FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

Ciber riesgos, una nueva era de riesgos para las empresas

Análisis del impacto en los resultados, la marca y la reputación. Modelos de prevención y de gestión

Autor: Carlota Campos Irisarri

Director: Raúl González Fabre

MADRID | Marzo 2023

I. Resumen

Este trabajo de fin de grado expone los riesgos que corren las empresas ante la ciberdelincuencia, las posibles implicaciones que entraña en la continuidad del negocio y su reputación; y el papel de la ciberseguridad como agente protector. Para ello se analiza el entorno cibernético actual explicando los principales tipos de ciberataques existentes, las tendencias de los últimos años y su principal impacto en la actividad operativa de una empresa.

De esta manera, se comprende la importancia de la ciberseguridad y se establecen los retos y desafíos para su evolución de cara al futuro. Asimismo, se realiza una entrevista con Guillermo Llorente Ballesteros, director de seguridad de MAPFRE para exponer los mecanismos de ciberseguridad que llevó a cabo la empresa para contrarrestar el ataque de 2020.

Por último y respondiendo al verdadero objetivo del trabajo, se desarrolla un protocolo de actuación para llevar a cabo una gestión reputacional exitosa en caso de amenaza. Por esta razón, el trabajo busca contribuir al fomento de una cultura empresarial de "*prevención y defensa*" ante los Ciberataques.

Palabras Clave: Ciberseguridad, Ciberataques, Riesgo Reputacional, Impacto Corporativo

II. Abstract

This essay exposes the risks that companies face from cybercrime, the possible implications for the business continuity and its reputation, as well as the role of cybersecurity as a shield. To do this, the current cyber environment is analyzed by explaining the main types of existing cyber-attacks, the trends of recent years and their main impact on an enterprise's operational activity.

Furthermore, it allows a better comprehension of the importance of cybersecurity and the challenges for its future evolution. Likewise, an interview is conducted with Guillermo Llorente Ballesteros, MAPFRE security director, to expose the mechanisms of cybersecurity that were carried out by the company to counteract the 2020 attack.

Finally, and attending the real objective of the work, an action protocol is developed to guarantee a successful management of the business reputation, in case of an attack. Therefore, the essay seeks to contribute to the promotion of a corporate culture of "prevention and defense" against cyber-attacks.

Key Words: Cybersecurity, Cyberattacks, Reputational Risk, Corporate Impact

III. Índice

IV. Índice de Figuras

It takes 20 years to build a reputation
and five minutes to ruin it' (Warren Buffett)

1. Introducción

1.1 Exposición de los objetivos

Hoy en día, la ciberdelincuencia no excluye a ninguna empresa del mundo, independientemente de su sector, tamaño, ubicación, tipología o resultados. Desde que a finales de junio en 2017 un virus como el "*Wanna Cry*" se convirtiera en el protagonista del primer gran ciberataque global de la historia al afectar a más de 200.000 equipos informáticos en más de 150 países (Fernández, 2014) y , a la vista de las evolución de las cifras mundiales de los ataques cibernéticos que sufren a diario las empresas de todo el mundo, la pregunta que se tienen que hacer hoy las empresas no es si *"recibiremos nosotros un Ciberataque",* sino "*cuándo recibiremos nosotros un Ciberataque y si estaremos preparados cuando nos llegue para que el golpe nos impacte lo menos posible y podamos recuperarnos pronto"*.

Así, el Ciberataque en general a las empresas en el mundo está evolucionando y cambiando tan rápido -nuevos métodos, nuevos tipos de *ransomware*, nuevos perfiles de ciberdelincuentes, nuevos tipos de rescates, de daños, etc.- que está resultando muy complicado para los gobiernos y legisladores atacar esta pandemia desde la elaboración y desarrollo de leyes y desde la creación de sistemas de defensa tecnológicos. De esta manera, el trabajo busca contribuir al fomento de una cultura empresarial de "prevención y defensa" ante los ciberataques. (Cisco, 2019)

1.1.1 ¿Por qué es la pandemia tecnológica para las pymes en el siglo XXI?

El Informe de Ciber Preparación de Hiscox del pasado 2022 identifica la amenaza cyber como el principal riesgo para las empresas de las grandes potencias del mundo empresarial actual, por encima de la pandemia, las consecuencias de la recesión económica y la falta de personal cualificado, entre otros. Gareth Wharton afirma que "si tenemos en cuenta que la concienciación del peligro es el primer paso para afrontarlo, seguramente esta es una señal alentadora. Sin embargo, la parte negativa es que han aumentado tanto el número de empresas que notifican ataques como la gravedad de estos, por lo que no cabe duda de la magnitud del desafío". Es decir, si bien históricamente los ciberdelincuentes han dirigido sus ataques a empresas de alto valor e influencia, está demostrado que ahora están apostando por un descenso en *"la cadena alimentaria"*. Como resultado, las pequeñas y medianas empresas con ingresos entre €90.000 y €450.000 son en blanco óptimo de un mayor número de ataques cibernéticos; recibiendo la misma cantidad que aquellas que facturan de €900.000 a €8,1 millones anuales. (Hiscox, 2022)

Sin embargo, la diferencia es que mientras las grandes empresas invierten diariamente en la creación de estrategias de ciberdefensa, el gasto de las pequeñas y medianas empresas ha disminuido considerablemente este año, debido a una reducción en el gasto total en TI en el extremo inferior del espectro empresarial. Pero la pandemia convierte a esta medida en algo problemático; ya que la digitalización parcial de las empresas como método de adaptación a la crisis sanitaria, ha obligado a las empresas a adoptar soluciones en la nube en vez de optar por implementar sus propios servicios remotos. Como resultado, ha aumentado su exposición a posibles ataques cibernéticos y ha alentado a los

ciberdelincuentes a aprovechar la vulnerabilidad de dichas empresas en la nube a causa de grandes brechas de seguridad. (Posada, 2019)

No obstante, las pequeñas y medianas empresas están reforzando sus sistemas de respuesta ante estos ataques mediante el desarrollo de planes de ciber resistencia; así como aumentando la concienciación en las altas esferas del tejido empresarial o formando a los empleados en materia de ciberseguridad con el fin de que la capacidad para detectar las amenazas y desempeñar los procesos de ciber preparación acordes se manifieste desde todos los ámbitos de la organización. La formación del personal, tanto de pequeñas y medianas, como de grandes empresas es esencial para evitar diversas vulneraciones cotidianas de seguridad como por ejemplo las técnicas de phishing por medio de correos electrónicos. Esta simple pero elemental medida contribuye a mejorar la calidad de respuesta y actuación de las empresas frente al desafío que supone el ciber riesgo.

De este modo, el análisis desarrollado a lo largo del trabajo busca establecer un modelo teórico-práctico que ayude a las empresas a identificar las fortalezas y debilidades en su sistema de ciber preparación, elaborar un plan de gestión del riesgo que aumente la resiliencia para afrontar los ciberataques, y conseguir mitigar la magnitud del impacto que estos podrían tener en la reputación y la cuenta de resultados.

Como se ha indicado anteriormente, los hackers han cambiado su foco de ataque. El nivel medio de ciber amenazas por empresa ha incrementado de forma muy moderada (de 179 a 190 ataques). Si bien en las grandes empresas este número ha experimentado un descenso leve (aunque la cifra promedio supere los 1.100 ataques en empresas con ingresos mayores a los €4.5 millones), en el colectivo de pequeñas y medianas empresas,

en cambio, ha aumentado, dado que los hackers están redirigiendo su foco de atención de objetivos “de primer nivel” a este conjunto más reducido. En proporción, aquellas empresas con una cantidad de empleados que varía entre los 250 y 999 sufrieron un aumento del 53% en el número de ataques; las que tienen de 10 a 49 empleados un 80%, y en las más pequeñas, aquellas con menos de 10 empleados, esta cifra se vio ascendió un 264% (de 11 ataques promedio a 40). (Hiscox, 2022)

1.1.2 La importancia de la Ciberseguridad

La ciberseguridad se entiende como la práctica de proteger ordenadores, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos; conformando así la seguridad de la información electrónica o seguridad de la tecnología de la información. A su vez, se aplica en situaciones de protección o seguridad en diversos contextos relacionados con aplicaciones, información, seguridad operativa, recuperación post-ataques, continuidad de negocio y capacitación de los usuarios. (Cisco, 2023)

De este modo, en la última década se ha experimentado un aumento vertiginoso de las ciber amenazas, destacando la preocupación por la continua filtración de datos en las empresas. Incluso previo a la pandemia, Risk Based reveló un informe en el que exponía la alarmante cifra de 7.900 millones de registros expuestos durante los primeros nueve meses del año 2019 como resultado de dichas filtraciones de datos; superando en más del doble la cifra de 2018 (112%). Por esta razón, es imprescindible invertir en formación para aumentar el número de profesionales especializados en ciberseguridad; y más teniendo en cuenta las tendencias alcistas de este mercado, el cual consiguió hacer frente a la crisis sanitaria creciendo un 6% en los meses posteriores. (PwC, 2020)

Por otro lado, empresas y organizaciones a nivel mundial se han visto obligadas a intensificar sus inversiones en seguridad de la información debido a la creciente gama de amenazas cibernéticas, el cual se ha intensificado tras la crisis del Covid-19. Como resultado, IDC ha declarado que el mercado de la seguridad nacional ha superado el alarmante nivel de crecimiento del 9,2% con respecto al 2022; alcanzando los 2.130 millones de euros en 2023. (IDC, 2022) Hay varios drivers que han motivado este cambio en el mercado, como por ejemplo el aumento del número de amenazas y la gran sofisticación que han adoptado en el modus operandi, aprovechando la falta de formación y la fragmentación de las organizaciones en materia de seguridad. Asimismo, 68% de las empresas europeas sufrieron ciberataques involucrando el robo de datos (Ransomware) el pasado 2022. Y las tendencias para este próximo 2023 apuntan a una mayor vulnerabilidad de dichas organizaciones debido al extenso número de vías que los ciberdelincuentes están explorando y explotando eficazmente. (PwC, 2022)

Este nuevo escenario requiere una mejora de las técnicas de defensa con el fin de automatizar la detección de ataques. Sin embargo, con este trabajo pretendo demostrar la inminencia de esta amenaza y concienciar de la necesidad de invertir también en estrategias de gestión ante el fraude de identidad y engaño financiero que tanto ponen en riesgo la reputación y la cuenta de resultados de las compañías españolas. Se estima que la inversión anual en ciber resiliencia y seguridad aumentará un 20% para 2024, alcanzando un gasto de 5.900 millones de euros por parte de las principales empresas a nivel europeo con el objetivo de protegerse del impacto del ciber riesgo, viéndose obligadas a reinventarse para adaptar su seguridad a un entorno de riesgo digital mucho más amplio. Por esta razón, en 2023 las prioridades de inversión nacional en seguridad

económica incluirán la creación de métodos de racionalización e integración de entornos y herramientas de seguridad, así como el desarrollo de estrategias de automatización e incorporación de la inteligencia artificial a los frameworks de las empresas españolas. Por ahora, el 39% de las organizaciones reconoce estar llevando a cabo esta transformación digital de sus sistemas de seguridad. (Hiscox, 2023)

Otro factor que convierte a la ciberseguridad en un aliado esencial para las empresas modernas es la dependencia de las tecnologías y la conectividad en línea; lo cual supone un mayor número de oportunidades para que los ciberdelincuentes ataquen. Un ciberataque deriva en graves desenlaces para una empresa, independientemente de su tamaño o influencia en el mercado. (Castellanos, 2019) Daños a la reputación, pérdida de datos confidenciales, exposición de información personal de clientes y secretos comerciales, o la inmediata interrupción del funcionamiento del negocio pueden dar fruto a graves consecuencias. Así, la privacidad de los datos en las empresas está siendo estrictamente regulada con el fin de proteger a los clientes y empleados del robo de sus datos personales. (Ahon, 2022)

Como resultado, las empresas deben adoptar las medidas de seguridad adecuadas; de las cuales, la mayoría hacen referencia a la encriptación de datos, la intensificación en los procesos de autenticación de usuarios y la detección y respuesta a incidentes. Sin embargo, en la misma medida, el establecimiento de políticas y procedimientos capacitados para detectar y responder automáticamente los ataques cibernéticos, así como la formación de los empleados, es esencial para identificar la amenaza a tiempo y minimizar los riesgos.

De este modo, invertir en garantizar la seguridad cibernética de una empresa es un elemento clave para mantener la confianza de los clientes y garantizar la continuidad del negocio; ya que, un incidente de seguridad puede tener un impacto significativo en la reputación de una empresa y puede resultar en la pérdida de clientes e ingresos.

En resumen, la ciberseguridad es una consideración crítica para las empresas actuales debido a los riesgos cada vez mayores de los ataques cibernéticos y las regulaciones cada vez más estrictas sobre la privacidad de los datos. (Cano, 2017) Las empresas deben adoptar medidas de seguridad adecuadas para protegerse contra los ataques cibernéticos y garantizar la privacidad de los datos de sus clientes y empleados. Por el contrario, no invertir en seguridad cibernética puede tener consecuencias graves para una empresa: pérdida de datos, interrupción del negocio, multas y sanciones legales, y pérdida de confianza. (Martín, 2018)

1.2 Exposición de la metodología

La orientación del trabajo se llevará a cabo mediante un enfoque impulsor desde cuatro frentes que considero de implementación necesaria en cualquier protocolo empresarial anti-ciberataques: (1) la Información, (2) la Formación, (3) la Prevención y (3) la Gestión de la crisis, cuatro aspectos que deben estar alineados totalmente para reducir los posibles daños en las empresas siendo todos imprescindibles para instaurar un sistema de protección empresarial frente al riesgo cibernético. Por ello, he decidido organizar mi trabajo de esa manera, al tiempo de que analizaré el impacto de los daños que pueden causar los ciberataques, no solo en las cuentas de resultados de las empresas, sino también en algo tan importante como es su imagen y reputación.

En primer lugar, busco fomentar una cultura de educación empresarial en medios de prevención de ciberataques; lo cual se consigue incrementando la concienciación en dicha materia. Hoy en día es crucial estar informado sobre los riesgos que conlleva ser *hackeado*; y desgraciadamente en España rebosa la presunción errónea de que las únicas víctimas de estos ataques tecnológicos son sólo las grandes empresas. Esto conduce a que las Pequeñas y Medianas Empresas generalmente carezcan de información, conciencia, medidas de prevención y gestión para combatir el ataque y la crisis reputacional que deriva en consecuencia. En realidad, es un riesgo latente del que no se libra nadie, independientemente del tamaño de la empresa, del sector, localización o influencia de poder. (Eckenrode, J. et al., 2018)

Por tanto, es necesario instaurar en la mente del empresario de multinacionales, de pequeñas y medianas empresas, así como en la mente del emprendedor, que convivimos con una pandemia empresarial que requiere el establecimiento de un plan de protección desde el momento en el que la empresa se pone en funcionamiento. Junto a esto, cabe destacar la importancia de destinar un porcentaje de la inversión empresarial a gastos tecnológicos con el fin de desarrollar tecnología preventiva efectiva para combatir el Ciber riesgo; dentro de lo cual abordaré la trascendencia del Aseguramiento Empresarial y su influencia en la posterior gestión reputacional.

