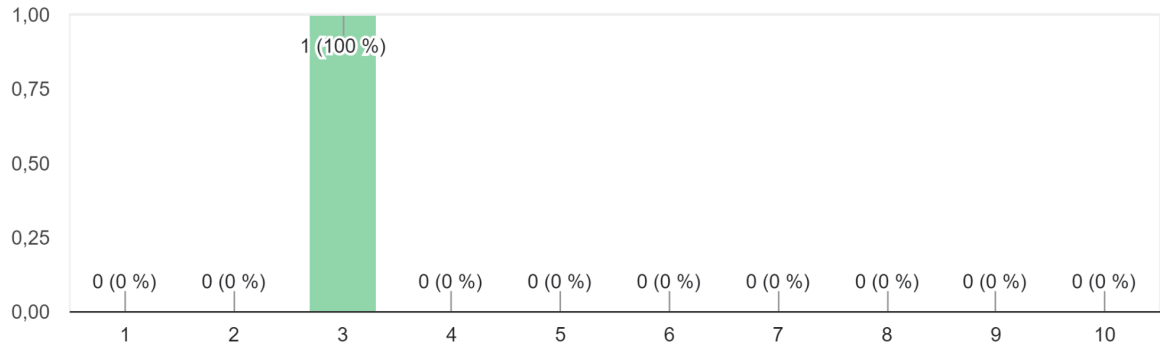
4- ¿Crees que se podrían realizar acciones políticas que favorezcan la mejora de la ciberseguridad de las empresas vascas? ¿Qué reto debería proponerse el sector político para ello?

Uf, no sé, honestamente no conozco la ley lo suficiente como para valorarla.

5- ¿Crees que se podrían realizar acciones durante la educación y formación de las personas que favorezcan la mejora de la ciberseguridad de las empresas vascas? ¿Qué reto debería proponerse el sector académico para ello?

Totalmente, el desconocimiento sobre lo expuestos que estamos a estos ataques y la ligereza con la que tendemos a compartir datos al exterior son preocupantes. El principal problema es que a nivel educativo estamos muy lejos en lo digital, que se confunde con poner unas tablets en las aulas. Dentro de esto, obviamente, la ciberseguridad tendría que estar presente.

6- ¿Qué nota le darías a la labor interna de las empresas vascas para mejorar la ciberseguridad de las empresas?



7- En relación con la pregunta anterior y teniendo en cuenta tu experiencia en departamentos tecnológicos, ¿Qué barreras crees que se encuentran las empresas para mejorar su ciberseguridad? ¿Qué retos crees que ellas mismas deberían proponerse en este aspecto y de manera interna?

Como decía antes, es un tema de concienciación, de darle el valor que realmente tienen los datos que almacenan, y que está a la orden del día que te hackeen en cualquier momento. Y luego, no todas las empresas se pueden permitir tener un departamento de IT y tiran con lo que pueden.

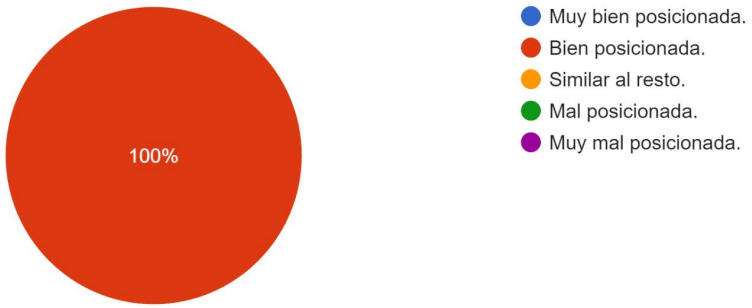
Una buena auditoría es necesaria, no he contestado esto en el apartado de acciones políticas porque en el momento que se convierte en obligación aparecen los chiringuitos de las consultoras a vender sin aportar valor, de ahí que: primero concienciación, luego acciones por voluntad propia cuando la empresa le vea el valor.

Entrevista Leyre Madariaga - Directora de Transformación Digital y Emprendimiento en Eusko Jaurlaritza - Gobierno Vasco

1- ¿Crees que la Ciberseguridad debería ser una de las prioridades de las empresas hoy en día?¿Por qué?

Sin lugar a dudas. Es un elemento fundamental de competitividad.

2- ¿Cómo dirías que se encuentra Euskadi en comparación con el resto del Estado en lo que respecta a la ciberseguridad de las empresas?



3- ¿Crees que se podrían realizar más acciones internas en las empresas que favorezcan la mejora de su ciberseguridad? ¿Qué reto o retos deberían proponerse para ello?

Siempre se puede hacer más. Interiorizar la necesidad de invertir en ella permanentemente.

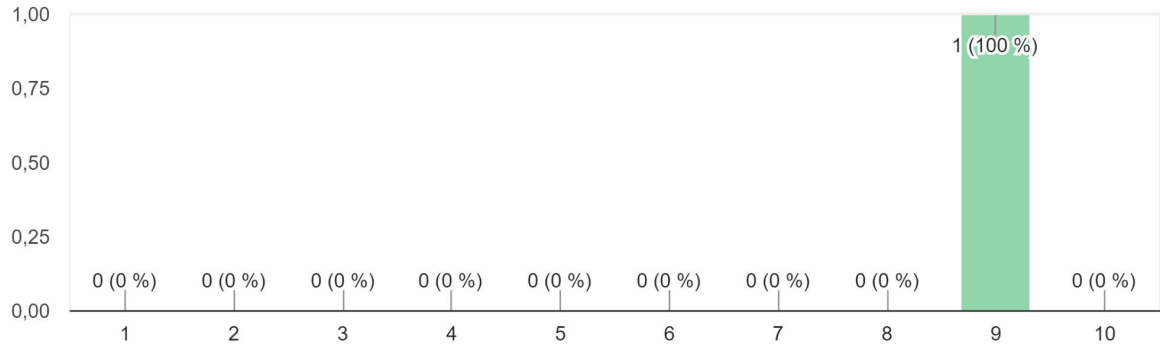
4- ¿Crees que se podrían realizar acciones jurídicas o legislativas que favorezcan la mejora de la ciberseguridad de las empresas vascas? ¿Qué reto debería proponerse el sector jurídico para ello?