Por otro lado, es necesario resaltar que la formación no está destinada únicamente a aprender a prevenir dicho ataque; sino que también comprende el aprendizaje de la gestión empresarial ante la crisis reputacional que este supone. Ya que, pese a orientar todos tus esfuerzos en prevenir un ataque cibernético, no servirá como solución una vez hayas sido atacado. Este último apartado es muy relevante para comprender el modus operandi a la hora de decretar si en última instancia es beneficioso para la cuenta de resultados la toma de ciertas decisiones polémicas; como, por ejemplo: pagar o no un

rescate, delimitar el origen de los fondos que serán derivados para financiar dicho rescate, avisar a las autoridades, determinar la estrategia de marketing y la línea de comunicación con los clientes, precisar qué unidad directiva será la encargada de dirigir la crisis, etc. Por último, para ilustrar la practicidad de este apartado me apoyaré en el estudio del Caso MAPFRE del pasado 2020, analizando el ciberataque y la gestión de la grave crisis reputacional que sufrió como consecuencia.

1.3 Desarrollo y estructura

El trabajo seguirá una estructura organizada en tres partes diferenciadas. Comenzará con un primer apartado Teórico; en el cual expondré una visión general de la Ciber tecnología, los ataques cibernéticos, el riesgo reputacional y su relación conjunta mediante un abordaje primordialmente conceptual. El segundo apartado corresponderá con una parte descriptiva, donde se desarrollarán varios casos relevantes en la vida empresarial española con el objetivo de ejemplificar los conceptos previamente expuestos.

Y finalmente, culminaré con un componente analítico-práctico, en el que estudiaré algún caso real, como el Caso MAPFRE de 2020 y analizaré su actuación modélica en la gestión reputacional del ciberataque. Accederé a la información necesaria para completar el trabajo a través de documentos académicos, experiencias personales y entrevistas con contactos internos y directivos de empresas relevantes del sector que me proporcionarán acceso a bases de datos que facilitarán el abordaje del trabajo.

2. Marco Teórico

2.1 Conceptos básicos de la ciberdelincuencia

Las empresas identifican el fraude que cometen los clientes, en primer lugar, seguido de los delitos cibernéticos, como aquellos fraudes más frecuentes. (PwC, 2020) Además, Según el Foro Económico Mundial 2020, "los ciberataques se perciben como el segundo mayor riesgo global para los líderes empresariales de las economías avanzadas, sólo superado por las crisis fiscales".

Aproximadamente, el 60% del conjunto de estas organizaciones clasifican la seguridad como un aspecto de vital importancia para la supervivencia de las empresas, para el cual es necesario incrementar la formación preparatoria para ser capaz de hacer frente a los ciberataques, así como fomentar la implantación de controles de seguridad continuos (PwC, 2020). Al mismo tiempo, es relevante comparar los resultados de la encuesta con otros de un estudio previo llevado a cabo dos años antes por la misma empresa, PwC, en el cual se estimó que el peso de la ciberdelincuencia crecerá en los próximos años, en volumen y en impacto, a causa del auge de las nuevas tecnologías que impulsan la complejidad y sofisticación de las amenazas.

El Instituto Español de Estudios Estratégicos afirma que "la ciberdelincuencia es toda aquella acción ilegal que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet" (Urueña Centeno, 2015). De igual manera, el concepto de criminalidad informática o cibercrimen hace referencia a delitos de mayor alcance, "como el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos utilizando ordenadores y redes como medio para realizarlos" (Urueña Centeno, 2015).

Asimismo, su práctica extrema se conoce por la denominación de ciberterrorismo, que corresponde a aquellos “ataques premeditados y políticamente motivados en contra de la información, los sistemas computacionales, los programas de computadoras y datos que pueden resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos” (Urueña Centeno, 2015).

El concepto de ciberataque deriva del conjunto de ciberdelincuencia, cibercrimen y ciberterrorismo. Estos se llevan a cabo al detectar fallos que hacen vulnerable al sistema de seguridad de las empresas e identifican deficiencias que facilitan la intromisión de un usuario no legítimo en el acceso a información operativa confidencial de forma remota. (INCIBE, 2020) El fruto de los fallos en el sistema es muy diverso; sin embargo, para conseguir evitar su propagación, las empresas son responsables de concienciarse de los riesgos que conlleva un incidente de este calibre, y por tanto, conocer las vulnerabilidades individuales que sufre su organización para estimar correctamente la probabilidad de que su sistema de seguridad se fragmente y prevenir un incidente mediante el establecimiento de un sistema de análisis de riesgos para detectar, controlar y en caso de que ocurra, mitigar el impacto.

2.1.1 Principales tipos de ciberataques y agentes de las ciber amenazas

Cualquier acción ilegal desarrollada por medios tecnológicos recibe el nombre de ciberataque. Por esa razón, el grado de peligrosidad de un ciberdelincuente varía en cuanto a la finalidad y el procedimiento de la amenaza se refiere. Asimismo, el foco principal de un ciberataque es el aprovechamiento de las debilidades de los sistemas de seguridad para proceder al robo de datos o cifrado de información, destrucción de esta o interrupción de la actividad operativa empresarial entre otros.

1. Según el Glosario de la Guía CCN-STIC 401 (Guía de Seguridad de las TIC del Centro Criptológico Nacional), el código dañino o malware malicious software hace referencia a un ataque informático que busca las debilidades dentro del sistema para proceder a la infiltración o daño de un ordenador sin el conocimiento de su dueño y con finalidades muy variadas.

   Aquí se engloban, los virus, spyware, ransomware o los troyanos. (CCN, 2020) Entre las acciones que realiza podemos encontrar el bloqueo al acceso de componentes de la red (predominante en los ataques de ransomware), la instalación de virus de malware o software dañinos, el robo de datos confidenciales del disco duro (en el caso de los ataques spyware) o la infección de partes esenciales del sistema para interrumpir el funcionamiento de la actividad operativa. (Martínez, 2019)

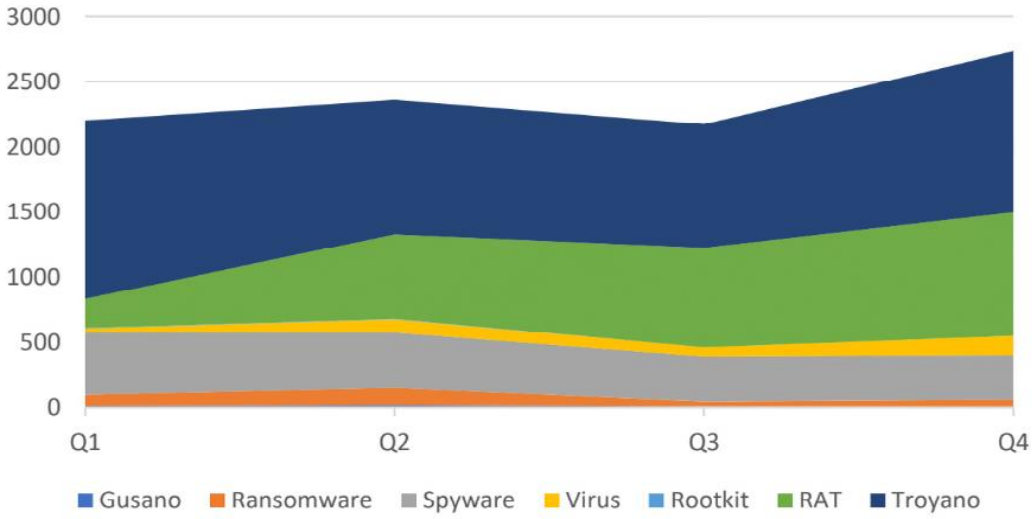

Figura 1: Tipología Malware 2021

Fuente: Ciber amenazas y tendencias. Edición 2022. Centro Criptológico Nacional

Se estima que, en España, aproximadamente uno de cada tres ordenadores está infectado, lo cual clasifica a nuestro país como uno de los cinco primeros del mundo con mayor cantidad de ordenadores infectados. Anualmente, se contabilizan a escala global unos 3.000 incidentes; cada uno de los cuales afecta de media a 20.000 máquinas, y deriva en el robo de cuatro gigabytes de información confidencial. Asimismo, una de cada diez páginas web de Google porta algún tipo de infección, y son los propios fabricantes de antivirus los que asumen su incapacidad para enfrentarse a los miles de códigos maliciosos que invaden los sistemas informáticos de empresas españolas diariamente. (CNN, 2008)

2. Por otro lado, encontramos la Amenaza persistente avanzada (APT); que consiste en una serie de ciberataques dirigidos a instituciones y organizaciones lanzadas específicamente con la finalidad de encontrar el acceso a un sistema informático para proceder al robo de información valiosa y propagar los ciberataques a otros sistemas similares. En las fases iniciales de este tipo de infección, típicamente la primera estrategia se centra en el secuestro de actualizaciones o archivos dañinos del sistema. Dichos archivos son ordenados dentro de los servidores de manera que cuando la organización proceda a la descarga e instalación del programa informático lo haga al mismo tiempo con el programa dañino. En los últimos años ha tenido resultados elevados debido a que las víctimas instalan el malware sin conocimiento. Esta técnica también recibe el nombre de cadena de suministro, y está empezando a emplearse de forma cada vez más habitual para llevar a cabo los ataques mediante dominios de correos fraudulentos, enlaces o archivos dañados. (Martínez, 2019)

3. El ciber espionaje es una técnica que nació en los Estados y organizaciones con el principal objetivo de obtener y/o destruir información confidencial a nivel geopolítico, comercial o de propiedad intelectual, para su posterior utilización para mejorar su posicionamiento en el mercado frente a las organizaciones víctimas.

4. Las amenazas híbridas se refieren al conjunto de técnicas coordinadas que engloban las estrategias de ciberataque, métodos militares, presión económica y diversas campañas en redes sociales para buscar la desestabilización e influencia en la opinión pública. Los responsables que llevan a cabo este tipo de amenazas son tanto agentes estatales como no estatales, y ambos emplean el ciberespacio como herramienta para aprovecharse de la desinformación de las personas, que descargan y abren los archivos sin conocimiento de su fraude. (García, 2018)

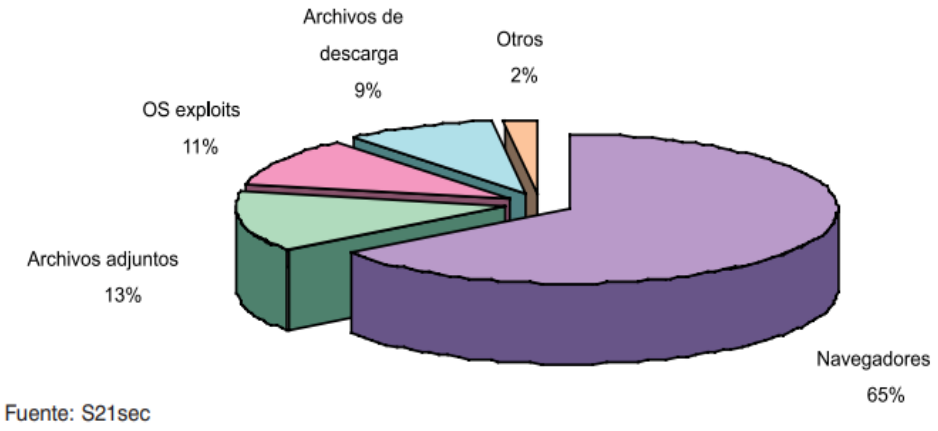

Figura 2: Origen de la infección

Fuente: Evolución del Código Dañino. Edición marzo 2008. Centro Criptológico Nacional de Inteligencia

5. La ciberdelincuencia por medio de los correos electrónicos continúa siendo una de las técnicas más utilizadas para llevar a cabo la primera fase de un ataque. Los agentes emplean este método para acceder fácilmente al sistema de las víctimas y obtener la información que deseen, o bien para analizar la manera en la que está configurado el sistema informático de forma que puedan infectar más partes de este. (CNN, 2008) De hecho, al principio, los objetivos eran individuos escogidos aleatoriamente o sin apenas influencia dentro de las organizaciones. Sin embargo, la tendencia actual redirige los ataques a personas con cierto poder de decisión en las organizaciones para así maximizar el beneficio económico potencial. La metodología principal de estos ataques es mediante el spam; que consiste en el envío de correos no deseados ni solicitados, comúnmente bajo la apariencia de publicidad. A su vez, esta técnica se divide en tres categorías:

a) Spam convencional: Se centra en la promoción de diversos productos o servicios potencialmente fraudulentos.
b) Malware Spam: Envío de correos electrónicos con una infección de malware adjuntos a un documento o una imagen, a través de los cuales se busca dañar el sistema informático de las víctimas de código dañino.
c) Phishing o suplantación de identidad por SMS: Los atacantes se hacen pasar por usuarios individuales u organizaciones y presionan a la víctima a proporcionarle cierta información comprometida sobre su identidad. En los últimos años se ha convertido en la técnica más popular. Aproximadamente, en 2021 el 90% de las infecciones causadas por código dañino, así como el 72% de robo de datos a empresas sucedieron a través del *phishing*. (Martínez, 2019)

6. El Ransomware es un tipo concreto de ciberataque que, mediante la introducción de un código dañino en los sistemas informáticos, consigue acceso a información relevante de las empresas víctimas y así posteriormente procede a exigir un rescate monetario. (García, 2018) Durante el secuestro de datos de ransomware el atacante bloquea los datos de la víctima, y tras el pago del rescate, que se suele realizar con criptodivisas, el atacante proporciona de nuevo la clave que desbloquea los datos cifrados. La constante amenaza de los ransomware fue la principal preocupación del año por parte de los equipos de seguridad de las organizaciones en estos años posteriores a la pandemia del Covid-19. De hecho, en el año 2021, el número de ataques incrementó sustancialmente respecto al comienzo de 2020. Sin embargo, en el segundo semestre de ese mismo año, los incidentes se vieron reducidos, probablemente vinculado al desmantelamiento de Emotet. Aun así, la variación trimestral entre ellos es de apenas un 1%. (CCN, 2022)

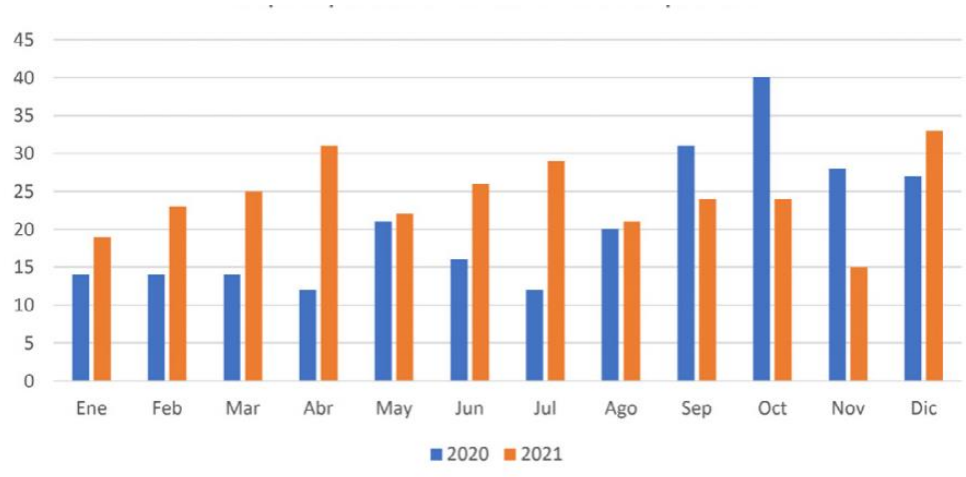

Figura 3: Ataques públicos de Ransomware por mes

Fuente: Ciber amenazas y tendencias. Edición 2022. Centro Criptológico Nacional

7. El cripto hacking consiste en la adquisición de beneficios a través de la creación de la moneda. Este tipo de técnicas son altamente peligrosas, y desgraciadamente han ido aumentando exponencialmente desde 2017. Además, es importante tener en cuenta que, pese a que generalmente estos ciberataques los llevan a cabo entidades externas a las compañías, es posible que también se realicen desde el interior de estas. (FadilpaŠIć, 2022)

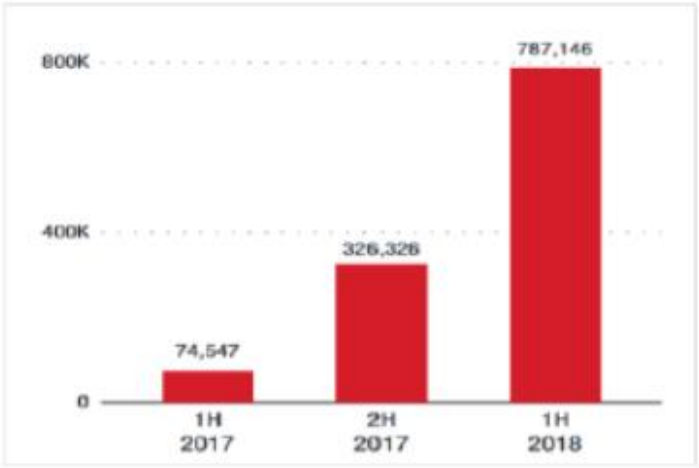

Figura 4: Evolución semestral de los Criptojacking

Fuente: Ciber amenazas y tendencias. Edición 2019. Centro Criptológico Nacional

Más adelante, en 2021, el aumento del valor de las criptodivisas creó una tendencia muy relevante en el empleo de este tipo de amenaza, y se convirtió en la tipología de malware más extendida a nivel global. Esto se debe, esencialmente, a que, en 2021, el valor del Bitcoin superó hasta en dos ocasiones su valor más alto históricamente (ATH): A 1 de enero de 2021, la criptomoneda tenía asignado un valor de 26.500 €: mientras que, a 12 de marzo, esta cifra superó los 51.260€ y el 12 de noviembre alcanzó los 56.280€. (FadilpaŠIć, 2022)

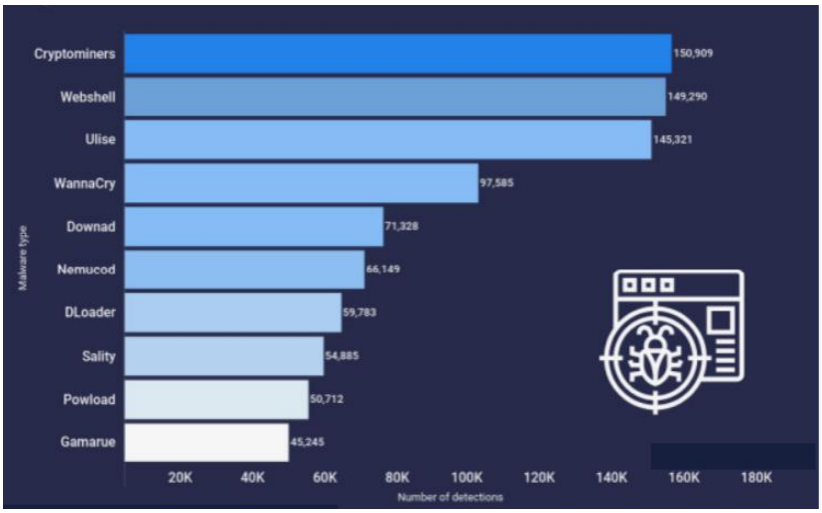

Figura 5: Top 10 malware families in terms of detections in 2021

Fuente: Ciber amenazas y tendencias. Edición 2022. Centro Criptológico Nacional.

8. El robo de identidad e información personal de forma masiva. Incluye incidentes en cuentas bancarias, domicilios o registros contables; y está estrechamente relacionado con el robo de datos de las grandes corporaciones. La Unión Europea ha establecido un nuevo Reglamento General de Datos (GDPR) define las normas a seguir por los propietarios de información personal perteneciente a terceros para la protección de estos; entre las cuales se encuentra el cifrado de datos. Por ende, incumplir esta normativa supone sanciones económicas elevadas. (European Central Bank, 2016)

9. Cada vez son más frecuentes los ataques en web conocidos como *Man-in-the-middle*. El objetivo principal de estos ataques es obtener acceso a información confidencial por medio del espionaje, interrumpiendo los flujos de información existentes entre emisor y receptor para proceder a la filtración y robo de dicha información. Las redes Wi-fi son una de las formas más fáciles de ataque. Es justo

al conectarse la víctima a la red, cuando el atacante aprovecha para introducirse en el dispositivo y acceder a los datos que desee. (CCN, 2022)

10. En 2018 fueron tendencia los ataques DDoS. Estos dañan el sistema operativo del dispositivo informático e imposibilitan la continuidad de la actividad habitual. Por esta razón, este ataque también recibe el nombre de ataques de denegación de un servicio. Su creciente popularidad ha obligado a muchas organizaciones, sobre todo las relacionadas con el sector financiero, a invertir grandes cantidades para ser capaces de defenderse en caso de un ataque.

11. Para entender cómo funcionan los códigos dañinos es necesario hacer referencia a los Botnets, una "colección de ordenadores conectados a Internet que interactúan entre sí para lograr la realización de cierta tarea de forma distribuida". (CCN, 2008) Mediante esta técnica, los ciberdelincuentes acceden fácilmente a los sistemas informáticos de varias víctimas de forma simultánea para robar información comercial relevante. Es un sistema malicioso que se compone de diversos equipos comprometidos que se introducen en la "botnet" sin conocimiento de los propietarios del dispositivo en cuestión. Son los denominados ordenadores "zombies".

12. La criptografía se ha empleado en los últimos años como medida de seguridad en los sistemas informáticos. Su función es impedir que, en caso de acceder al sistema, los atacantes obtengan la totalidad de los datos que buscan. Sin embargo, si los atacantes se conectan a una red Wi-fi, la criptografía no podrá frenar el traspaso de los datos a través del análisis del comportamiento del equipo. Estos

ataques reciben el nombre de canal lateral; y para su realización, los atacantes cada vez más aprovechan el machine learning como para recolectar más rápidamente el comportamiento de un equipo. (Martínez, 2019)

13. Por último, los delincuentes también recurren como método adicional a la ingeniería social para la distribución del virus por medio de USB u otros dispositivos olvidados (consolas, móviles, PDA, etc.). Se espera que esta técnica se perfeccione de cara al futuro gracias al Bluetooth y a los mensajes de contenido multimedia. Hoy en día, son muchos los países que cuentan con una permisividad que indirectamente ampara los delitos cibernéticos. Es el caso de Rusia, Hong Kong, Panamá o Corea del Norte. Y en general, son pocos los países que cuentan con una legislación apropiada en el contexto internacional. (CCN, 2008)

Es relevante mencionar brevemente los principales agentes o grupos que realizan de manera organizada los ataques cibernéticos contra las empresas. En primer lugar, los Estados generalmente lanzan códigos dañinos para identificar las vulnerabilidades de los sistemas informáticos que almacenan la información de las estructuras críticas empresariales. Se ha detectado que el foco de estos ataques principalmente se centra en objetivos europeos, y su finalidad es recoger información sobre el estado de las medidas de seguridad de organizaciones similares.

Por otro lado, están los ciberdelincuentes, el grupo más activo. Sus ataques se dirigen principalmente a empresas, bancos e instituciones financieras, y su metodología más habitual es el phishing; técnica que cada vez es más sofisticada gracias a la ingeniería social y las innovaciones en la automatización y la inteligencia artificial. (Martínez, 2019)

Otro impulsor de ciber amenazas es el ciberterrorismo; grupos cuyos ataques generalmente tienen una motivación religiosa. No se han documentado incidentes relevantes recientemente, pero, aunque escasean, estos grupos terroristas son muy peligrosos; y se diferencian de otros individuos en el uso que hacen de las tecnologías legítimas, como pueden ser las redes sociales para promover su causa, obtener fondos o captar a gente nueva.

Los activistas se enfocan en la destrucción de diversas páginas web, ataques DDoS y la divulgación de información que vulnera la reputación y posicionamiento en el mercado de la entidad dañada. Su finalidad es llamar la atención mediante los ataques para reivindicar sus ideas; mientras que no están motivados por la obtención de beneficio económico. (FadilpaŠIć, 2022)

Por último, existe un grupo de actores internos formado por individuos que a su vez son usuarios propietarios de sistemas de información, o conforman una red de proveedores (en ocasiones por parte de los empleados de la compañía) que de forma premeditada y negligente abren una brecha de acceso en el sistema de seguridad de la entidad correspondiente y se lo proporcionan a los atacantes, generalmente motivados por una compensación económica. (Martínez, 2019)

2.1.2 Análisis macroeconómico: impacto y vulnerabilidad empresarial

La ciberseguridad se coloca indefinidamente en el mapa estratégico de los líderes de toda empresa, ya sea pública o privada, pequeña o grande, así como de los máximos responsables de la política de los países. Cinco años atrás, el indecente Wanna Cry causó un gran impacto mediático que resaltó la importancia de invertir en este sector con el objetivo de minimizar el impacto operacional de los ataques, en el negocio en sí y en la

reputación corporativa; no para tratar de evitar los incidentes. Recientemente, la guerra de Ucrania ha supuesto un telón de fondo que durante el último año ha ido dibujando una posición geopolítica muy compleja, en el que la ciberseguridad regresa como foco de preocupación para los líderes empresariales y públicos. Su impacto se ve reflejado en el volumen de ataques cibernéticos que se han producido en lo que lleva de año. Estos se han multiplicado en número, y lo que es peor, cada vez cuentan con una mayor sofisticación, profesionalidad y por tanto peligrosidad, impulsada especialmente con el auge de las herramientas de generación de inteligencia artificial. (CCN, 2020)

El equipo de CSO ha elaborado un reportaje donde esclarece las Tendencias de Ciberseguridad de 2023 en el que incluye una serie de datos muy relevantes. En primer lugar, comparte el último informe con cifras oficiales del Sistema Estadístico de Criminalidad (SEC), correspondiente al pasado 2021, donde redacta el registro de más de 305.000 ciberdelitos en España, superando en un 6% a la cifra del año anterior. En consecuencia, multinacionales como la consultora Deloitte, clasifican a nuestro país en tercera posición en el ranking mundial de empresas con mayor volumen de ataques informáticos; ya que, aproximadamente el 94% de las empresas españolas fue víctima de un incidente cibernético en 2022. Por ello, incluso el Foro Económico Mundial (FEM) incluye por primera vez en la historia el cibercrimen como parte de la lista de los mayores riesgos latentes que existen a escala mundial, recogido en *The Global Risk Report.*

El lado positivo es que el presupuesto que las compañías destinan a ciberseguridad se verá incrementado en 2023. De hecho, Canalys prevé que este aumento alcance el 13,2% más que en 2022, cuantificando el gasto a nivel mundial en productos y servicios de ciberseguridad en 223.800 millones de dólares. Además, esta inversión se acompañará de

la implementación de nuevas medidas legislativas que serán impulsadas principalmente por la Unión Europea y el sector público; y que irán destinadas al refuerzo de la ciberseguridad en materia de actividad empresarial digitalizada. Un ejemplo de estas nuevas normativas son la NIS2 o DORA; ambas recién aprobadas para entrar en funcionamiento en varios países en 2024. (Foro Económico Mundial, 2023)

Por ende, el mercado de la seguridad cibernética está en pleno auge y cambio constante, acelerado a causa de la proliferación de las herramientas de inteligencia artificial y automatización, que rápidamente comenzarán a aplicarse al entorno de la nube. Este mercado, indirectamente ha activado el ecosistema emprendedor; y ya podemos observar varias *startups* españolas creadas a raíz de estas tecnologías y cuyo futuro es explosivo y prometedor. De hecho, el *Observatorio de Startups* de la Fundación Innovación Bankinter afirma que esto se ve claramente reflejado en la subida desde octava posición en el ranking de inversión sectorial en startups españolas, hasta alcanzar la sexta posición únicamente en el periodo que lleva transcurrido de 2023.

Sin embargo, aún está expuesto a muchos retos, derivados no solamente de la sofisticación de la tecnología y de los atacantes, la cual mejora rápidamente gracias a los avances de la tecnología artificial; sino que, a su vez deberá afrontar los desafíos causados por la fragmentación del propio sector, sumada a la escasez de talento profesional en el mercado tecnológico, y que se agudiza en este segmento industrial. (IDC, 2023)

Así, una cita del presidente mundial de ciberseguridad en Baker McKenzie refleja a la perfección el sentido de este trabajo. Cyrus Vance afirma que *"Estamos viviendo una pandemia mundial de ciberseguridad, pero sin una vacuna. Desafortunadamente, las*

previsiones actuales en dicha materia favorecen al actor criminal, sobre la capacidad de la sociedad para combatirlos. Esto ya no se trata solo de extraer dinero o datos: estos ataques sirven para disminuir la confianza en nuestras instituciones más importantes y sembrar miedo e incertidumbre entre la población".