No creo tanto en la "obligación" sino en la sensibilización y formación.

5- ¿Crees que se podrían realizar acciones durante la educación y formación de las personas que favorezcan la mejora de la ciberseguridad de las empresas vascas? ¿Qué reto debería proponerse el sector académico para ello?

Sí, es un elemento fundamental. Adquirir, desde jóvenes, competencias digitales, es uno de los retos de nuestra sociedad.

6- ¿Qué nota le darías a la labor política vasca para mejorar la ciberseguridad de las empresas?



7- En relación con la pregunta anterior y teniendo en cuenta tu experiencia en el sector digital y de la ciberseguridad, ¿Qué barreras crees que se encuentra la política vasca para mejorar la ciberseguridad de las empresas? ¿Qué retos crees que el Gobierno Vasco u otros organismos políticos deben proponerse para favorecer la mejora de la ciberseguridad de las empresas vascas?

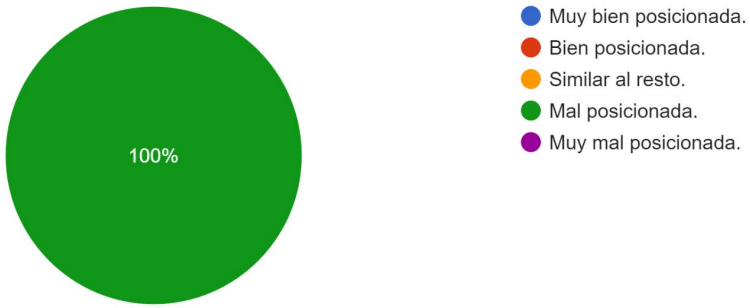
El mayor reto es entender la transversalidad de la transformación digital. Afecta a todos los ámbitos de la sociedad y de la empresa. Desde lo público, a veces nos cuesta gestionar esa transversalidad.

Entrevista Javier Allende Astigarraga - Auditor de Seguridad de Sistemas de Información

1- ¿Crees que la Ciberseguridad debería ser una de las prioridades de las empresas hoy en día?¿Por qué?

Si. Las empresas son tecnología y por ende se debe invertir y cuidar la tecnología.

2- ¿Cómo dirías que se encuentra Euskadi en comparación con el resto del Estado en lo que respecta a la ciberseguridad de las empresas?



3- ¿Crees que se podrían realizar acciones políticas que favorezcan la mejora de la ciberseguridad de las empresas vascas? ¿Qué reto debería proponerse el sector político para ello?

Cualquier iniciativa política es bienvenida si se aterriza no si es un canto al aire

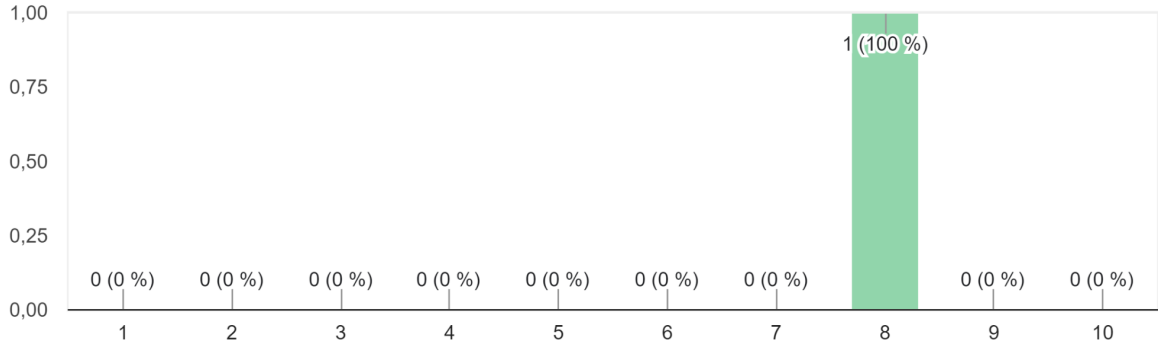
4- ¿Crees que se podrían realizar acciones jurídicas o legislativas que favorezcan la mejora de la ciberseguridad de las empresas vascas? ¿Qué reto debería proponerse el sector jurídico para ello?

Ya existe normativa para ello.

5- Por lo general, ¿Crees que se podrían realizar acciones internas en las empresas que favorezcan notablemente la mejora de la ciberseguridad? ¿Qué reto deberían proponerse los departamentos tecnológicos de las compañías para ello?

Creer que van a ser atacados y que cualquier empresa debe cambiar su manera de trabajar.

6- Habiendo sido docente del ámbito de la ciberseguridad, ¿Qué nota le darías a la labor del sector académico-educativo para mejorar la ciberseguridad de las empresas?



7- En relación con la pregunta anterior y teniendo en cuenta tu experiencia en departamentos tecnológicos así como en otros organismos directamente relacionados con la ciberseguridad de las empresas y la enseñanza sobre ella, ¿Crees que la formación previa y simultánea al trabajo de las personas es una barrera para la mejora de la ciberseguridad en las compañías vascas? ¿Qué retos crees que el sector académico debería proponerse en este aspecto?

No, recalcar la prioridad de la seguridad dentro del negocio.