2.2 La realidad de los ataques cibernéticos

Si bien es cierto que el ciber riesgo ya es considerado como la principal amenaza para las empresas modernas, la probabilidad de concienciación empresarial y cautela ante este supuesto está positivamente correlacionada con la *experiencia* de un ataque cibernético y el consecuente sufrimiento de primera mano de su repercusión en el funcionamiento de la organización. Por esta razón, países como Irlanda califican la ciber amenaza por detrás de las consecuencias de la pandemia. De este modo, se puede identificar la existencia de una brecha muy destacada entre las empresas que han sido víctima de un ciberataque y las que no. Concretamente, el 55% de las primeras, califican el riesgo cibernético como elevado e inminente; mientras que, en el caso contrario, la cifra alcanza únicamente el 36%. (García, 2021)

Sin embargo, todas las empresas coinciden en la importancia de garantizar la protección de los datos de los clientes, socios y empleados; ya que, de lo contrario, supondría graves daños reputacionales. La brecha de percepción se agudiza al comparar las declaraciones de las empresas víctimas de ciberataques frente a las que no han sufrido ninguno, al cuestionar si el grado de exposición al riesgo ha aumentado, disminuido o permanecido en equilibrio en el último año; siendo del 41% y 23% respectivamente. De todos modos, cabe destacar que hay sectores específicos que independientemente de haber sufrido previamente un ataque cibernético, califican la ciber amenaza de "alto riesgo"; como puede ser el sector financiero, quien a pesar de que apenas un 36% haya sido afectado, el

55% de las organizaciones reclama la importancia de la ciberseguridad. Cierto es, que las empresas de servicios financieros se colocaron muy arriba en el ranking de ataques el año de la crisis sanitaria. Como contraste, aquellos sectores relacionados con la alimentación y las bebidas (que corresponden a los más amenazados en 2022), sitúan a la pandemia, la escasez de formación y el aumento de competencia como los principales desafíos, por encima del ciber riesgo. (Cisco, 2023). Un segundo indicador que evalúa la percepción del riesgo es el flujo de capital invertido en seguridad y su variación en los diferentes sectores empresariales. Liderado por el sector servicios con un gasto medio de €31 millones (casi seis veces mayor que la cifra promedio), destaca frente a sectores como el ocio y turismo, que alcanzan los niveles más bajos. (IBM, 2023)

De nuevo, empresas con un grado elevado de *expertise* sumadas aquellas que cuentan con alguna forma de cobertura en materia de ciberseguridad muestran un nivel más alto de concienciación ante el riesgo. Como resultado, el número de organizaciones expertas que califican la exposición a la amenaza del ciber riesgo como latente y elevada aproximadamente dobla (59%) las declaraciones por parte de las startups (32%), aunque cuenten con una estrategia de defensa más reforzada. Asimismo, el 80% de las organizaciones que carecen de cobertura alguna y declaran no tener intención de obtenerla, no han sido víctimas de ciberataques en el último año. Sin embargo, la mayoría (el 51%) son startups, y no han experimentado el cambio de percepción que adquieren las empresas que han sufrido el ciber riesgo de primera mano. De este modo, las grandes empresas, y en especial las víctimas de ciberdelincuencia, tienen una mayor confianza a la hora de enfrentarse y salir victoriosos ante un ataque de esta naturaleza que las pequeñas y medianas empresas. (Martínez, 2023)

Por último, el teletrabajo aumenta la exposición y por tanto la vulnerabilidad a recibir ataques (apoyado por el 62% de las empresas aproximadamente); de las cuales, en aquellas que cuentan con una plantilla mayor a 250 empleados la cifra aumenta hasta 69%, 76% de media en las empresas expertas y 49% de las novatas. El trabajo remoto ha transformado el foco de los ciberataques. Ahora, los hackers optan por emplear tanto los servidores de empresa como el servidor almacenado en la nube como portal de entrada. Por tanto, la aceleración de la digitalización de las pequeñas y medianas empresas a causa de la pandemia, así como el extenso volumen de teletrabajo en las grandes organizaciones actúan en consonancia con la advertencia de que las agencias de seguridad internacional están difundiendo en relación con la infraestructura en la nube como blanco latente de la ciberdelincuencia. (Hiscox, 2022)

Pero ¿Son sendos indicadores de percepción acordes con la realidad? ¿Se asemejan adecuadamente al riesgo real? Como se ha demostrado anteriormente, hay cierta relación entre el grado de exposición al riesgo percibido y la incidencia de ciber amenazas. A mayor experiencia, mayor probabilidad de concienciación ante el ciber riesgo. Dicha lógica se demuestra en tanto que estas empresas captan la atención de los ciberdelincuentes con más frecuencia que las otras, probablemente debido a su tamaño. Sin embargo, sigue existiendo una brecha de información que separa la percepción de la realidad, y es la relacionada con los tipos de ataques. La mayoría de las empresas fracasa a la hora de identificar las áreas con un mayor riesgo de ataque. donde. Muchos derivan su foco de atención al riesgo de extorsión cibernética, cuando en realidad, la distribución indebida de los recursos de TI y el fraude a causa del desvío de pagos conforman los dos tipos principales de ciberataques actualmente, con un porcentaje del 19, 32 y 31 respectivamente. Por tanto, las organizaciones deben seguir una formación continua para

estar al tanto de los riesgos latentes que amenazan la continuidad del negocio. (Mossburg, 2016)

3. Ciberdelincuencia en las empresas: Impacto Corporativo de un ciberataque

"El mundo empresarial funciona con tecnologías diseñadas para compartir información, no para protegerla. Por ello, también se pueden dar incidentes en los que la información es cambiada por información falsa lo que perjudica el correcto funcionamiento de las empresas" (Martínez, 2019)

Los ciberataques buscan perjudicar la infraestructura de la compañía a través del espionaje o robo de información para después publicarla y dañar la imagen de la compañía. Por esta razón, la gestión del ciber riesgo está experimentando un profundo cambio. Los ejecutivos y los consejos de administración empiezan a creer que los ciberataques son más probables -y quizá inevitables-. Los líderes empresariales están descubriendo que las tecnologías creadas para compartir información, no para preservarla, se han utilizado sobre todo para conectar a nuestra sociedad. Entienden que, para gestionar información sensible y hacer funcionar infraestructuras cruciales, deben confiar en las personas, tanto en sus propios trabajadores como en los terceros con los que hacen negocios. Empiezan a darse cuenta de que les resulta imposible priorizar constantemente la seguridad y bloquearlo todo, debido a la estrecha relación entre su plan estratégico y el desarrollo del riesgo cibernético. (IMF, 2018)

Como resultado, muchas empresas han comenzado a adoptar un modelo basado en la Seguridad, Vigilancia y Resiliencia; el cual consigue implementar un sistema de equilibrio entre los fondos invertidos en ciberseguridad, y las iniciativas dirigidas a la

concienciación del ciber riesgo y al desarrollo de métodos de respuesta más rápidos y eficaces. La formación en las organizaciones sobre el riesgo cibernético es indispensable; puesto que, gracias a ello, los empleados estarán capacitados para enfrentarse a una amenaza potencial, podrán evaluar con éxito los pasos a seguir, y adoptarán una comprensión completa sobre los posibles efectos que habrá en su empresa. (Llorente, 2021)

Sin embargo, existen percepciones generalizadas acerca del impacto de la ciberdelincuencia. Están sobre todo determinadas en función a la información que las empresas están obligadas a notificar públicamente, principalmente cuando se trata del robo de información personal identificable (IPI), la violación de la privacidad de datos de pago e información sanitaria personal (IPS). De esta manera, el foco del debate suele posicionarse en los costes asociados a la notificación del incidente a los clientes, la supervisión del crédito y las posibles implicaciones reglamentarias. Por consiguiente, las empresas han comenzado a invertir grandes cantidades en estrategias diseñadas para precisar y mitigar estos costes. Y en general, el sector concurre en el desarrollo de un "coste por registro" para tratar los casos relacionados con las violaciones de datos de la red de clientes; ya que, comúnmente, las consecuencias de este tipo de ciberataque son las más visibles para el consumidor y aparecen en la fase inicial del proceso. (IBM, 2020)

No obstante, los ciberdelincuentes no siempre fijan su objetivo en el robo de información personal. En su lugar, escasea el manifiesto de incidentes dirigidos a la destrucción de datos y la propiedad intelectual (PI); que indagan en el espionaje, o aquellos enfocados en la inutilización de infraestructuras esenciales para interrumpir la continuidad del negocio. Casualmente, la realidad es que el impacto de estos ataques cibernéticos puede

ser mucho más perjudicial para las empresas; aunque su cuantía es más difícil de calcular. Para hacer frente a los impactos menos superficiales, una opción acertada sería aplicar una estrategia multidisciplinar centrada en conocer en profundidad el contexto empresarial en el que ocurren los ciberataques, para así poder aplicar las técnicas de valoración adecuadas y estimar la cuantificación financiera de los daños. Por tanto, visibilizar la variabilidad desmedida de estas implicaciones en el funcionamiento de un negocio, puede motivar a los líderes a optimizar el método de gestión del riesgo cibernético de su empresa; y, por ende, perfeccionar su capacidad de respuesta y recuperación al ser víctimas de un ciberataque. (Montoya Moreno et al., 2019)

Figura 6: Evolución de los riesgos globales en términos de probabilidad

Fuente: (Montoya Moreno et al., 2019)

A la hora de estudiar el impacto derivado de un ciberataque se puede o bien llevar a cabo una clasificación superficial atendiendo a un enfoque temporal, o bien un análisis más profundo haciendo referencia al tipo de coste; dentro del cual se distinguen dos subvariables: aquellos que perjudican directamente la cuenta de resultados e impiden a la continuidad del negocio, y aquellos cuyo impacto va más allá del financiero, afectando a

la reputación corporativa, el valor de la marca y su relación con los clientes y diferentes entidades socias. (Montoya Moreno et al., 2019) A partir del primer método de clasificación, podemos distinguir dos tipos de costes:

En primer lugar, identificamos los costes transitorios que surgen como resultado de un ataque de seguridad. Estos incluyen costes por la interrupción de la actividad de negocio y la reducción de la productividad derivada de la indisponibilidad de los recursos que han sido afectados por el hackeo. Aparte, cabe destacar los costes materiales y financieros que tendrán que ser destinados a la detección, contención, reparación y reconstrucción de dichos recursos; así como la recopilación de pruebas, investigación y procesamiento del atacante; los asociados a las fuentes encargadas de suministrar la información a los clientes y al público; y otros costes relacionados con la gestión de los medios de comunicación. (Mossburg, E., 2016)

Por otro lado, existen unos costes permanentes; cuyo impacto se mantiene a largo plazo y cuyos efectos tienen un alcance más significativo en el flujo de caja futuro de la respectiva compañía. Algunos de estos costes se enfocan en el impacto que supone la pérdida de clientes (los cuales tienden a reconducirse hacia la competencia) combinado con la gran dificultad de atraer a un nuevo grupo de clientes a causa del aura de inseguridad e incertidumbre que ha provocado la brecha en el sistema de seguridad. Como consecuencia surge el coste derivado de la pérdida de confianza por parte de la red de clientes y socios comerciales; sumado a las responsabilidades legales a las que tendrá que enfrentarse la empresa al haberse violado el acceso a información confidencial y de propiedad, a secretos comerciales… De este modo, la percepción de un riesgo empresarial más elevado es directamente proporcional a un aumento del coste del seguro de la

empresa, y consecuentemente también de los costes de capital en el mercado de deuda y acciones. (PwC, 2022)

3.1 Principales Daños

3.1.1 Daño Operativo y Financiero

- Costes asociados a la investigación técnica

Estos costes directos se ocupan de llevar a cabo un análisis exhaustivo que consiga determinar el origen del incidente, la identidad del responsable y el alcance de los daños a nivel técnico. Su principal objetivo es actuar como plataforma de soporte para detener la propagación de los daños y mitigar el impacto que ha repercutido en las infraestructuras técnicas y bases de datos. Así, los costes de investigación proporcionan un análisis forense digitalizado completo del malware y del resto de amenazas potenciales; y una vez identificada la raíz, su función es contribuir a la recuperación de sendos sistemas dañados atendiendo a la complejidad del ciberataque. (Castellanos, 2019)

- Notificación del incidente a los clientes

Notificar una violación de los derechos de un cliente genera una serie de gastos relacionados con la gestión de dicha información y el asesoramiento proporcionado a los clientes cuyos datos se han visto comprometidos, acorde a la normativa exigida por la legislación estatal, federal o la referente a ese específico sector. Pueden incluir servicios de impresión, correo y centros de llamadas, entre otros.

- Costes de protección de la red de clientes

Los costes de protección del cliente tras la violación son los costes directos asociados a los servicios de detección y protección frente a posibles intentos de uso de los datos personales para fines no autorizados. (Mossburg, 2016)

- Costes regulatorios y normativos

Estos costes hacen referencia a las multas o tarifas impuestas como consecuencia de incumplir las leyes / regulaciones (bien sean federales o estatales) asociadas con ataques cibernéticos. Cabe destacar que, de cara al futuro, el enfoque mayormente empleado en las infracciones está provocando un creciente escrutinio regulatorio y legislativo. Por tanto, es posible que complique los costes de cumplimiento en ambos niveles (incluyendo la preparación y defensa en contra de las acciones de cumplimiento del gobierno). (PwC, 2020)

- Costes de Relaciones Comerciales

Son aquellos costes directos que están relacionados con el proceso de gestión de las comunicaciones externas o los encargados de realizar el seguimiento de la marca tras una infracción cibernética.

- Costes por honorarios y litigios

Incluyen una extensa variedad de honorarios de asesoría legal; así como la imposición externa de los costes de liquidación y costes derivados de acciones legales que la compañía puede emplear para defender sus intereses. Existe la posibilidad de compensar dichas tarifas si se recurre a la recuperación de daños como consecuencia de un litigio iniciado contra un atacante, especialmente al tratarse de un robo de propiedad intelectual.

Aunque el proceso puede alargarse años hasta ser completado a través de litigios, además de no poder garantizar el éxito en última instancia, independientemente del veredicto. Según un informe realizado por Deloitte, las empresas podrían tener que hacer frente, de media, a $10 millones aproximadamente en costes por honorarios de abogados y liquidaciones potenciales de reclamos por pérdidas, entre otros. (Mossburg, 2016)

- Costes para reforzar el sistema de ciberseguridad

Es muy importante derivar ciertos costes a mejorar la infraestructura del sistema de ciberseguridad, los controles de acceso, y establecer una monitorización regular de los procesos afectados para reiniciar la actividad comercial tras un incidente o con el fin de evitar futuras brechas de seguridad.

3.1.2 Daño Reputacional

- Costes derivados del aumento de la prima de seguros

Los aumentos de las primas de seguro son una serie de costes adicionales que la entidad asegurada puede incurrir para adquirir o renovar las pólizas de seguro de ciber riesgo después de un ataque cibernético. Deloitte publicó un estudio en 2020 que indica que cada vez es más común que un asegurado se enfrente a un aumento del 200 por ciento en las primas de seguro; bien sea para la misma cobertura u otra nueva.

- Costes de deuda

Al caer la posición en la calificación crediticia indirectamente aumenta consigo el coste derivado de la deuda. Tras el incidente, la víctima tendrá que asumir tasas de interés más elevadas para acceder a capital prestado; ya que pasarán a ser considerados como prestatarios de alto riesgo tras haber sufrido un ataque cibernético. A corto plazo, en los

meses posteriores al incidente, las agencias de calificación crediticia suelen disminuir de categoría a estas organizaciones. (Mossburg, 2016)

- El impacto de la interrupción del negocio

La interrupción de la actividad empresarial produce costes elevados y a su vez muy variables. Pérdidas a causa de la manipulación de las operaciones comerciales y capital invertido en la reconstrucción de dichas capacidades operativas son algunos de los costes asociados con el impacto indirecto de la destrucción operativa. Incluye la reparación de los equipos e instalaciones afectadas, así como la reconstrucción de la infraestructura global, la desviación de recursos o aumento de estos con el objetivo de financiar operaciones comerciales alternativas que reemplacen aquellos que hayan sido paralizados temporalmente a causa del ataque. El método de cálculo de estos costes depende específicamente de la naturaleza de la destrucción operativa. Se debe adecuar a cada situación y requiere por lo tanto el conocimiento directo de varios componentes determinados de información acerca del incidente. (Ureña Centeno, 2015)

- Pérdida de valor de las relaciones con los clientes

En el periodo inmediatamente posterior a un ciberataque puede resultar complicado cuantificar el volumen de clientes que se perderán. Sin embargo, economistas expertos asignan un “valor” a cada uno de los clientes de la empresa para determinar la cantidad que se necesita invertir para adquirir o mantener dicho cliente. Después, proceden a realizar un análisis de probabilidad de los ingresos que cada cliente de manera individual puede generar para la empresa durante un periodo más duradero. De esta manera, los resultados se evalúan y clasifican en base a la industria a la que pertenecen y a las particularidades de cada organización, para determinar una estimación aproximada de la inversión necesaria para atraer a un nuevo cliente.

- Valor de los ingresos de contratos perdidos

Este coste indirecto hace referencia a la pérdida tanto de ingresos como de oportunidades potenciales de aquellos contratos que han sido rescindidos como resultado de un ataque cibernético. El impacto financiero de este coste de oportunidad perdido se cuantifica por medio de una estimación ajustada del valor de los contratos antes y después del ciberataque; de tal manera que, si la empresa en cuestión sufre pérdidas de contratos, se asume una consecuente disminución en los ingresos. (Montoya Moreno et al., 2019)

- Devaluación de la marca comercial

La pérdida de valor del nombre comercial, marca o símbolos organizativos distintivos de un producto o servicio es un coste intangible que conlleva un fuerte impacto reputacional en las organizaciones víctimas de un ciberataque; el cual se determina analizando el valor aproximado del nombre comercial tanto antes como después de evaluar el incidente cibernético.

- Pérdida de propiedad intelectual (PI)

Los costes adicionales asociados a la pérdida de PI son directamente proporcionales a la pérdida del control exclusivo sobre información patentada confidencial; como pueden ser los secretos comerciales, patentes, derechos de autor, diseños, marcas comerciales y planes de inversión: Es decir, todo aquello que puede conducir a la pérdida de una ventaja competitiva y que además incurre en un daño económico a largo plazo y potencialmente irreparable para la empresa. (Mossburg, 2016)

3.3 Tendencias en ciberataques en 2023

“Los ciberataques en todos los sectores de la industria aumentaron un 28% en el tercer trimestre de 2022 en comparación con 2021. Y, si no se toman las medidas adecuadas, la

cifra aumentará" revela Miguel Hernández, director de ingeniería de Checkpoint México. Prevé que los ciberdelincuentes recurrirán mayoritariamente a las técnicas de ataque del malware, el phishing, el hacktivismo y los *deep fakes* en este próximo 2023.

A su vez, permanecerán inminentes los ataques de ransomware, que ya fueron la principal amenaza corporativa durante los primeros meses de 2023, y que aumentaron hasta un 42% hacia finales del segundo semestre. Estima que este año el ecosistema del ransomware evolucionará y aumentará el volumen de ataques, pero esta vez serán perpetrados por grupos reducidos y ágiles. (Foro Económico Mundial, 2023)

Adicionalmente, el phishing se sofisticará y abandonará los ataques por dominios de correo electrónico. Los ciberdelincuentes incluirán nuevas herramientas colaborativas como Teams, OneDrive, Google Drive o Slack como fuente de obtención de datos críticos para las empresas; ya que, tras la pandemia, un porcentaje amplio de los empleados trabajan de manera remota.

Por último, la tecnología deep fake será utilizada cada vez más con el objetivo de manipular la opinión pública, engañar a los empleados para colaborar inconscientemente con el atacante al cederles sus correspondientes credenciales de acceso al sistema. Por otro lado, LexisNexis Risk Solutions publicó un estudio sobre el "Estado de Fraude e Identidad" en el que afirma que de cara al 2023, los hackers centrarán su objetivo en aquellas personas cuyo conocimiento del uso de dispositivos tecnológicos sea menor; especialmente el uso de los teléfonos móviles, cuyo conjunto representa aproximadamente el 77% del volumen de las transacciones de pagos diarios a través de Internet. (IDC, 2023)

Los ataques de Botnets experimentaron un incremento del 38% en 2022, y este dato empeora en lo que se refiere a las empresas dedicadas al comercio electrónico, cuyo valor alcanzó el 155%. Geográficamente, Europa junto a Oriente Medio y África registraron el mayor volumen de ataques de bots, 98%; seguidos por América Latina con un 83%.

Cabe destacar, que la introducción de nuevos métodos de pago y la rápida digitalización de las empresas ha acelerado la evolución de las técnicas fraudulentas; en especial el fraude de códigos QR debido a la fuerte demanda de los pagos *contactless*. Además, la tendencia de "compre ahora y pague después" ha revolucionado el continente asiático y recientemente está ganando presencia en Europa y África particularmente; lo cual deriva en un aumento considerable del fraude de apertura de nuevas cuentas de pago.

(Jabbour, 2022)

4. Ciclo de vida de la ciberseguridad empresarial

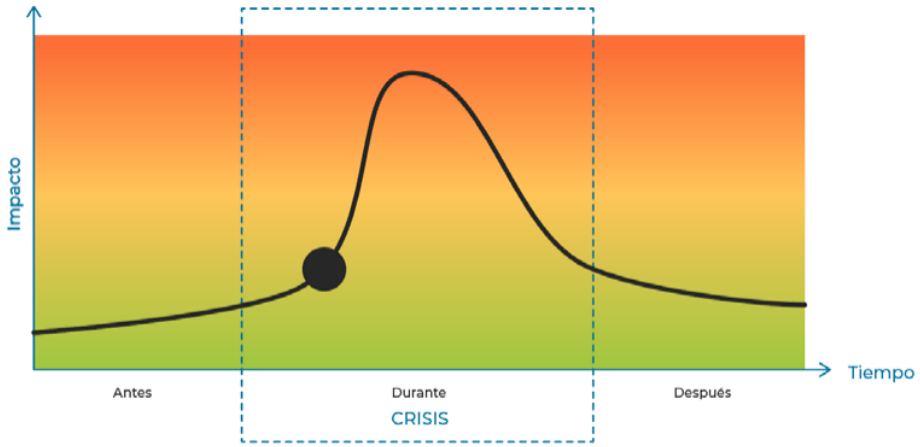

Figura 7: Ciclo temporal de un incidente que deviene una crisis

Fuente: Gestión de crisis para ciber incidentes en entidades locales. Centro Criptológico Nacional 2023

Toda crisis requiere tomar decisiones sometidas a mucha presión, con un periodo de tiempo reducido y generalmente con información incompleta, en diferentes frentes de forma simultánea y con diversos grupos y personas interviniendo en paralelo. Concretamente, las ciber crisis se diferencian por requerir tiempo y personal especializado en el análisis del incidente y la posterior recuperación del sistema operativo, y, por ende, es habitual encontrar dificultades en la conciliación de las prioridades entre la investigación de los hechos y la necesidad de reactivar los servicios que presta la empresa; así como cohesionar los diferentes lenguajes y cultura de silos que existen entre los equipos de soporte. Por eso, es esencial planear con antelación un esquema de actuación, respuesta y participación. (Martínez, 2019)

Por otro lado, para gestionar correctamente una ciber crisis es necesario tener en cuenta que estos incidentes cuentan con unas características muy específicas:

a) Hay un riesgo muy elevado de que la amenaza supere la capacidad de la empresa.
b) Se debe seguir a la perfección la normativa de obligado cumplimiento establecida para estos incidentes, como por ejemplo la relativa a protección de datos.

Teniendo en cuenta estas condiciones, el Centro Criptológico Nacional plantea una guía secuenciada en etapas o fases para asegurar que determinados incidentes escalen internamente de forma rápida y afecten a la operatividad y reputación de la entidad. (CCN, 2020)

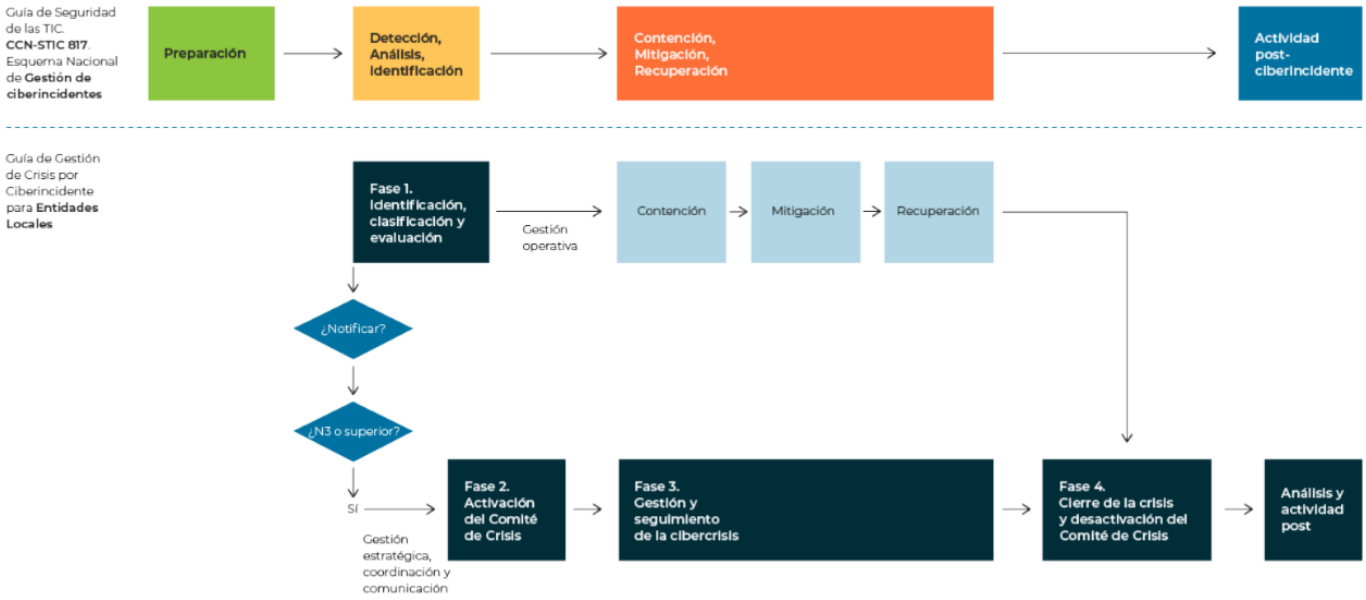

Figura 8: Fases de la gestión del incidente en caso de que se pueda clasificar como crisis

Fuente: Gestión de crisis para ciber incidentes en entidades locales. Centro Criptológico Nacional. 2023

Un estudio realizado por el Fondo Monetario Internacional revela que los ciberataques son capaces de comprometer entre el 9% y el 62% de los ingresos netos de una empresa (IMF, 2018). Este riesgo se agrava debido a que el sistema financiero está interconectado; lo cual ralentiza la resolución de la avería, propaga el miedo de que la brecha financiera se expanda rápidamente y cunde el pánico.

Adicionalmente, ser víctima de un ciberataque provoca la pérdida de confianza en la empresa y daña su reputación. Es importante diferenciar los ataques cibernéticos de los choques financieros. Ambos crean inestabilidad sistémica pero su metodología y su finalidad son muy dispares. El primer punto diferencial es la premeditación y preparación del ataque; los ciberataques se planean con mucho tiempo de antelación, mientras que las crisis financieras carecen de programación previa. La complejidad es también un punto

clave que diferencia los riesgos cibernéticos de los financieros, siendo el sistema de los primeros mucho más complejo, y, por tanto, incapaz de ser estudiado mediante modelos generalizados. Por último, se debe destacar el carácter internacional de los ciberataques. Estos se realizan intencionadamente con un fin malicioso y fraudulento, y consecuentemente suelen amenazar la estabilidad financiera de la entidad víctima. Sin embargo, una crisis financiera surge por un fallo del mercado, sin aviso previo (Montoya Moreno et al., 2019).

Un ataque que daña el sistema de pago de una empresa puede derivar en una mayor inestabilidad económica debido a la inevitable interrupción de la actividad operativa y prestación de servicios críticos durante un periodo de tiempo indeterminado y generalmente de larga duración, así como el robo de información y datos confidenciales. De esta manera, en la Figura 9 (Granados Franco, 2020) se puede observar la rapidez con la que los riesgos tecnológicos se han convertido en una preocupación cada vez más relevante en la sociedad, alcanzando la quinta y octava posición en la escala de riesgos principales del año 2020.

Figura 9: Principales riesgos que se espera que aumenten en 2020

Fuente: (Granados Franco, 2020)

4.1 Plan de Acción

4.1.1 Prevención

El primer paso para implantar un plan de ciberseguridad exitoso es invertir en sistemas de prevención; y para ello es fundamental ser consciente sobre los riesgos y la constante evolución de las amenazas y el desarrollo de nuevas soluciones para frenar los ataques. Un pilar clave para una prevención efectiva es la formación en materia de ciberseguridad y el conocimiento sobre el funcionamiento de las herramientas necesarias para afrontar un incidente. (García W., 2021) Asimismo, es muy importante garantizar que las instalaciones físicas están altamente protegidas y restringir al personal no autorizado para evitar su acceso y manipulación de información crítica. De esta manera, el proceso de prevención se compone de:

a) La imposición de medidas reglamentarias técnicas, organizativas y legales; como por ejemplo instalar programas antimalware y antifraude, proteger las comunicaciones comerciales, controlar el tráfico de los datos confidenciales, invertir en la inteligencia de seguridad, etc. “Las copias de seguridad son la salvaguarda básica para proteger la información de la empresa” (INCIBE, 2017); y, por tanto, proteger la integridad y confidencialidad de la información comercial de la entidad también se puede conseguir a través del cifrado de datos o protección del *malware*.

b) La red es segura en tanto la empresa invierta en el establecimiento de acciones diseñadas para garantizar la protección de los sistemas informáticos de los ordenadores físicos y los recursos de red; cuya finalidad es salvaguardar la fiabilidad de integridad de los datos

almacenados en los discos duros de la organización. Para que dicho sistema de seguridad proteja los datos de forma efectiva, deberá estar compuesto por muchas capas; para que, en caso de que una falle, el resto permanezcan operativos, actúen de blindaje de la información y detengan el ataque. Por esa razón, la fase de prevención requiere tres pilares para ser eficaz: la definición de una política de seguridad que sea clara, su implementación en todo el sistema informático y el sometimiento a continuas revisiones de auditoría (Fundación Telefónica, 2016). Este esquema de acción estratégico marca las directrices a nivel de seguridad en todo proceso del negocio.

Las prácticas de seguridad en el ámbito organizativo son establecer "un código de buenas prácticas, una política de seguridad, procedimientos de clasificación de la información, establecimiento de roles y niveles de acceso, formación e información interna y sistemas de gestión de seguridad de la información" (Fundación Telefónica, 2016). Por tanto, cuando una empresa se encarga del desarrollo y difusión de una política de seguridad que identifique claramente las fases a seguir en un ciberataque, refleja una mayor preparación para la gestión de una ciber crisis y es síntoma de un fuerte compromiso con la seguridad de la empresa. Además, la existencia de un sistema normativo que establezca procedimientos encargados de desarrollar las obligaciones a las que están sujetos los empleados sugiere que se trata de un plan de prevención seguro.

- La gestión de identidades es otro aspecto organizativo esencial. La empresa debe asignar las credenciales y permisos correspondientes al acceso a activos críticos a una persona concreta. Esta política de control

mediante herramientas de control de accesos consigue mitigar el riesgo de filtración interna. (Economist, 2015) Adicionalmente, es recomendable que la empresa desarrolle un sistema de previsión organizado para reducir las brechas de seguridad, especialmente cuando se producen cambios de roles, al autorizar y desautorizar de forma continuada el acceso a la información confidencial. Es por ello, que la existencia de un protocolo eficaz y ágil de autorización e identificación puede suponer una diferencia en el refuerzo del sistema de seguridad de la organización.

c) Por último, es esencial tomar una serie de medidas legales para prevenir la fuga de datos críticos; como por ejemplo la solicitud de aceptación de política de seguridad y confidencialidad, para garantizar una mayor seguridad interna con la plantilla de empleados. Aparte de la preocupación por una posible fuga de datos, la seguridad legal de una empresa es un requerimiento para el obligatorio cumplimiento de la normativa que engloba a la organización; hacen referencia al conjunto de contratos vinculantes entre la empresa y los servicios externos subcontratados. Estos acuerdos identifican qué activos se encargan de vigilar al proveedor, a la empresa, quién realiza la clasificación de incidentes, las tareas de seguridad y las obligaciones contractuales. (García W., 2021)

4.1.2 Detección

La detección de un ciberataque puede ocurrir durante el desarrollo del propio ataque o una vez este haya finalizado. El escenario ideal es detectar la amenaza en tiempo real a través del antivirus instalado para frenar los ataques de malware. Sin embargo, una

detección posterior suele implicar mayores secuelas ya que los atacantes han podido infiltrarse en la documentación restringida y actuar libremente. (Cisco, 2019)

Las herramientas de seguridad de red son efectivas para detectar patrones de ataque conocidos. La desventaja de estos patrones es que son un fenómeno creciente entre los ciberdelincuentes que cambian constantemente sus estrategias. Los ataques ya tienen diferentes patrones que se pueden ejecutar en cualquier momento. Por lo tanto, la detección proactiva es un elemento crítico en la detección temprana de amenazas, mientras que la detección reactiva proporciona una solución cuando se ha producido un ataque en una ubicación esperada. La efectividad de los modelos proactivos está asegurada por su revisión periódica y una configuración de red más agresiva. (García W., 2021)

El dilema surge cuando las empresas no realizan escaneos de vulnerabilidades a menudo, sino una vez al trimestre o una vez al año. Por lo tanto, el monitoreo continuo es esencial, ya que, cualquier ataque después del parche permanecerá sin ser detectado hasta la próxima revisión. De este modo, la implementación de un programa continuo de monitoreo de riesgos y vulnerabilidades es esencial para la ciberseguridad; y para que este sea eficaz, deberá tener en cuenta el tamaño de la empresa y definir las responsabilidades de aquellas personas que activarán el plan (Fundación Telefónica, 2016).

4.1.3 Respuesta

Una vez materializado un ciberataque, es importante que la empresa active su respectivo protocolo de actuación. Por un lado, es necesario proporcionar una respuesta en materia

técnica al daño informático. Mientras que, por otro lado, la empresa deberá acudir a las fuerzas y cuerpos de seguridad del Estado para emprender consecuencias legales. (Castellanos, 2019)

El periodo posterior a un ciberataque sigue una cronología específica y a su vez un protocolo de respuesta diferenciado. En primer lugar, según un estudio realizado por Carlota García en 2021, las tres fases en las que se divide la respuesta al ataque se clasifican en:

1. Triaje del ataque: Sucede apenas horas o días después del ataque. Aquí se deben tomar las decisiones de actuación a corto plazo, se acuerda la forma en la que se comunicará al entorno externo de la compañía, se desarrolla una estrategia para garantizar la continuidad del negocio y se realiza un análisis técnico de lo ocurrido.

2. Gestión del impacto: Esta fase empieza semanas o meses después del ataque y se centra en combatir y solventar las consecuencias más visibles del incidente. Mitigar el daño a la relación con la red de clientes, reajustar el proceso operativo a las necesidades actuales de la organización, llevar a cabo auditorías internas periódicas que verifiquen la eficacia de seguridad implantada e iniciar los procesos legales referentes al ataque.

3. Recuperación del negocio: Ocurre meses después del incidente, y consiste en finalmente reparar los daños a largo plazo y desarrollar una estrategia de prevención para evitar que vuelva a pasar. En esta fase se rediseña el proceso del

negocio, y se desarrollan estrategias para recuperar y mejorar la reputación de la compañía, garantizar la seguridad de la información y monitorizar el funcionamiento de los sistemas de detención.

4.2 Problemática en la defensa de la Ciberseguridad en las empresas

La única forma que existe para que las organizaciones puedan hacer frente a las ciber amenazas es incorporando las medidas de seguridad adecuadas. Para defenderse correctamente es necesario tener la capacidad de anticiparse al ataque antes de que este ocurra, para así poder planificar una estrategia que esté a la altura de la amenaza. Asimismo, es esencial que se tenga conciencia de la vulnerabilidad de la organización; ya que, esto identificará las evidencias perceptibles de las posibles consecuencias e impacto del ataque y posteriormente probará la eficacia de las medidas adoptadas. (Foro Económico Mundial, 2023)

Sin embargo, en líneas generales, actualmente solo se lleva a cabo la asignación de recursos una vez se haya producido una violación grave de la seguridad de la empresa. De este modo, en los últimos años, la estrategia escogida por las empresas como la más rápida y rentable es optar por la subcontratación de “gran parte de la complejidad de la gestión de seguridad cibernética a proveedores de servicios de seguridad”. (Martínez, 2019)

De hecho, es remarcable la baja importancia que se otorga a que una organización desarrolle un software de seguridad o cuente con la última actualización de software. En muchas ocasiones, los planes de acción y los programas empleados están anticuados y defectuosos; y, por lo tanto, son incapaces de ofrecer una protección de calidad a los

sistemas frente a la sofisticación de los nuevos ciberataques. Incluso, han sido registradas 34 ocasiones en las cuales las organizaciones optan por no implementar las medidas mínimas necesarias que en su defecto hubieran podido garantizar dicha protección o habrían conseguido reducir el impacto del ataque. (IBM, 2020)

Adicionalmente, las organizaciones se ven obligadas a enfrentar el problema de la desinformación sobre los ciberataques; y eso dificulta la creación de un sistema de seguridad adecuado para gestionar el riesgo de las amenazas. Incluso, la mayoría de ellos ni siquiera se encuentran recogidos en la legislación vigente a nivel global. Por ello, entre otros, es que las empresas derivan su foco de preocupación únicamente a incidentes ya ocurridos, o en aquellas más comunes. Consecuentemente, sobrestiman su protección ante posibles amenazas e ignoran muchas brechas de sus sistemas de seguridad, y tampoco tienen en cuenta las pérdidas potenciales tanto a corto como a largo plazo. The Economist publicó un artículo que afirma que una empresa tarda alrededor de 205 días en ser consciente de que ha sido atacada, lo cual pone en peligro a todo el sector; ya que, deja tiempo suficiente como para que los atacantes puedan atacar a otras entidades. (The Economist, 2015)

Esto sirve como demostración de que las pruebas de intrusión son críticas para tratar de detectar cuánto antes un ciberataque, evitar el robo de datos e identificar dónde existen brechas dentro del sistema de seguridad. Este mismo artículo expone que durante el último trimestre del año 2016 habían aumentado exponencialmente los ataques, pero que, a su vez, solo el 20% consiguió robar fondos de estas empresas. Sin embargo, desde entonces, hay muchos más incidentes, y cada vez más consiguen sustraer información

confidencial de la entidad, ocasionando pérdidas a la empresa e intercambiando datos y conocimientos técnicos a otras empresas o incluso a otros países.

De esta manera, los principales problemas para la empresa para la respuesta de los ciberataques se pueden resumir en que:

- Los ciberataques implican consecuencias a toda escala y en cualquier lugar del mundo.
- La amenaza se puede llevar a cabo desde cualquier parte del mundo; otorgando cierta ventaja a los atacantes.
- La ejecución del ataque no requiere ningún material especialmente técnico salvo la conexión a internet y un ordenador; por lo que cualquier persona podría hacerlo.
- Suponen graves repercusiones sociales y reputacionales, impulsadas por los medios de comunicación.
- Su apariencia es muy diversa, lo cual dificulta su detención. Y también es muy complicado hacer una estimación aproximada de las pérdidas reales ocasionadas por un ciberataque, ya que, existe un impacto subcutáneo muy subjetivo derivado de los daños colaterales, la recuperación y puesta en marcha de la actividad operativa, el coste reputacional, etc. (Urueña Centeno, 2015)

5. Protocolo empresarial ejemplar: El Caso MAPFRE 2020

Para esta parte analítica se ha entrevistado a Guillermo Llorente Ballesteros, actual director de seguridad del Grupo MAPFRE España. Para explicar el incidente del viernes 14 de agosto de 2020, Guillermo recalca la importancia de entender una serie de aspectos clave:

- Ninguna empresa es 100% segura

- Los grupos criminales llevan a cabo estos ataques con un objetivo principal claro: Obtener beneficio económico
- El entorno actual favorece a la expansión de la ciberdelincuencia debido a:

    1. La dependencia tecnológica de las empresas por la transformación digital, lo cual sitúa a las compañías en una posición más propensa a recibir amenazas y expone sus vulnerabilidades.

    2. Como hemos mencionado antes, se persigue la monetización de los ataques; y hoy en día se puede realizar rápida y fácilmente. Anteriormente, el objetivo de los ciberataques se centraba en las entidades financieras. Atacar a un banco era la opción más fácil de materializar y monetizar las recompensas. Esto se podía hacer cambiando las cuentas, extrayendo el dinero de los cajeros automáticos o haciendo transacciones a través de las tarjetas de crédito. Sin embargo, ahora existen grupos de ciberdelincuentes que persiguen finalidades alternativas, que se centran o bien en bloquear el funcionamiento de la actividad de negocio o bien buscan dañar la reputación de la entidad por medio del robo de datos confidenciales y extorsión a cambio de beneficio económico.

    3. La creación y evolución de las criptodivisas ha dificultado en gran medida la atribución del delito. A menudo la identidad del atacante permanece desconocida mucho tiempo debido a la capa de invisibilidad que proporciona operar bajo criptodivisas irrastreables.

4. Además, el carácter internacional de los ciberataques crea una barrera a la hora de identificar el origen del ataque. Pueden atacar a una empresa española desde Ucrania únicamente accediendo a una conexión a Internet.

En conclusión, el cibercrimen está evolucionando y creciendo a una escala muy alarmante, y la legislación española aún no cuenta con una guía normativa que prepare a las empresas a defenderse adecuadamente de estas amenazas. Por ello, muchas veces se ven solas en la gestión del incidente; y sin la ayuda activa del Estado, las empresas colapsan. La creación de un marco regulatorio implica mayores exigencias a las empresas, e indirectamente esto afecta al conjunto de pequeñas y medianas empresas que carecen de los recursos necesarios para proteger su negocio. Es por ello, que desgraciadamente muchas de ellas se ven obligadas a optar por el Silencio y el Pago de la extorsión. MAPFRE contaba con los medios para poder escoger una vía alternativa y consiguió dar ejemplo de cómo gestionar un ataque de este calibre.

5.1 Gestión reputacional del ataque

El viernes 14 de agosto MAPFRE sufrió el despliegue de un "ransomware" cifrando ficheros de miles de servidores y puestos Windows, y sus características son muy específicas:

- Es importante entender que este ataque estaba muy bien *preparado*. Los atacantes habían comprado los dominios un año antes de lanzar la amenaza.

De hecho, la fecha en la que sucedió el incidente estaba pensada estratégicamente para conseguir maximizar el daño a los servidores de la compañía. El 15 de agosto es el día de

más trabajo de todo el año para las empresas de prestación de servicios, y el grupo atacó la noche anterior. Esa madrugada es la que menos gente hay trabajando de todo el ejercicio económico, correspondía con un fin de semana, en un horario nocturno y en una situación de Pandemia Mundial. (Llorente, G., 2021) Todos los factores se acumulan creando el escenario perfecto para atacar ya que es el momento en el que la compañía era más vulnerable a una intrusión.

- Fue un ataque *profesional* para el que se emplearon herramientas de hacking de escalada de privilegios desconocidos anteriormente.

- Fue diseñado *específicamente* para MAPFRE. Los atacantes trataron de lanzar varios virus hasta finalmente lograr ser indetectables por los sistemas de seguridad de MAPFRE. Estos consiguieron bloquear hasta tres intentos; desgraciadamente el cuarto código pudo penetrar en el sistema.

Adicionalmente, el daño fue aumentado debido a que todos los empleados estaban trabajando en remoto a causa de la pandemia del Covid-19, y por tanto, todos los servidores de los ordenadores estaban encendidos. Los ciberdelincuentes lanzaron un ataque de *ransomware* y lograron entrar en la red de la compañía a partir de la captura de un usuario y una contraseña de acceso a MAPFRE, posiblemente empleada para acceder de forma remota al sistema de la organización desde un puesto particular infectado. La cronología del incidente se dividió en 5 fechas remarcables:

Madrugada del 15 de Julio: Los atacantes capturan las credenciales del usuario

1 de agosto: Ocurre el primer acceso a VDI con el usuario comprometido. Los ciberdelincuentes inician una fase de exploración en el que el TA (Threat Actor) aprovecha las credenciales robadas para conectarse a diversos equipos y servidores en busca de usuarios con mayores privilegios y así poder acceder a información crítica. Esta estrategia la llevaron a cabo desde 4 países diferentes.

---

7 de agosto: El TA se hace con las credenciales de un usuario administrador de puesto, y continúan la fase de exploración en busca de servidores con mayor potencial perjudicial para la compañía.

---

11 de agosto: El TA consigue obtener credenciales de mayor capacidad e inicia una fase de Análisis de la red de MAPFRE. Procedió a conectarse a servidores que contenían información crítica y carpetas de red; a partir de los cuales trató de extraer información desde varios puntos estratégicos, que fueron automáticamente bloqueados por elementos de seguridad.

---

14 de agosto: El TA finalmente distribuye el cifrador a los puestos y servidores, y lanza la orden de cifrado que consigue penetrar en el sistema. Accedió libremente durante las 2 horas siguientes a diversos equipos para verificar la eficacia de dicho cifrado, y acto seguido la compañía pudo activar la contención del ataque.

5.2 Responsabilidad empresarial y ocultamiento

Cuatro minutos tardó MAPFRE en detectar y poner en funcionamiento su protocolo de gestión de incidentes cibernéticos, empezando por tirar abajo todas las comunicaciones

del servidor. Esto creó un ambiente de incertidumbre porque supone el desconocimiento de lo que está sucediendo en el sistema. 18.000 puestos con 3.500 servidores fueron dañados de forma simultánea al estar conectados entre ellos por el teletrabajo. Sin embargo, la pandemia también obligó a las empresas a trabajar en un constante modelo de crisis, lo cual permitió a MAPFRE poner en marcha de forma automática la gestión del incidente en 5 pasos simultáneos: Contención, Restauración, Análisis Forense, Refuerzo y Comunicación.

El paso más decisivo de la cadena es el análisis forense; ya que con él pudieron identificar el origen del ataque y solventar la brecha en el sistema. El gabinete de seguridad no tardó en conocer que los atacantes no habían robado datos confidenciales; por lo que, o bien no estaba orquestado por un grupo profesional o bien su objetivo no era económico. Sin embargo, hasta que pasaron tres meses y confirmaron que no había fuga de datos, tuvieron que tomar la decisión de No Pagar, No comprar los descifradores que ofrecen los atacantes en la extorsión, y por lo tanto Comunicar al mundo lo que estaba sucediendo, arriesgando su reputación.

Guillermo Llorente destaca el hecho de que en esta situación se trata de una empresa que Sí podía permitirse declinar el pago de la extorsión. Históricamente MAPFRE ha hecho frente a las amenazas de grupos criminales, como cuando ETA incendiaba sus oficinas en el País Vasco. Además, contaban con una copia limpia de todos los datos almacenada en un servidor externo, y tenían fondos necesarios para enfrentar los procedimientos legales para la persecución del atacante. En cambio, una Pyme generalmente no goza de dichos recursos, por lo que el camino de No Pagar es incluso más perjudicial para la continuidad del negocio.

Una vez hecho el comunicado, MAPFRE puso en riesgo su reputación y se expuso a revisiones constantes de supervisores externos. Todo ello sumado al hecho de que todo el mundo conocía la noticia, lo cual supuso una gran oleada de preguntas por parte de los clientes e inversores, además de convertirse en el foco de ataque de miles de ciberataques, ya que habían mostrado públicamente que se encontraban en una posición de vulnerabilidad.

Esta situación pilló por sorpresa a la junta directiva, pero supieron llevar a cabo una Plan de Acción que actuó en paralelo a la rapidez del ataque. El viernes 14 de agosto a las 21:04 pm se ejecutó el malware en servidores y Pc Windows y a las 21:11 pm el Centro de Control dio la primera alerta; 20 minutos más tarde se activó el Plan de Contención y se aisló el DC de Alcalá. Acto seguido MAPFRE activa la cooperación con empresas externas encargadas de apoyar en la investigación del análisis forense. La madrugada del sábado se contactó con los socios del negocio y se lanzó la primera batería de medidas rápidas para reforzar la seguridad de la compañía. Ese mismo día notificaron el incidente al resto de la compañía y a las entidades regulatorias, y en el transcurso de los dos días posteriores se lanza una segunda batería de medidas y se inicia el análisis forense.

La rapidez del ataque muestra un "*Time to Market*" muy preciso, y, por tanto, la respuesta de la compañía debe corresponder dicha velocidad para sobrevivir. Guillermo asegura que una compañía que no es segura no es sostenible en el tiempo, y que la clave del éxito en la defensa de un ciberataque está en la rapidez de la toma de decisiones y la coordinación de la respuesta por parte de la compañía. Además, recalca que la nueva muralla de seguridad no seguirá siendo el Firewall, sino que se hace a través de la Identidad Digital (usuario y contraseña), y, por ende, se convertirá en el foco de ataque.

Por ello, insiste en la necesidad de establecer un plan de respuesta y de invertir en el refuerzo de la seguridad de la compañía.

1. Se deben realizar actuaciones preventivas para robustecer el entorno de seguridad y poder prevenir, detectar y ganar capacidad de respuesta en caso de un ataque, con el objetivo de reducir las posibilidades de éxito de los atacantes.

2. Actuaciones para minimizar la propagación de un ataque, que busquen minimizar la posibilidad de propagación de la amenaza de una entidad a otra. Esto puede realizarse restringiendo la conectividad, reforzando la segmentación, distribuyendo las pautas de actuación, etc.

3. Actuaciones para acelerar la recuperación, cuyo objetivo es capacitar a la empresa para reactivar la actividad del negocio lo antes posible en caso de un ataque exitoso, implementando medidas técnicas y operativas.

4. Estableciendo una comunicación directa y transparente con terceros. En este caso, MAPFRE realizó más de 250 comunicados a los reguladores, socios, mediadores y proveedores, grandes clientes, empleados, medios de comunicación y redes sociales.

5. Por último, Guillermo recomienda que toda empresa almacene una copia de los datos fuera del servidor central, que deriven una serie de fondos a la adquisición de un seguro de ciber riesgo para contar con apoyo financiero externo en caso de ataque, y acudir a servicios de consultoría periódicos para estar al tanto de las evoluciones y últimas novedades del sector. Un estudio realizado por MAPFRE

indica que aproximadamente el 60% de las empresas víctimas de un ciberataque desaparecen, mayoritariamente por su falta de formación o por haber escogido una estrategia de comunicación fallida.

Por ello, es vital fomentar la concienciación sobre este riesgo y en caso de que el ataque sea exitoso, mantener una comunicación activa con la red de clientes para darles la tranquilidad de que, si algo ocurre, van a saberlo al instante; así como ofrecer una compensación por la baja calidad del servicio durante el ataque (MAPFRE, por ejemplo, indemnizó a todos aquellos que la noche del incidente recibieron un servicio tardío). De esta manera, se conseguirá reducir todo lo posible el impacto reputacional derivado del ataque.

6. Desafíos futuros para la ciberseguridad

El Foro Económico Mundial, realizó un estudio con 524 organizaciones de 17 industrias diferentes en 17 países, cuyas principales localizaciones geográficas fueron Estados Unidos, América Latina, Europa, Asia y Oceanía, que indica que los riesgos tecnológicos más recurrentes son los ciberataques, los fallos críticos de los sistemas informáticos y los fraudes de datos. En concreto, este último acarreó unas pérdidas del 82% en 2019 (Castellanos, 2019); señal de que los ciberdelincuentes se han vuelto más ambiciosos con sus objetivos. Recientemente, la industria financiera se coloca en tercer lugar en mayores pérdidas, costes por filtraciones de datos, y número de ciberataques debido a la naturaleza de la información que almacenan. (IBM Security, 2020)

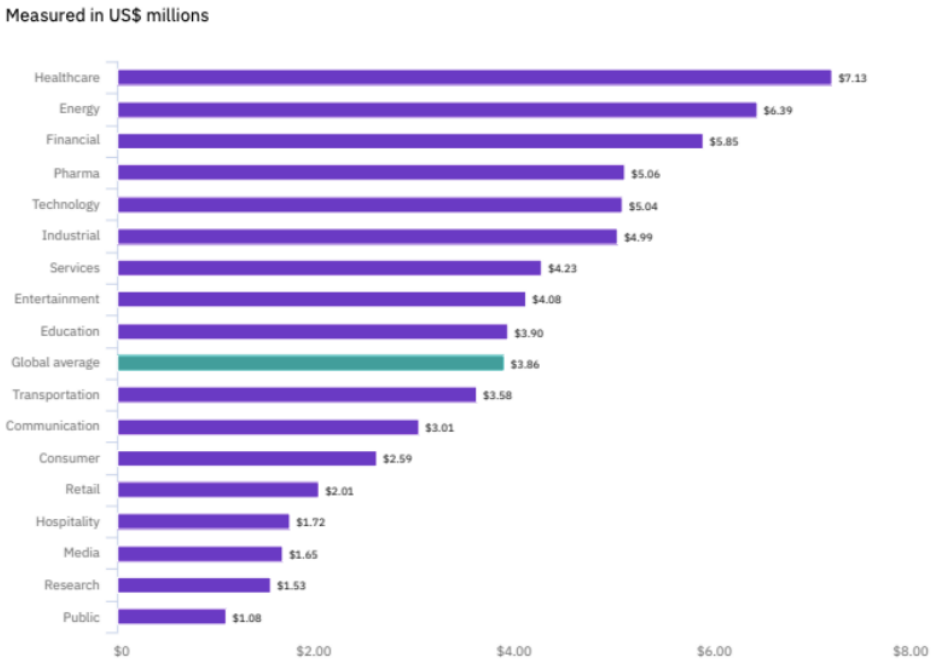

Figura 10: Coste total medio de filtraciones de datos por industria

Fuente: (IBM Security, 2020)

6.1 Aspecto Técnico

Actualmente, el riesgo cibernético ocupa el tercer lugar en las prioridades de las empresas, mientras que la ciberseguridad ocupa la duodécima posición (Deloitte, 2016). Claramente, existe un desajuste de prioridades que se debe resolver con urgencia. La presencia de un riesgo potencial debe implicar la activación automática del protocolo de defensa; y para ello las organizaciones deben derivar más fondos y recursos al desarrollo de los programas de ciberseguridad.

La evolución del ciber entorno ha llevado a cambios más dinámicos en el enfoque de las capacidades de la seguridad cibernética. Por tanto, se ha de garantizar la seguridad de las estrategias de protección. En primer lugar, hay que mejorar el sistema de controles de

riesgo para hacer frente a las amenazas conocidas y emergentes. En segundo lugar, las estrategias de ciberseguridad deben ser capaces de detectar amenazas y anomalías a través de un mejor conocimiento del panorama cibernético. A su vez, estas deben ser resistentes, habilitando la recuperación y puesta en marcha de la actividad habitual, y reparación rápida de los daños a la infraestructura operativa de la empresa. (IBM, 2020)

Para ello, será necesario aumentar la inversión en programas de ciberdefensa, aunque siempre contando con una buena planificación y priorizando la respuesta a los ciberdelitos más frecuentes. Estos programas se deben caracterizar por ser preventivos e inteligentes en materia de riesgos, y han de ser capaces de construir una defensa fuerte con diferentes capas de seguridad difíciles de penetrar. Los sistemas de ciberseguridad serán revisados y actualizados periódicamente para lograr garantizar las tres capacidades anteriores: ser seguros, vigilantes y resistentes. (Castellanos, 2019)

6.2 Aspecto Humano

El aumento de la inversión en herramientas y tecnologías para frenar el éxito de las amenazas es una parte fundamental; pero no siempre supone una mejoría en la ciberseguridad. Es importante considerar el factor humano y acompañar las prácticas técnicas con una exhaustiva formación de los empleados; porque la falta de concienciación y respuesta a las amenazas nos indica que incluso las tecnologías más preventivas, actuando por sí solas, son probablemente inadecuadas.

La Figura 11, representa el error humano como el tercer motivo por el que se producen filtraciones de datos en instituciones financieras (IBM, 2020). Por ello, los sistemas de

formación pueden marcar la diferencia; ya que pueden ser materializados en sistemas de capacitación que instruyan y doten a los empleados con las herramientas necesarias para saber detectar las ciber amenazas; como, por ejemplo, implementar un correo específico para consultas, impartir charlas formativas, desarrollar una guía de buenas prácticas, etc.

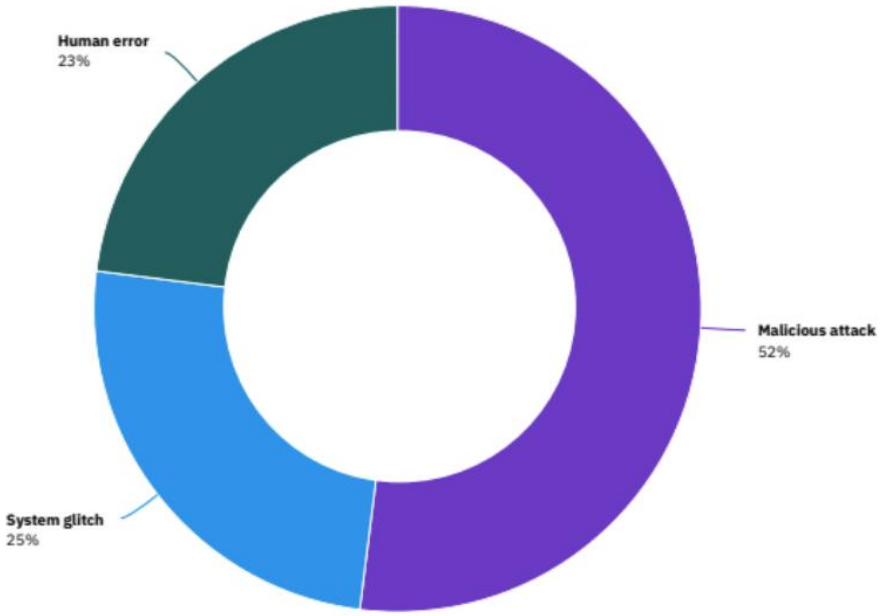

Figura 11: Principales causas de las filtraciones de datos

Fuente: (IBM Security, 2020)

6.3 Acción del CISO

El director de Seguridad de la Información (CISO) es el ejecutivo responsable de la seguridad de la información y datos de una empresa. Por tanto, es crucial que cuente con el conocimiento técnico necesario para adaptarse a los avances del panorama cibernético. Al igual que los sistemas, el CISO debe tomar las decisiones de forma segura, vigilar el entorno y ser resiliente al cambio. En la Figura 12 se observa que el 46% de los encuestados responsabilizan al CISO de los fallos de seguridad. Sin embargo, únicamente

el 26% de ellos le atribuye la responsabilidad de tomar las decisiones en materia tecnológica y política de la ciberseguridad de la empresa. Estos datos demuestran una incoherencia en los objetivos; ya que las responsabilidades del CISO deben corresponder al proceso de toma de decisiones, el cual corresponde en un 45% al CIO/ CTO, también conocido como el director de información y tecnología (IBM, 2020)

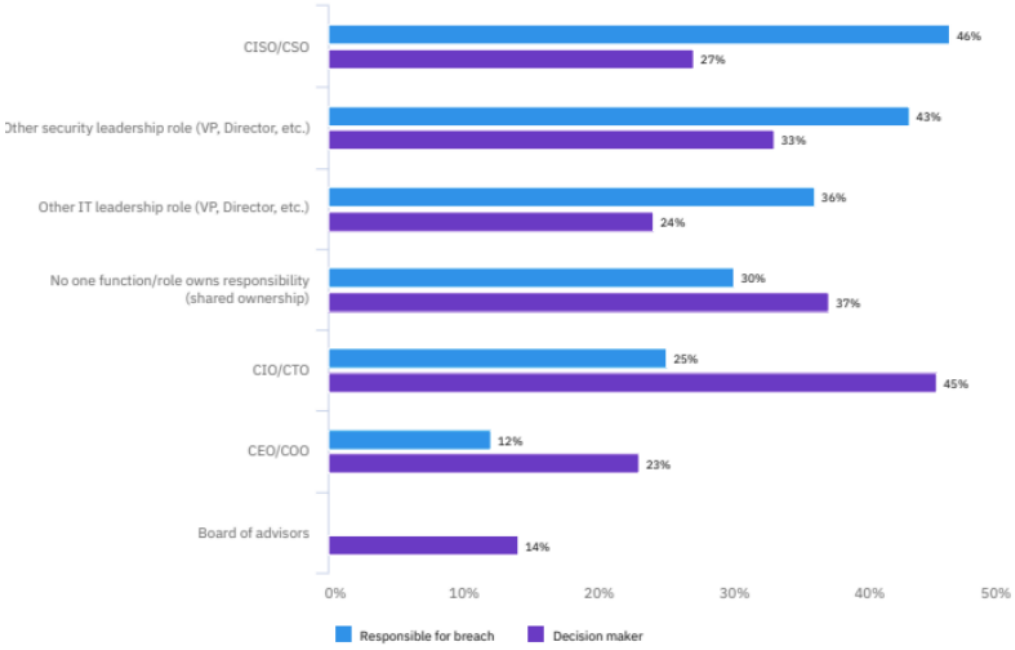

Figura 12: Responsables de las decisiones tecnológicas, las brechas y la política de ciberseguridad

Fuente: (IBM Security, 2020)

De esta manera, el CISO tendrá que hacer frente a varios desafíos de cara al futuro:

- Fomentar la colaboración entre los equipos de red y seguridad para intercambiar la información y mejorar los resultados fruto de las sinergias: Aunque implementar una metodología de trabajo en equipo será difícil con la creciente tendencia del teletrabajo. Por ello, el CISO deberá establecer una relación de confianza y cooperación con los proveedores de seguridad; ya que, la unión de

fuerzas será un aspecto clave para el éxito de los avances en ciberseguridad. (García W., 2021)

- Asociar la estrategia corporativa al protocolo de actuación para garantizar la protección de datos que establecen las nuevas regulaciones: La información confidencial será almacenada mediante *cloud computing.*

- Adaptarse a los nuevos avances tecnológicos como la Inteligencia Artificial y el aprendizaje automático, y aprovecharlos para crear nuevos métodos de detección y prevención de ciberataques. (Cisco, 2023)

- Aparte de sus funciones intrínsecas, el CISO deberá tener un perfil estratega capaz de dirigir la empresa y llevar a cabo la estrategia de ciberseguridad promoviendo a la vez que promueve un cambio transicional en la gestión del riesgo. Asimismo, tendrá que integrar funciones asesoras, influir en el proceso decisivo e impulsar la estrategia comercial. (CCN, 2020)

7. Conclusión

Este trabajo ha aportado consciencia sobre el concepto de ciberseguridad, tema que se ha convertido en tendencia debido al gran tráfico de ciberataques que reciben periódicamente las empresas. De hecho, mientras redactaba el trabajo, se llevaron a cabo múltiples ciberataques contra el Hospital Clínic de Barcelona, el Buró de Crédito en México e incluso a una red de telecomunicaciones del Poder Judicial. Esta noticia confirma la importancia de este tema y reafirma los motivos de su elección.

A lo largo del trabajo hemos podido observar que los daños en la cuenta de resultados de una empresa ocasionados por las pérdidas económicas derivadas de un ciberataque a veces no suponen un impacto tan significativo. Sino que, el daño realmente perjudicial tiene lugar en la confianza con la red de clientes e inversores. De esta manera, el riesgo reputacional lidera la pirámide de riesgos para las empresas en la gestión de la ciberdelincuencia. La finalidad de este trabajo ha sido marcar unas pautas que determinen cómo desarrollar una gestión exitosa del protocolo de defensa ante un ciberataque, así como concienciar a las empresas sobre la importancia de la formación del personal para un mejor futuro de la ciberseguridad.

Aunque las empresas cada vez son más conscientes de que se trata de un peligro latente, permanecen vulnerables debido a la sofisticación, rapidez y facilidad de los ciberdelincuentes para adaptarse a las nuevas tecnologías. Por eso, el trabajo ha dado luz a la vital relevancia implementar medidas de prevención para detectar las amenazas antes de que tengan lugar y poder garantizar la supervivencia del negocio. Se han indicado una serie de medidas adecuadas para proteger a la empresa del riesgo cibernético, al igual que un protocolo de actuación en el caso de que haya un incidente cibernético. Concretamente, para defender correctamente la entidad, se deberá conocer profundamente el modelo de negocio y el sector dónde operan, identificar los riesgos a los que están expuestos y estimar los impactos asociados a la posible materialización de esta amenaza.

Sin embargo, este análisis ha destapado ciertas brechas problemáticas para protegerse de un incidente cibernético. Algunas de ellas se corresponden con la insuficiencia de recursos (como suele ocurrir en las Pequeñas y Medianas Empresas), la falta de

información sobre el atacante o la rápida tendencia cambiante y evolución de las técnicas de ciberdelincuencia.

Es por ello, que la ciberseguridad se ha convertido en materia de seguridad nacional, y se han desarrollado varias guías normativas y leyes para intentar mitigar las amenazas latentes; como sería el caso de la ya implantada Ley de Protección de datos (GDPR) en toda la Unión Europea.

Para finalizar, todas las fuentes analizadas indican que actualmente no existe ningún método infalible para evitar un ataque, por lo que aún queda mucho camino por recorrer para conseguir que los ciberataques no signifiquen una amenaza real para el mundo empresarial. Pero mediante una estrecha cooperación entre las entidades reguladoras y las empresas, la evolución de la ciberseguridad, la concienciación y formación del personal, y el seguimiento de un protocolo de actuación adecuado, avanzaremos a pasos agigantados.

9. Bibliografía

Ahon, E. S. La reputación corporativa frente a las brechas de ciberseguridad. https://static1.squarespace.com/static/606344953ac19934572a88f5/t/6092c6b23cc2a90044a21ceb/1620231859907/DBA+IX+-+La+reputación+corporativa+frente+a+las+brechas+de+seguridad+de+la+información+-+EIriarte+vf.pdf

Cano, J. (2017). *Ciberseguridad empresarial*. Academia.edu. https://www.academia.edu/32619102/Ciberseguridad_empresarial?sm=b

Castellanos, W. A. (2019). Retos de gestión de riesgo cibernético en la Transformación Digital. [PowerPoint slides]. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Retos%20cyber%20ris k%2026-feb-2019.pdf

Centro Criptológico Nacional (CCN). (2020). Ciber amenazas y Tendencias. Edición 2020. https://cuadernosdeseguridad.com/wp-content/uploads/2020/10/Informe-Ciberamenazas-Tendencias-2020.pdf

Centro Criptológico Nacional (CCN). (marzo, 2008). Evolución del Código Dañino. Revista Auditoria y Seguridad 0.PDF (cni.es)

Cisco (2019). Defensa contra las amenazas más graves de la actualidad. https://www.cisco.com/c/dam/global/es_es/assets/pdfs/es_cybersecurityseries_thrt_01_0219_r2- 2.pdf

Cisco. What is cybersecurity? Recuperado el 5 de enero del 2023 en: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Eckenrode, J. & Friedman, S. (2018, 21 de mayo). The state of cybersecurity at financial institutions. There's no "one size fits all" approach. Deloitte Insights & Financial Services Information Sharing and Analysis Center (FS-ISAC). Deloitte-Risk-Cybersecurity-Financial-Institutions.pdf

European Central Bank. G7 Fundamental elements of cybersecurity for the financial sector.https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

FadilpaŠIć, S. (2022, 14 abril). *Cryptominers were the most common malware threat in 2021*. TechRadar. https://www.techradar.com/news/cryptominers-were-the-most-common-malware-threat-in-2021

Fernández, J. R. C. (2014). *La Ciberseguridad Nacional, un compromiso de todos*. Academia.edu. Retrieved November 10, 2022, from (PDF) La Ciberseguridad Nacional, un compromiso de todos | Jose Ramon Coz Fernandez - Academia.edu

Fundación Telefónica. (2016) Ciberseguridad, la protección de la información en un mundo digital. Editorial Ariel, S.A. https://publiadmin.fundaciontelefonica.com/index.php/publicaciones/verifica_captcha

Foro Económico Mundial. *Esa es la razón por la que debemos reforzar la ciberseguridad en esta era de policrisis*. (2023, 1 marzo). https://es.weforum.org/agenda/2023/03/ciberseguridad-en-la-era-de-la-policrisis/

García, P., Barragán, R. & Fuentes, NM (2018). Actas XV Reunión Española de Criptología y Seguridad de la Información, 96-101. Ciberdefensa empresarial: Un marco conceptual y práctico en un entorno digitalmente inestable (urosario.edu.co)

García Wirton, C. (2021). *Ciberseguridad en el Sector Financiero: ¿Cómo transformar una amenaza en una oportunidad?* [Universidad Pontificia Comillas]. https://file:///C:/Users/YA694XQ/OneDrive%20-%20EY/Desktop/TFG-Garcia%20Wirton,%20Carlota.pdf

Granados Franco, E., (2020). The Global Risks Report 2020. World Economic Forum in partnership with Marsh & McLennan and Zurich Insurance Group. [15th edition] https://www.marsh.com/ve/es/insights/research/global-risks-report-2020.htm

IBM Security. (2020). Cost of a Data Breach Report https://www.ibm.com/downloads/cas/RZAX14GX

Informe de Ciberpreparación de Hiscox 2022 | Hiscox España. (s. f.). Hiscox. https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2022

International Monetary Fund (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx

Instituto Nacional de Ciberseguridad (INCIBE). (2020). Glosario de términos de ciberseguridad. Una guía de aproximación para el ciudadano. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad _metad.pd

Jabbour, G. (2022, 7 diciembre). *Tendencias de ciberataques para 2023: hacktivismo, deep fakes y fraudes*. Expansión. https://expansion.mx/tecnologia/2022/12/07/tendencias-ciberataques-2023

Llorente, G. (2021). Ocho lecciones aprendidas de un ciberataque combatido por MAPFRE. *Actuarios*, (48), 50-52. Fundación MAPFRE. http://rightsstatements.org/vocab/InC/1.0/

Martín Rodríguez, G. (2018). La gestión de los riesgos tecnológicos (ICT).

http://hdl.handle.net/11531/33058

Martínez Landrov, N. (2019). *CIBERSEGURIDAD Y RIESGO OPERACIONAL EN LAS ORGANIZACIONES* [Icade Business School]. https://file:///C:/Users/YA694XQ/OneDrive%20-%20EY/Desktop/TFM001173.pdf

Montoya Moreno, G., Rincón Arteaga, J., Quijano Díaz, A., & Tocaría Díaz, D. (2019, 26 de marzo). Riesgo cibernético y el futuro de la estabilidad financiera. https://www.asobancaria.com/wp-content/uploads/semana-economica-edicion-1178.pdf

Mossburg, E. (2016). *Beneath the surface of a cyberattack: A deeper look at business impacts*. Deloitte. https://file:///C:/Users/YA694XQ/Downloads/Deloitte-ES-GRC-Los-riesgos-ocultos-de-un-ciberataque%20(1).pdf

New IDC Spending Guide Forecasts Worldwide Security Investments Will Grow 12.1% in 2023 to $219 Billion. (s. f.). IDC: The premier global market intelligence company. https://www.idc.com/getdoc.jsp?containerId=prUS50498423

Posada, J. M. (2019). *El entorno corre y los ciberriesgos vuelan*. Ciberriesgo: Un riesgo sistémico (Núm. 151) https://doi.org/10.29236/sistemas.n151a2

PriceWaterhouseCoopers (PwC). (2020). Fighting fraud: A never-ending battle. PwC's Global Economic Crime and Fraud Survey PwC's Global Economic Crime and Fraud Survey 2020

PwC Research, (2022). Global Digital Trust Insights: The C-suite guide to simplifying for cyber readiness, today and tomorrow. https://www.pwc.es/es/publicaciones/digital/global-digital-trust-2022.pdf

The Economist (November 2015). The cost of immaturity https://www.economist.com/business/2015/11/05/the-cost-of-immaturity

Urueña Centeno, Francisco Javier. 2015. Ciberataques, la mayor amenaza actual. Documento de Opinión nº 09/2015. Instituto Español de Estudios Estratégicos IEEE, http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf