FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

Ciberseguridad en el Sector Financiero

¿Cómo transformar una amenaza en una oportunidad?

Autor: Carlota García Wirton
Director: Raúl González Fabre

MADRID | Junio 2021

I. Resumen Ejecutivo y Palabras Clave

A través de este trabajo de fin de grado se desarrollan los aspectos clave de la ciberseguridad en el sector financiero en nuestros días, para poder entender cómo va a evolucionar en un futuro. Para ello se revisa el panorama cibernético actual explicando los tipos de ciberamenzas existentes, los agentes que las desarrollan y las tendencias que se han dado en los últimos años. Gracias a esta puesta en situación se comprenden los aspectos más relevantes de la ciberseguridad y las consecuencias que entraña en las empresas. Asimismo, se explican los mecanismos de ciberseguridad que llevan a cabo las empresas para contrarrestar los ataques.

El foco del trabajo gira en torno al análisis de la ciberseguridad en las instituciones financieras. Este estudio deja constancia de la importancia de la seguridad de los datos. Debido a la naturaleza de la información que tienen las instituciones financieras, como cuentas bancarias, son uno de los objetivos más codiciados de los ciberatacantes.

Por último y respondiendo al objetivo principal del trabajo, se establecen los retos y desafíos en materia de ciberseguridad para las instituciones financieras. Se detallan las mejoras que se han de hacer en cuando al aspecto técnico de la ciberseguridad y al aspecto humano, formando y desarrollan a los empleados para fortalecer la defensa de la organización. Asimismo, se pone en valor la importancia del rol del CISO (Director de Seguridad de la Información) y del equipo con el que trabaja.

La razón de ser de este trabajo es la de tratar de anticipar cómo evolucionará la ciberseguridad. ¿Evolucionará a la par que las ciberamenazas o podrá anticiparse a ellas?

Palabras Clave: Ciberseguridad, Ciberamenazas, Sector financiero, Ciberatacantes, Seguridad de la Información

II. Abstract and Key Words

This thesis develops the key aspects of cybersecurity in the financial sector nowadays, in order to understand how it will evolve in the future. To this end, the current cybernetic panorama is reviewed, explaining the types of existing cyber threats, the agents that develop them and the trends that have emerged in recent years. Thanks to this overview, the most relevant aspects of cybersecurity and the consequences it entails for companies are understood. It also explains the cybersecurity mechanisms that companies use to counter attacks.

The focus of this work is on the analysis of cybersecurity in financial institutions. This study highlights the importance of data security. Due to the nature of the information held by financial institutions, such as bank accounts, they are one of the most coveted targets for cyber attackers.

Finally, and in response to the main objective of this work, the cybersecurity challenges for financial institutions are set out. It details the improvements to be made in terms of the technical aspect of cybersecurity and the human aspect, training and developing employees to strengthen the organisation's defence. It also highlights the importance of the role of the CISO (Chief Information Security Officer) and the team he or she works with.

The man purpose of this work is to try to anticipate how cybersecurity will evolve: will it evolve along with cyberthreats or will it be able to anticipate them?

Keywords: Cybersecurity, Cyberthreats, Financial Sector, Cyberattackers, Information Security

III. Índice

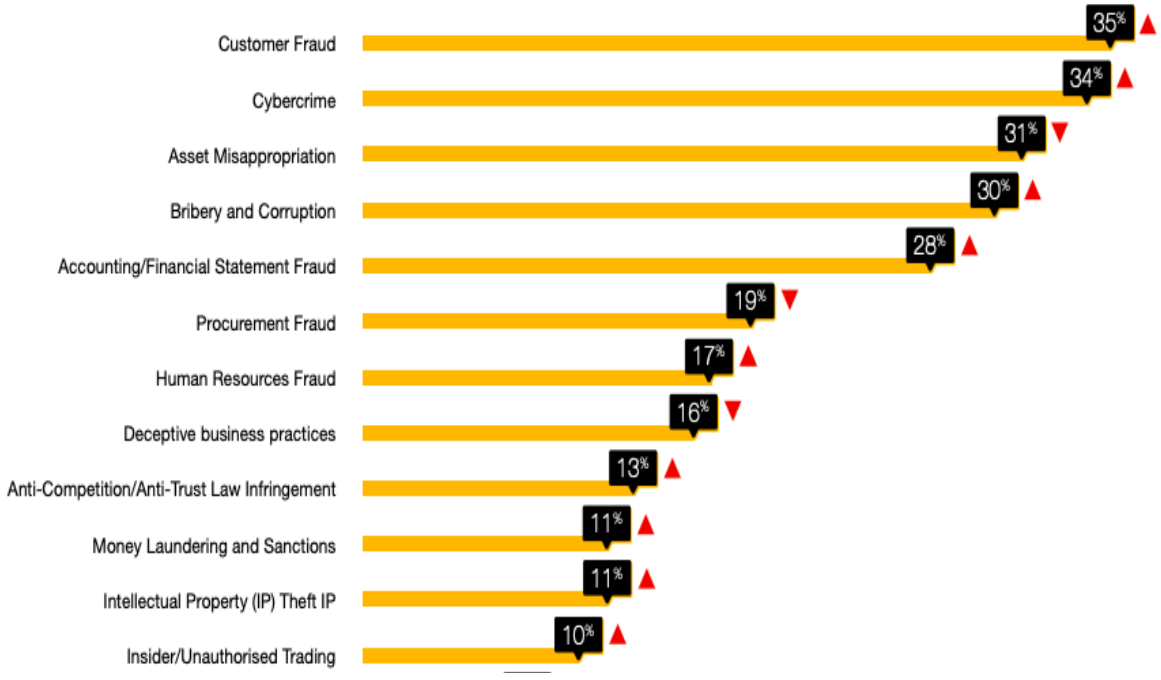
IV. Índice de Figuras

1. Introducción

Hoy en día, podemos decir que la gran mayoría de las empresas desarrollan su actividad económica con más efectividad gracias a las nuevas tecnologías. La tecnología es una herramienta fundamental para que las organizaciones sean más productivas, abarquen más mercados y dispongan de nuevos canales de comunicación con clientes y proveedores. Sin embargo, este nuevo entorno requiere que las empresas se adapten al nuevo medio de trabajo, dotando a sus sistemas de una seguridad de calidad, para que puedan evitar ataques.

Los fraudes económicos más recurrentes para los encuestados[1] son el fraude cometido por los clientes seguidos de los delitos cibernéticos, como vemos en la Figura 1 (PwC, 2020). "Según el Foro Económico Mundial, los ciberataques se perciben como el segundo mayor riesgo global para los líderes empresariales de las economías avanzadas, sólo superado por las crisis fiscales" (CISCO, 2020).

Figura 1. Frecuencia de los fraudes económicos



Fuente. (PwC, 2020)

[1] Estudio realizado con más de 5.000 respuestas de 99 zonas geográficas de EE. UU. y Europa principalmente (PwC, 2020).

El 60% de las organizaciones encuestadas[2] consideran la seguridad un tema de vital importancia, por ello, están incrementando su preparación frente a los ataques e implementado los controles (PwC, 2020). Mientras que en un estudio diferente llevado a cabo también por PwC (2018), los encuestados[3] estiman que los ciberdelitos van a ganar peso a lo largo de los años, tanto en número como en impacto. Esto es debido al auge de las nuevas tecnologías que capacita a los ciberdelincuentes a incrementar la complejidad de las amenazas.

1.1. Exposición de los objetivos

A lo largo de este trabajo se tratará de dar una visión global de la ciberseguridad para poder entender cómo va a evolucionar en los próximos años. Por ello, el objetivo principal consiste en concretar los retos y desafíos de cara a la ciberseguridad futura y, establecer las claves para que una empresa tenga éxito en la implantación de un sistema de ciberseguridad.

Para llegar al objetivo principal se detallarán los objetivos secundarios para entender todas las dimensiones de la ciberseguridad y las implicaciones que tiene en una empresa. Los objetivos secundarios son los siguientes:

- Sintetizar la visión 360 de la ciberseguridad en la empresa, categorizando los tipos de amenazas, los agentes y las consecuencias de los ciberataques.
- Detallar el mecanismo de la ciberseguridad en una empresa: prevención, detección y respuesta, entendiendo el rol del riesgo cibernético.
- Analizar el estado de la ciberseguridad en las instituciones financieras.
- Establecer las áreas de mejora de las instituciones financieras en materia de ciberseguridad.

[2] Estudio realizado con más de 5.000 respuestas de 99 zonas geográficas de EE. UU. y Europa principalmente (PwC, 2020).
[3] Encuesta realizada por 7.228 encuestados de 123 territorios repartidos por Europa, América, Asia y África. Del total de encuestados, el 52% son altos ejecutivos de sus respectivas organizaciones, el 42% representan a empresas que cotizan en bolsa empresas que cotizan en bolsa y el 55% representan a organizaciones con más de 1.000 empleados (PwC, 2018).

1.2. Explicación de la metodología

Este trabajo de investigación está sustentado sobre una metodología de revisión bibliográfica. El marco teórico está desarrollado en base a informes de consultoras y de instituciones financieras.

Una vez orientada la cuestión se van a analizar los problemas de la ciberseguridad en las instituciones financieras mediante informes y artículos de prensa. Este análisis pretende contrastar la información relevante sobre la ciberseguridad de las instituciones financieras en España y en el mundo.

Por último, se van a plantear una serie de retos y oportunidades aportando una visión completa de la ciberseguridad en el futuro.

1.3. Desarrollo y estructura

Con el fin de alcanzar el objetivo principal abordaremos la cuestión en diferentes apartados. Por un lado, en el capítulo dos, marco teórico, se van a explicar los tipos de ciberataques más comunes, se enunciarán los agentes que llevan a cabo los ciberataques, y se detallarán las consecuencias de los ataques cibernéticos y las tendencias que se han dado en 2020.

Por otro lado, en el capítulo tres se desarrolla el ciclo de la ciberseguridad, es decir los pasos que sigue una empresa a la hora de prevenir, detectar y responder a un ciberataque. Para ello se define el riesgo cibernético y sus implicaciones en la ciberseguridad.

En el cuarto capítulo se estudiará detenidamente cómo se gestiona la ciberseguridad en las instituciones financieras, mencionando sus características y determinando sus áreas de mejora.

En el capítulo cinco se planteará cómo va a evolucionar la ciberseguridad en los años venideros. Para ello, se sugerirán posibles retos para las instituciones financieras, y se expondrán diversas oportunidades frente a las amenazas crecientes a las que se enfrentan.

Finalmente, en el capítulo de conclusiones se dará respuesta a la cuestión planteada en un principio apoyándose en el análisis previo de la ciberseguridad en las instituciones financieras. La conclusión pretende establecer cuáles van a ser las claves de la ciberseguridad en el futuro. Mediante este trabajo de investigación se pretende aunar información para que las instituciones financieras y los responsables de seguridad tengan unas nociones en las que basarse para focalizar e implementar las nuevas medidas de seguridad.

2. Marco Teórico

2.1. Conceptos básicos de los ciberataques

2.1.1. Definición de conceptos e introducción en la materia

Según el Instituto Español de Estudios Estratégicos, "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). Asimismo, tenemos por extensión del término "criminalidad informática o cibercrimen que tiene mayor alcance, en él se incluyen delitos 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).

La culminación de estas prácticas sería el ciberterrorismo, "ataque premeditado y políticamente motivado contra la información, sistemas computacionales, 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 conjunto de ciberdelicuencia, cibercrimen y ciberterrorismo se denominan ciberataques. Los ciberataques se materializan cuando se detectan vulnerabilidades en las organizaciones, es decir "fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota" (INCIBE, 2020) . Estos fallos en el sistema pueden ser fruto de errores de diseño o de fallos de configuración entre otras muchas razones. Para evitar estas amenazas las organizaciones tienen que ser primero conscientes de las vulnerabilidades que sufren, y después saber cual es la probabilidad de que se vulnere su sistema de seguridad. Para prevenir estos ataques hay que establecer un sistema de análisis de riesgos y una vez detectados controlarlos.

2.1.2. Principales tipos de ciberataques

Los ciberataques responden a una definición muy amplia, cualquier acción ilegal llevada a cabo mediante la tecnología. Por ello, los ciberincidentes tienen diferentes características y grados de peligrosidad. A continuación, los clasificaremos según su finalidad y su procedimiento.

2.1.2.1. Finalidad de los ciberataques

Los objetivos principales a los que responden los ciberataques consisten en aprovechar las vulnerabilidades de los sistemas para robar información o cifrar contenido. En este apartado estudiaremos los principales propósitos por los que son llevados a cabo los ciberataques: robo o cifrado de información, destrucción de información o interrupción de la actividad empresarial entre otros.

2.1.2.1.1. Cifrar información mediante *Ransomware*

El *ransomware* es un *malware*, es decir un software malicioso. Su objetivo es cifrar el contenido del disco duro bloqueando nuestro dispositivo electrónico. Los ciberdelincuentes exploran el sistema en el que han penetrado para localizar los activos de mayor valor y que el *ransomware* se expanda ocasionando el máximo daño. Cuando el usuario ya ha perdido el control de su ordenador, el equipo reclama un rescate generalmente en pago de criptmonedas, como los *bitcoins*.

Este tipo de ciberataque se puede dar también en *smartphones* y *tablets*, además de en ordenadores. El *ransomware* se activa cuando se clica sobre el archivo que lleva oculto el virus. Generalmente el archivo infectado llega vía correo electrónico o mensajería instantánea como WhatsApp. El virus también puede infectar a través de páginas web de dudoso origen, como pornografía o descargas de contenido visual o musical.

2.1.2.1.2. Robo de información corporativa

La fuga de información es un incidente en el cual una persona externa a la organización tiene en su poder información confidencial de la organización. Las fugas de información pueden ser internas y externas, intencionadas y no intencionadas.

Por un lado, las fugas de información internas se dividen en intencionadas y no intencionadas. Las intencionadas se dan cuando un trabajador vende información a la competencia. Las fugas de información no intencionadas suceden cuando un empleado pierde un documento confidencial, un ordenador, un teléfono móvil o un pendrive en un lugar público.

Por otro lado, las fugas de información externas siempre son intencionadas y se producen cuando un agente externo a la organización acceda a una base de datos, o cuando un sistema infectado con un *spyware* roba la información sin que la organización sea consciente de ello.

Las consecuencias de una fuga de información pueden ser reparables si la fuga es inintencionada. Sin embargo, si la fuga es intencionada puede causar grandes daños a la reputación de la organización o del sector, también puede implicar una pérdida de confianza de los clientes, inversores o de un país. Finalmente, una fuga de información puede implicar pérdidas económicas en la organización.

2.1.2.1.3. Ataques Web

Los ataques web son una de las principales amenazas de 2019 y se dividen en dos grupos: los ataques de Denegación de Servicio Distribuidos (DDoS) y los ataques a servidores web. Su objetivo es localizar los ficheros para tomar el control del sistema y manipular o extraer datos. Los ataques de Denegación de Servicio pretenden bloquear un sistema o aplicación, hasta tal punto que los propios usuarios no pueden acceder a él, para que no pueda proveer el servicio para el que está destinado. Este tipo de ataques suele ser utilizado por los hacktivistas y su objetivo principal es damnificar la reputación de la víctima que incurre en pérdidas económicas o beneficiarse de la caída de los servidores (CCN, 2020).

2.1.2.2. Procedimientos de los ciberataques

2.1.2.2.1. Phising

El *phising* es un tipo de ciberataque bastante común. La víctima de *phising* recibe un correo electrónico con un enlace que le redirige a una página web dónde tiene que revisar sus datos personales. Habitualmente, el *phising* se hace pasar por una entidad de confianza para robar información confidencial como contraseñas, datos de la tarjeta de crédito entre otros.

El *phising* más frecuente es aquel en el que el atacante clona una página web para dar seguridad al visitante y que introduzca sus credenciales auténticas, que se envían al atacante. Sin darse cuenta, el visitante será redirigido a la página oficial. El 90% de los ciberataques son debidos al *phising* (Interreg, 2020).

Existen varios tipos de *phising*:

- El *Deceptive Phising* es el que se ha explicado previamente, quiere las credenciales para entrar en una página web con el usuario y contraseña robados.
- El *Malware-Based Phising* tiene como objetivo que el usuario se descargue un archivo o visite una página web donde se infectará del virus.
- El DNS-*Based Phising* o *Pharming* "consiste en modificar el host de una empresa o el sistema de nombres de dominio de la misma, para que las solicitudes de URL devuelvan una dirección falsa y las comunicaciones sean dirigidas a un sitio web falso" (Interreg, 2020). Este ciberataque se puede evitar si las contraseñas de los administradores de los routers se cambian una vez instalados.
- El *Content-Injection Phising* es aquel en el que se sustituye el contenido legítimo de una página oficial por contenido falso para engañar y guiar al usuario a desvelar su información confidencial.
- El *Search Engine Phising* tiene la capacidad de infectar a través de una búsqueda en Google o Bing, ya que los enlaces maliciosos están indexados en los motores de búsqueda. De esta manera los enlaces infectados se ofrecen en los resultados de una búsqueda normal y corriente.

- El *Main-In-The-Middle-Phising* es el más difícil de detectar porque el delincuente se cuela en el dispositivo de la víctima y del servidor, grabando la información que transmite.

2.1.2.2.2. Código dañino avanzado

Este procedimiento de ciberataque aprovecha las vulnerabilidades inherentes al sistema y habilita puertas traseras y brechas de seguridad para robar información y datos. Este tipo de amenazas suponen un nivel de sofisticación avanzado para los ciberdelincuentes que podría considerarse como un proceso I+D+i (CCN, 2020).

2.1.2.2.3. Botnets

Botnet viene de los términos ingleses "*robot*" y "*network*". Esta herramienta permite acceder a varios sistemas informáticos de diferentes víctimas a la vez, con el fin de robar datos confidenciales y lanzar ataques de denegación (DooS). Los botnets permiten sincronizar todos los dispositivos infectados en una red de "*bots*" que se puede gestionar de manera remota (CCN, 2020).

2.1.2.2.4. Ataques a sistemas de acceso remoto

Este ataque utiliza Internet para vulnerar los sistemas, controlarlos o hacerse con información sensible. Este método de ataque ha sido muy utilizado durante 2019 y 2020 para entrar en sistemas de acceso remoto a las redes corporativas. Algunos ejemplos de explotación de vulnerabilidad del sistema son VNP Pulse Secure o de Microsoft Exchange, este tipo de vulnerabilidades son conocidas como "vulnerabilidades del día 1" ya que todavía no existe una solución. La obtención de credenciales legítimas a los sistemas de la víctima, como VPN, sesiones de escritorio remoto o acceso vía web al correo constituyen otros mecanismos para la toma de control de sistemas de acceso remoto.

2.1.2.2.5. Ataque por Ingeniería social

La ingeniería social es la principal puerta de acceso a la información y consiste en engañar con técnicas psicológicas y habilidades sociales para conseguir información de terceros. Esta técnica utiliza el punto más débil de la cadena de seguridad: los seres humanos.

Hay diferentes técnicas de ingeniería social desde ofrecer algo concreto para que el usuario descargue un archivo malicioso hasta un correo fraudulento para que comparta información personal. También es habitual que los atacantes se hagan pasar por otras identidades con el fin de conseguir acceso a información privilegiada o el *scareware*, que consiste en hacer creer al usuario que su equipo está infectado con el fin de ofrecerle una solución que realmente infecta al ordenador.

La ingeniería social es clave para la realización de los ciberataques ya que da pie al resto de ataques descritos previamente: *ransomware*, *malware*, etc. Sin embargo, el acto de la ingeniería social termina cuando se ha conseguido la información que se buscaba, lo que se haga con lo información después pertenece a otra técnica de ciberdelincuencia. Mediante estos engaños basados en las debilidades de las personas se consigue penetrar en el sistema. Basta con una llamada a un empleado desprevenido para acceder al sistema.

Las APT, Amenazas Persistentes Avanzadas, son ataques sofisticados que van dirigidos a una empresa concreta. Para alcanzar sus objetivos de robar y filtrar información utilizan técnicas de ingeniería social. La peculiaridad de este tipo de ataques es que suele ser orquestado por la dirección de un país o grandes corporaciones por razones políticas en vez de financieras. Dado que los ataques se lanzan a entidades que tienen una ciberseguridad avanzada, normalmente el ataque requiere de ayuda interna. Esto no implica necesariamente que alguien de dentro colabore conscientemente, si no que se lanzan ataques para encontrar el eslabón débil que rompa la brecha de seguridad. Este tipo de ataques funcionan debido a la mala praxis de los usuarios que reutilizan sus contraseñas. El robo de información se suele llevar a cabo durante un largo periodo de tiempo, y el objetivo es conseguir acceso continuo al sistema. Los APT se denominan amenazas persistentes porque incluso habiendo

descubierto la amenaza y aunque parezca que ha desaparecido, puede que los hackers tengan algunas puertas traseras abiertas que les permita volver a acceder (CCN, 2020).

2.1.2.2.6. Ataques contra la cadena de suministros

El ataque de cadena de valor o de terceros supone una amenaza ascendente. Tiene diferentes formatos como el de herramientas de creación de *software* comprometido, código robado, entre otros. Este tipo de ataques es diferente ya que evade los controles de detección por comprometer directamente a los proveedores y a los clientes. Debido a que la regulación de riesgo de terceros todavía no está muy avanzada, las empresas todavía no son expertas en materia de ciberseguridad de terceros. Un ejemplo común de ataques contra la cadena de suministro es el de secuestro de actualizaciones de software (CCN, 2020).

2.2. Ciberataques contra las empresas

Los investigadores afirman que los delitos derivados de los ciberataques irán en aumento tanto en número como en impacto en los próximos años. Este incremento se debe en parte al auge de las nuevas tecnologías, que han aumentado la sofisticación y la complejidad de los ataques, que permiten a los ciberdelincuentes fijar objetivos más estratégicos. De hecho, más de un tercio de las empresas encuestadas[4] han sido objetivos de ciberataques. En un periodo de 24 meses las empresas encuestadas han sufrido un 36% de ataques de *malware* y un 33% de *phising* (PwC, 2018).

Los tipos de fraude más recurrentes en España como consecuencia de los ciberataques según las empresas encuestadas son en un 30% las disrupciones en los procesos empresariales, en

[4] Encuesta realizada por 7.228 encuestados de 123 territorios repartidos por Europa, América, Asia y África. Del total de encuestados, el 52% eran altos ejecutivos de sus respectivas organizaciones, de los cuales el 42% representaba a empresas que cotizan en bolsa empresas que cotizan en bolsa y el 55% representaba a organizaciones con más de 1.000 empleados (PwC, 2018).

un 24% la apropiación indebida, en un 21% la extorsión y en un 12% el robo de la propiedad intelectual principalmente (PwC, 2018).

Después de un análisis del sector, se concluye que "el 44% de las industrias no tienen antivirus, el 47% no realiza copias de seguridad y un 49% no dispone de una adecuada gestión de incidentes" (CCN, 2020). Estos datos confirman que las ciberamenazas son reales, pero que las empresas no siempre están tan preparadas en materia de ciberseguridad como deberían. A continuación, se estudiará la razón por la que se dan los ciberataques, quiénes los realizan y qué consecuencias tienen en las empresas.

2.2.1. Objetivo de los ciberataques: El valor de la información

La información con la que se trabaja forma parte del valor real de cada negocio, y por ende uno de los principales objetivos de los ciberataques. Es clave saber cuales son las fuentes de información y de donde provienen los activos con los que trabajan las organizaciones. La pérdida de la información, mediante un ataque *ransomware*, es grave para la supervivencia de una empresa, ya que, sin ella, la empresa no puede seguir con su actividad empresarial.

El mundo empresarial funciona con tecnologías diseñadas para compartir información, no 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. Los ataques dirigidos tienen como objetivo dañar la infraestructura de la compañía mediante actos de espionaje o robo de información para hacerla pública lo que perjudica la imagen de la compañía. Asimismo, los ataques orquestados por personas para romper la seguridad de una organización mediante un APT suelen estar relacionados con motivos políticos.

La información se define como datos que tienen un significado concreto y de los cuales se pueden extraer conclusiones. Las empresas contienen y generar una gran cantidad de información, como datos relacionados con el funcionamiento del negocio, por ejemplo, datos de ventas o de contabilidad. No obstante, la empresa también necesita recopilar información sobre sus clientes o el entorno que les rodea entre otros. Para almacenar y recoger esta

información, las organizaciones recurren a sistemas de información, como *software* que de manera automatizada captan, procesan y transmiten la información para mejorar la toma de decisiones.

Hay que tener en cuenta que no todo lo que se comparte en los medios digitales se hace de forma consciente. En muchas ocasiones es imposible evitar compartir información cuando se establece conexión a internet. A continuación, veremos tres circunstancias en las que se comparte información.

En primer lugar, la información que se comparte por defecto es aquella que emana de la mera interacción con distintos dispositivos y plataformas, como realizar búsquedas. Esta información generada se queda registrada, deja "trazas" y no desaparece al terminar la sesión.

En segundo lugar, la información que se comparte de forma forzada es aquella que es necesario introducir en la web para que acceder a ciertos beneficios de internet, como por ejemplo transacciones, compras o acceso a determinados servicios. Este tipo de prácticas suele ser firmar en plataformas o compartir datos privados. Esta información se queda en la página web ya que no siempre se es consciente de los términos de privacidad de datos.

Por último, la información que se comparte de forma voluntaria es aquella que genera la organización como muestra de expresión de información u opiniones, como puede ser en redes sociales o en la página oficial de la empresa. Esta información queda expuesta en Internet para cualquier usuario, ya que el fin de esta es que otros la vean.

Asimismo, es importante diferenciar entre la seguridad informática y la seguridad de la información. Por un lado, la seguridad informática es aquella vela por que la infraestructura tecnológica funcione correctamente para que el negocio pueda desarrollarse. Por otro lado, la seguridad de la información se refiere al activo que realmente tiene valor, los datos y la información de la organización. Aunque también es importante tener en cuenta el ciclo de la vida de la información, es decir que lo que hoy nos puede parecer de vital importancia, en un futuro puede dejar de tenerla.

2.2.2. Tendencias de los ciberataques en 2020

La pandemia de la COVID-19 y las medidas adoptadas del confinamiento afectaron a la situación laboral y la continuidad de los negocios. Desde que se decretó súbitamente el Estado de Alarma en España, en marzo 2020, se puso en marcha de manera precipitada el teletrabajo. No obstante, la rapidez con la que se tuvo que instalar el mecanismo del teletrabajo supuso que no se evaluaran correctamente los riesgos asociados a la ciberseguridad, los protocolos de actuación en caso de ciberataque.

Las nuevas herramientas de teletrabajo como las videoconferencias, las soluciones en la nube, servicios y tecnologías de acceso remoto, herramientas colaborativas… han supuesto una oportunidad para los ataques en entornos digitales. Los ataques a redes domésticas o dispositivos personales aumentaron en número y en complejidad ya que estos objetivos son los más vulnerables. La necesidad de trabajar en remoto ha generado riesgos para los técnicos de mantenimiento y las empresas encargadas de la ciberseguridad que han de adecuar los procesos de seguridad.

También ha sido importante durante esta crisis el rol de la tecnología para facilitar el seguimiento de personas infectadas con el virus. Ha habido varios intentos de un modelo de aplicación similar en Europa, sin embargo, no se ha conseguido la coordinación de todos los países europeos en materia de conceder libre acceso a los datos como los terminales móviles, el *bluetooth*, la criptografía, etc.

Los ciberataques también se han visto influidos fuertemente por la pandemia en sectores como el farmacéutico. Debido al desarrollo de una vacuna por los laboratorios, aumentaron los riesgos de un ataque, de ciberespionaje, de destrucción de información o de operaciones de influencia sobre la opinión pública.

Las tendencias observadas en 2020 han indicado un aumento en la cantidad de ataques recibidos teniendo en cuenta que el número de dispositivos conectados a Internet aumenta año tras año. La situación empeoró ya que las organizaciones no estaban preparadas para

gestionar la diversidad de dispositivos con distintos propósitos y necesidades de conectividad.

Las tendencias de 2020 se vieron acentuadas con la crisis sanitaria, como es el caso de los ataques *ransomware* a los hospitales o servicios sanitarios. También se detectaron ataques contra compañías y laboratorios que estaban desarrollando la vacuna contra el coronavirus. Este tipo de ataques pretenden afectar sistemas de información como los historiales médicos, y pueden llegar a atacar los sistemas de generación de energía de emergencias, los equipos por diagnóstico por imagen o tratamiento.

La tendencia a la sofisticación de los ataques *ransomware* con un medio de acción parecido al APT aumentaron, en ellos se compromete a la víctima mediante vulnerabilidades, y una vez controlada la infraestructura se puede filtrar información. Este prototipo de ataque se utiliza para cifrar la información y pedir un rescate, amenazando con publicar la información sensible.

En el ámbito de la inteligencia artificial, las tecnologías *Deep Fake* lanzaron ataques de *phishing* más complejos, que llegaban a imitar la voz de un directivo o su manera de redactar, para hacer más realistas los cebos. La inteligencia artificial se posiciona como una de las tecnologías con mayor proyección para la ciberseguridad y los ciberataques en los próximos años.

Por su lado, las organizaciones también han desarrollado nuevas herramientas originadas de la inteligencia artificial. En ellas se monitoriza el comportamiento de los empleados y se detectan desviaciones de reacciones anómalas. También existen herramientas que dan una repuesta en tiempo real como el *Adaptive Cybersecurity.*

Sin embargo, la inteligencia artificial sigue en periodo de desarrollo y está lejos de sustituir a los expertos técnicos. Esta tecnología será clave para la ciberseguridad en el futuro, tanto organizaciones como ciberatacantes trabajarán para dominarla y beneficiarse de ella (CCN, 2020).

2.2.3. Agentes de las ciberamenazas

A continuación, se van a detallar los agentes que llevan a cabo los ciberataques contra las empresas. Se va a explicitar los motivos que los mueven y las herramientas de las que disponen para operar.

2.2.3.1. El Estado

Los Estados y grupos patrocinados por Estados exploran las vulnerabilidades de los sistemas de información de las estructuras críticas lanzando código dañino. Sus acciones se dividen en tres ámbitos: la ciberguerra, el ciberespionaje y las operaciones de influencia. En este apartado nos centraremos en el ciberespionaje ya que es la amenaza que lanzan los Estados a las empresas.

El ciberespionaje es una técnica utilizada por los Estados para recopilar información bajo falsas pretensiones con la intención de utilizarla en perjuicio de la organización espiada, o en beneficio propio. Requiere muchos recursos económicos y un personal muy especializado, con el fin de permanecer ocultos y obtener la mayor información posible. Hoy en día, el ciberespionaje representa una gran amenaza que va en aumento debido al auge de las nuevas tecnologías. Además, el ciberespacio, en el que se realizan estas operaciones de obtención de información, es un terreno clave ya que supone bajo riesgo para el actor hostil y un enorme potencial beneficio para el atacante (CCN, 2020).

2.2.3.2. La Ciberdelincuencia

En segundo lugar, tenemos a los ciberdelincuentes que representan el grupo de mayor actividad. Su objetivo es atacar organizaciones con el fin de robar y manipular información, e interrumpir y manipular servicios. Generalmente llevan a cabo estos objetivos mediante correos electrónicos o *phising* aunque estas técnicas van mejorando debido a la ingeniería social. La ciberdelincuencia tiene una naturaleza sin fronteras, y por ello resulta muy complicado para los organismos legales impartir justicia a estos delitos transnacionales.

Un caso representativo de los ciberdelincuentes es el fraude del CEO. Se trata de una maniobra que consiste en hacerse pasar por el CEO de la empresa y solicitar transferencias al empleado. A pesar del nombre, los ciberdelicuentes se marcan objetivos menores que el CEO en la jerarquía de las organizaciones. Este tipo de ataques ha aumentado en un 100% desde 2018 a 2019, según el FBI (CCN, 2020). Esta amenaza es un asunto de ingeniería social meramente, que entra a través del correo electrónico y los mensajes de texto principalmente.

2.2.3.3. El Hacktivismo

En tercer lugar, los hacktivistas se dedican a destruir páginas webs, realizan ataques de denegación de servicio y divulgación de información crítica para perjudicar a la empresa. Su objetivo es interrumpir los servicios, robar o manipular información con el fin de reivindicar sus ideas llamando la atención, a diferencia de otros no buscan un beneficio lucrativo. En España, no se ha detectado una estructura hacktivista que cuente con los recursos para coordinar y ejecutar ciberataques.

2.2.3.4. Los Actores internos

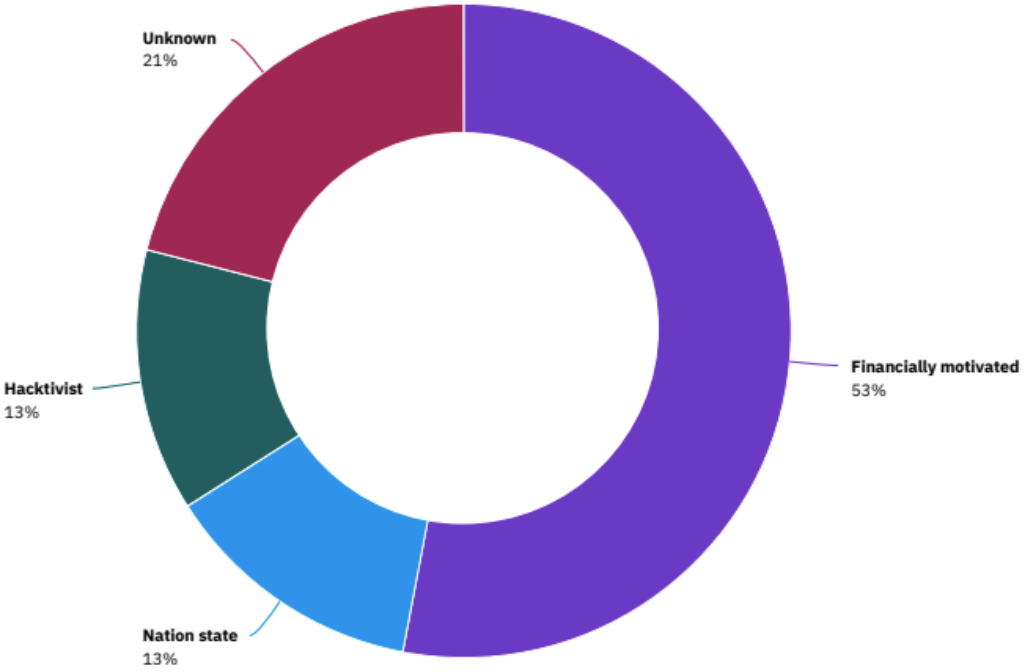
Por último, tenemos los actores internos que están constituidos por personal interno de la organización. Son agentes que actúan intencionada o inintencionadamente. Los actores internos que actúan de manera premeditada tienen como objetivo principal el beneficio económico. Este tipo de agente se puede asemejar a los ciberdelincuentes pero con acceso interno y con motivaciones diferentes, ya sean ideológicas, o de venganza por mal trato recibido por parte de la empresa.

El segundo subgrupo son los actores internos que abren una brecha en el sistema informático de la empresa por negligencia. Esto supone una gran preocupación para los encargados de seguridad de las empresas. La gran mayoría de estos incidentes se dan debido a un error o negligencia por falta de concienciación y formación de los empleados.

Estos incidentes son determinantes para las entidades ya que suponen un coste reputacional importante debido a la filtración de datos confidenciales. Asimismo, el coste económico ya sea de manera directa, como fraude, o de manera indirecta, como robo de la propiedad intelectual son amenazas serias para las organizaciones.

A modo de conclusión, vemos en la Figura 2[5] que más de la mitad de los atacantes han sido motivados por una causa económica. Los Estados estuvieron implicados en 13% de las filtraciones de datos, al igual que los hacktivistas, quedando un 21% restante cuya motivación es desconocida (IBM Security, 2020).

Figura 2. Filtraciones de datos organizadas según el agente atacante



Fuente. (IBM Security, 2020)

[5] Estudio realizado a partir de una muestra de 524 organizaciones de 17 industrias y 17 países, cuyas principales áreas geográficas son EE. UU., América Latina, Europa, Asia y Oceanía (IBM Security, 2020).

2.2.4. Consecuencias de los ciberataques para las empresas

Los ciberataques suponen un riesgo para las organizaciones ya que se ve vulnerada su barrera de ciberseguridad. Estos ataques suelen entrañar costes económicos y reputacionales. Para mantener un control sobre estas amenazas y poder prevenirlas, las organizaciones miden el impacto de los ataques.

El riesgo cibernético representa la posibilidad de pérdida tanto financiera como no financiera provocada por ciberataques internos o externos a la organización. El robo y el daño de información esencial de la organización suponen eventos clave ya que pueden llegar a parar la actividad de la empresa.

Los eventos que pueden suceder en una organización se evalúan en función de la frecuencia y la severidad. La frecuencia es la cantidad de veces que se produce un evento y la severidad es la pérdida cualitativa del suceso. Por lo general, las organizaciones tienen eventos de mucha frecuencia y poca severidad. Ambas variables frecuencia y severidad se suelen relacionar inversamente, por ello las organizaciones deben centrarse en los sucesos que ocurren con poca frecuencia pero que entrañan una gran pérdida.

Las pérdidas para las empresas víctimas de ciberdelitos económicos son diversas. Por un lado, están los costes económicos directos. "En España el 66% de las empresas encuestadas[6] asegura haber tenido pérdidas por encima de los 100.000€ como consecuencia del delito más grave experimentado en los últimos dos años" (PwC, 2018). Por ejemplo, si una empresa recibe un ataque de denegación de servicio, su servicio online se bloqueará y por ende incurrirá en pérdidas de ventas, lo que supondrá una reducción de los ingresos.

El impacto económico de un ciberataque conlleva distintos aspectos a evaluar como la respuesta que tendrá que dar la empresa sobre el incidente en cuanto a costes de servicios de

[6] Encuesta realizada por 7.228 encuestados de 123 territorios repartidos por Europa, América, Asia y África. Del total de encuestados, el 52% eran altos ejecutivos de sus respectivas organizaciones, el 42% representaba a empresas que cotizan en bolsa empresas que cotizan en bolsa y el 55% representaba a organizaciones con más de 1.000 empleados (PwC, 2018).

asesoramiento y gestión de las comunicaciones de cara a los grupos de interés. La empresa también deberá tener en cuenta los costes productivos por la interrupción del servicio, la pérdida o reposición de activos… El cumplimiento de las obligaciones como las sanciones o el rating de crédito y el coste de financiación también se incluyen en los costes económicos. Por último, un ciberataque siempre implicará un coste en el refuerzo de la seguridad como la incorporación de nuevas medidas de seguridad, verificaciones o reparaciones de brechas (Deloitte, 2017).

Por otro lado, están los costes indirectos están compuesto por los gastos adicionales en los que debe incurrir la empresa como el gasto en abogados, investigaciones internas y externas entre otros. Por último, otra de las pérdidas que sufren las empresas son los daños intangibles como la reputación o la percepción de los grupos de interés de la empresa, como los empleados, los clientes, los inversores entre otros. En el caso de que una empresa sea víctima de un incidente informático, éste afectará a la reputación corporativa que entrañará una pérdida de confianza de los mercados y por ello una reducción de las expectativas y de la confianza de los accionistas (Deloitte Advisory, SL. , 2013).

3. El ciclo de vida de la ciberseguridad en las grandes empresas

La ciberseguridad es un proceso mediante el cual se trata de prevenir ciberataques antes de que sucedan y paliar los efectos de aquellos que ya se han dado. La ciberseguridad se divide en tres etapas: prevención, detección y reacción. Es importante que este proceso esté acompañado de un aprendizaje para situaciones futuras. Debido al carácter global de los sistemas de una organización es esencial dotar a los sistemas de ciberseguridad de inteligencia que facilite el aprendizaje y que permita la integración de información de diferente naturaleza. Por ello, es vital que los datos se compartan y estén interconectados. En primer lugar, abordaremos el riesgo que entrañan los ciberataques, para comprender cómo prevenirlos, detectarlos y resolverlos.

3.1. Riesgo Cibernético

El riesgo cibernético responde a toda pérdida financiera o interrupción de la actividad operativa resultado de un daño provocado en los sistemas informáticos debido a la intrusión de medios electrónicos no autorizados, con el objetivo de usar, interrumpir, modificar o destruir los sistemas. Abordaremos el riesgo cibernético desde la perspectiva de las entidades financieras ya que suelen contar con gran cantidad información confidencial, lo que les vuelve un objetivo atractivo para los ataques cibernéticos.

Según el Foro Económico Mundial, los riesgos cibernéticos, como el robo de datos o los ciberataques, representan un riesgo importante en la escala de riesgos globales después de los desastres naturales, como se aprecia en la Figura 3 Montoya Moreno et al. (2019). Los riesgos cibernéticos están relacionados con los riesgos financieros, ya que los ciberataques tienen como objetivo destruir o comprometer de manera premeditada el funcionamiento del mercado, lo que genera inestabilidad financiera.

Figura 3. Evolución de los riesgos globales en términos de probabilidad

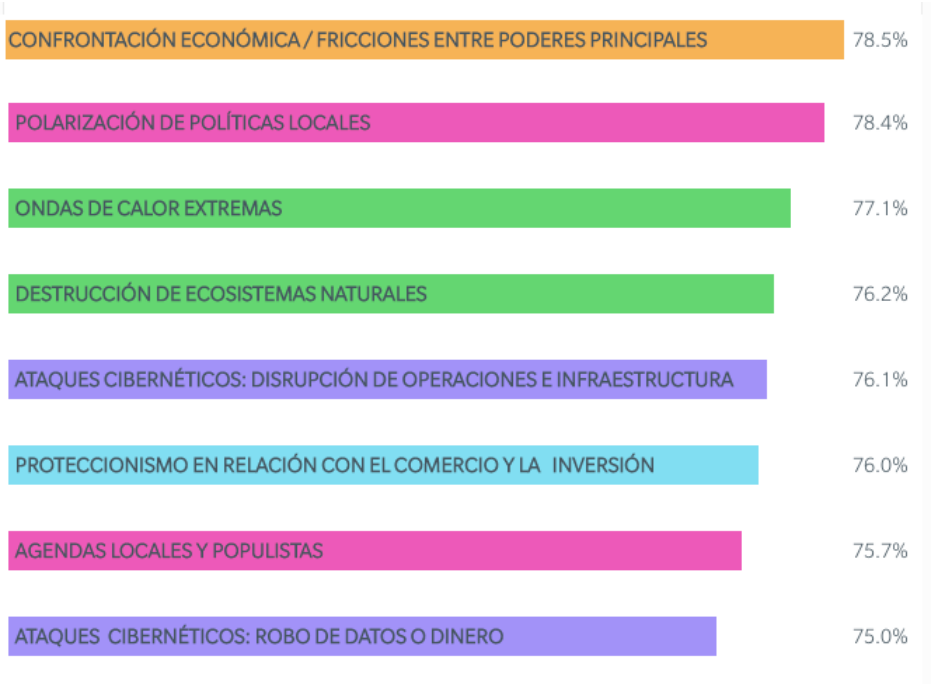
Fuente. (Montoya Moreno et al., 2019)

Según un estudio del Fondo Monetario Internacional, los ciberataques pueden llegar a comprometer desde el 9% hasta el 62% de los ingresos netos de las entidades (Montoya Moreno et al., 2019). Los canales por los que los riesgos pueden ser transmitidos son diversos. El hecho de que el sistema financiero esté interconectado obstaculiza la resolución de problemas y hace que el miedo de un choque financiero se expanda con mayor rapidez y cunda el pánico. Además, los ataques cibernéticos generan una pérdida de confianza y de reputación importante para las entidades financieras.

Las diferencias clave entre los ataques cibernéticos y los choques financieros que pueden crear inestabilidad sistémica son tres. La planeación de los ataques es el primer punto diferencial, ya que los ataques cibernéticos están planeados con mucho tiempo de antelación, mientras que las crisis financieras no están programadas. La complejidad también diferencia los riesgos cibernéticos de los financieros, ya que los primeros forman parte de un sistema altamente complejo, mientras que los segundos son estudiados por especialistas mediante modelos. La intencionalidad de estos ataques es el último punto diferencial. Mientras que las crisis financieras surgen de fallos del mercado, los ciberataques son intencionados y con fines maliciosos que suelen derivar en inestabilidad financiera (Montoya Moreno et al., 2019).

Los ciberataques que pueden afectar en mayor impacto a la estabilidad económica son los ataques a sistemas de pago ya que puede irrumpir la prestación de servicios esenciales durante largos periodos de tiempo, los robos a gran escala de datos, especialmente aquellos dirigidos a Depósitos Centrales de Valores, y ataques a consumidores minoristas y la sociedad en general. Como vemos en la Figura 4 (Granados Franco, 2020), los riesgos tecnológicos se sitúan en la quinta y octava posición en cuanto a importancia en 2020 con respecto al resto de riesgos.

Figura 4. Principales riesgos que se espera que aumenten en 2020



Fuente. (Granados Franco, 2020)

3.2. Prevención

Para prevenir los ciberataques es fundamental estar informado sobre la evolución de las amenazas y de las soluciones que existen. Uno de los pilares clave para la prevención es la formación constante acompañada de un amplio conocimiento sobre la ciberseguridad, el funcionamiento de las herramientas y de los productos de seguridad. Asimismo, es esencial garantizar la protección física de las instalaciones para evitar el acceso de personal no

autorizado y posibles manipulaciones. La prevención se compone de diferentes procesos críticos que se estudiarán a continuación.

Para afrontar las ciberamenazas, las empresas cuentan con un conjunto de medidas que se dividen en medidas técnicas, organizativas y legales. Entre las medidas técnicas se encuentran soluciones *antimalware* y antifraude, protección de las comunicaciones, control de tráfico de datos, inteligencia de seguridad entre otros. "Las copias de seguridad son la salvaguarda básica para proteger la información de la empresa" (INCIBE, 2017). Para garantizar la integridad y confidencialidad de la información de la empresa también se puede cifrar la información o invertir en protección *malware*.

La seguridad de red está compuesta por aquellas acciones diseñadas para proteger una red de sistemas u ordenadores y recursos de red. El objetivo principal es proteger la fiabilidad e integridad de las redes y de los datos. Las organizaciones consiguen esto mediante un sistema de seguridad compuesto por varias capas, por si falla una, las demás estén operativas para actuar y detengan el elemento atacante. Para ello es fundamental desarrollar medidas de seguridad de *hardware* y *software*. La política de seguridad de red debe incluir tres pilares esenciales: la definición de una política de seguridad clara, su implementación y su continua auditoría (Fundación Telefónica, 2016). La arquitectura de seguridad de la información es un esquema de acción estratégico mediante el que se definen directrices a nivel de seguridad en cada uno de los procesos 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). Difundir una política de seguridad que identifique los pasos a seguir en caso de ciberataque indica que la organización está preparada y comprometida con la seguridad de la empresa. Asimismo, la existencia de normativas y procedimientos que desarrollen las obligaciones y las directrices a las que están sujetos los empleados es síntoma de un buen plan normativo de ciberseguridad.

La gestión de identidades forma parte de los aspectos organizativos a tener en cuenta. Consiste en asignar a una persona concreta unas credenciales o una serie de permisos para acceder a unos determinados sistemas y recursos. Prácticamente todas las empresas tienen unas zonas donde almacenan una serie de información confidencial. Por consiguiente, es interesante desarrollar políticas de control sobre los accesos a activos críticos para minimizar los riesgos. Estos procesos se llevan a cabo mediante las herramientas de control de accesos.

Para llevar a cabo los controles de identidades hay que establecer unos criterios de acceso basados en permitir el acceso a ciertas zonas a determinadas personas exclusivamente cuando sea necesario para el desarrollo de la tarea. Uno de los problemas de estos métodos es que los procedimientos manuales no son del todo eficientes. Por ende, establecen ciertos retos para las organizaciones. Es importante que las organizaciones tengan un sistema de previsión organizado para evitar problemas en materia de seguridad, concretamente cuando puede haber cambios de roles, es decir que se autoricen o desautoricen accesos a zonas con información sensible. Por ello las organizaciones deben tener un protocolo eficaz y ágil para autorizar accesos a medida que surgen cambios.

Las soluciones de cara a problemas de gestión de identidades se suelen llevar a cabo con diversos componentes. Los servicios de directorios, los metadirectorios y los directorios virtuales son componentes de red que autorizan la administración de información centralizada y permiten el almacenamiento de usuarios y de recursos simultáneamente.

En cuanto a las medidas legales que se pueden tomar para prevenir la fuga de datos están la solicitud de aceptación de política de seguridad y confidencialidad, que corresponde a la seguridad interna con los empleados. Más allá de la fuga de datos, la seguridad legal de una empresa es fundamental para garantizar el cumplimiento de las normativas y las leyes que atañan a la organización. La seguridad con terceros representa los contratos vinculantes que existen entre la empresa y los servicios externos subcontratados. En estos acuerdos se determinan los activos que vigilará el proveedor, y los que vigilará la empresa, una clasificación de incidentes, las tareas de seguridad y las obligaciones contractuales.

3.3. Detección

El proceso de detección de ciberataques puede darse durante la consecución del propio ataque o después de que se haya producido. La detección de la amenaza en tiempo real es lo idóneo y se suele dar gracias al antivirus en caso de *malware*. Mientras que si se descubre con posterioridad que la empresa ha sido atacada, las secuelas son mayores ya que los atacantes han podido actuar libremente.

Las herramientas de ciberseguridad detectan de forma eficaz patrones de ataques conocidos. El inconveniente de los patrones de ataque desconocidos es que se han vuelto un fenómeno creciente entre los ciberdelincuentes que han cambiado su forma de actuar. Los ataques han pasado a tener un modelo diversificado que se puede ejecutar en cualquier momento. Por ello la detección proactiva es un elemento primordial para la detección de amenazas precoces. Mientras que la detección reactiva ofrece una solución cuando el ataque ya se ha producido en vez de preverlo. La efectividad de los modelos proactivos viene de su revisión periódica de la red y de una configuración más agresiva.

El dilema surge cuando las empresas no realizan escaneos de vulnerabilidades frecuentemente, sino de forma trimestral o anual. De ahí que la monitorización constante sea tan importante, ya que cualquier ataque realizado después de la revisión no será detectado hasta la próxima revisión. El plan de monitorización continua de los riesgos y vulnerabilidades es imprescindible para la ciberseguridad. A la hora de poner en marcha el plan hay que tener en cuenta el tamaño de la empresa y definir las responsabilidades de los encargados que activarán el plan (Fundación Telefónica, 2016).

3.4. Respuesta

En caso de que se haya materializado un ciberataque y que no se haya podido evitar, es importante que la empresa tenga un protocolo de actuación. Por un lado, habría que dar una respuesta técnica al daño informático. Y por otro lado habría que acudir a las fuerzas y cuerpos de seguridad del Estado y emprender acciones legales.

Los pasos a seguir en caso de ciberataque son en primer lugar desconectar el equipo de Internet y de la Intranet, de esta manera se interrumpe la expansión del virus por la red. En segundo lugar, la empresa debe disponer de un antivirus si es que no lo tiene instalado todavía. La eficacia de esta herramienta es clave sobre todo cuando es proactiva y tiene la capacidad de detectar amenazas constantemente. En tercer lugar, la empresa debe analizar su sistema al completo incluyendo todos los discos del equipo en busca de amenazas o daños. A continuación, debe modificar todas las contraseñas de aquellos servidores que requieran autenticación, de esta manera evitaremos el robo de credenciales. Finalmente, la empresa debería realizar una limpieza manual asegurándose de que la limpieza automática ha sido eficaz y no se ha dejado ningún dispositivo infectado.

Si el ciberataque ha consistido en robo de datos o suplantación de identidad, la empresa ha de tomar acciones legales y denunciar el suceso a las autoridades. La denuncia es fundamental para perseguir los delitos. Sin embargo, en muchas ocasiones el derecho evoluciona más lento que la ciberdelincuencia, por ello la ley no siempre tienen las herramientas suficientes para perseguir estos delitos.

Los sistemas de recuperación y la recolección de evidencias digitales son los componentes clave para dar una respuesta contundente y eficaz a los ciberataques. Los sistemas de recuperación permiten a los usuarios volver al estado de su equipo antes del ataque para solucionarlo. Microsoft desarrolló una herramienta que filtraba los archivos que sufrían cambios, copiándolos antes de que fueran sobrescritos. Todas estas herramientas son apoyos para la ciberseguridad, pero para que sean efectivos en su conjunto deben realizar copias de seguridad periódicamente.

Para la recolección de evidencias definimos evidencias digitales como cualquier fichero o dato contenido en un soporte digital. El rastro digital que dejan las evidencias digitales es esencial para perseguir los ciberdelitos y a los ciberdelincuentes. Una evidencia digital tiene que cumplir con tres requisitos para ser válida. Tiene que ser auténtica, es decir que sea veraz y no haya sido modificada. Tienen que ser precisa, es decir que se relacione inequívocamente

con el delito. Por último, la evidencia digital tiene que ser suficiente, es decir que por ella sola pueda demostrar un hecho, sin necesidad de elementos externos.

Por todas estas razones es vital para la empresa llevar un registro electrónico de sus movimientos y poder garantizar la integridad de ellos. Esto se puede conseguir trabajando con el *cloud computing* o la nube en la que se guardan ficheros (Fundación Telefónica, 2016).

3.5. Tendencias para los próximos años

Las tendencias en innovaciones tecnológicas tienen un impacto constante en todas las industrias, especialmente en la de ciberseguridad. Estas nuevas tendencias son retadoras ya que demandan nuevas habilidades y diferentes aptitudes. De hecho, los 10 trabajos más demandados en 2020 no existían en 2004 (Castellanos, 2019). A lo largo de las últimas décadas, los avances tecnológicos se han multiplicado exponencialmente, evolucionando de Internet en los años 90, a las redes sociales en los años 2000, pasando por los *Smartphones* en 2010, hasta llegar a la inteligencia artificial o la analítica de Big Data entre muchos otros avances. Estos avances suponen grandes oportunidades para que las empresas se expandan y crezcan. Sin embargo, habrá sectores que perecerán en la revolución digital. "En los próximos 10 años, 30% de los trabajos en Bancos serán reemplazados por Automatización de Procesos y tecnologías Cognitivas" (Castellanos, 2019).

La era Post Digital, aquella que empieza ahora, será también una oportunidad que aprovecharán los ciberdelincuentes para mejorar sus herramientas de ataque. Las transformaciones que se están dando por la evolución tecnológica tendrán grandes implicaciones en la sociedad humana. Las tecnologías implantables conseguirán el primer teléfono móvil implantable disponible en el mercado en 2023. El 50% del tráfico de los Internet estará generado por los aparatos electrodomésticos de los hogares en 2024. El 10% de las gafas de lectura estarán conectadas (Castellanos, 2019). Todos estos avances supondrán oportunidades y amenazas, ya que el mundo digital se va a hacer cada vez más amplio. Los ataques aumentarán y por ello la ciberseguridad debe aumentar a la par, si no más rápido.

Las tendencias tecnológicas afectan directamente a los negocios. La automatización de los procesos robóticos es una de las tendencias con mayor énfasis en el mercado y que se va a dar en un periodo muy corto de tiempo. Consiste en configurar un *software* que automatice e imite las actividades manuales realizando tareas repetitivas siguiendo reglas sencillas para la toma de decisiones. El Internet de las cosas (IoT) también va a ser una gran revolución. Son objetos físicos incrustados en ordenadores que pueden detectar sus entornos y cambiarlos para comunicarse con sistemas remotos. Las tecnologías cognitivas encabezadas por la Inteligencia Artificial (IA) serán tendencia de aquí a 4 años. Esta tecnología consiste en desarrollar sistemas computacionales capaces de desarrollar tareas que habitualmente requieren de la inteligencia humana (Castellanos, 2019).

El estallido de la pandemia en todo el mundo ha desencadenado innumerables consecuencias económicas, financieras, sociales… Pero sobretodo esta situación ha acelerado el proceso de digitalización. Desde que los gobiernos establecieron las cuarentenas a nivel mundial para protegerse contra la COVID-19, la cultura del teletrabajo se ha impulsado. Estos acontecimientos representan una disrupción de las infraestructuras tecnológicas de las empresas. La necesidad de trabajar en remoto incrementa la dependencia tecnológica. Los trabajadores han adquirido más responsabilidades debido al uso que hacen de la tecnología, contar con una seguridad cibernética fuerte es requisito imprescindible para proteger los sistemas centrales. En estos tiempos de incertidumbre digital las empresas han de velar por la continuidad del negocio, para ello la capacidad de adaptación de este es imprescindible para luchar contra los actores maliciosos.

Las empresas han sabido adaptarse a esta nueva situación reubicando a sus empleados y tomando decisiones rápidamente en cuestión de días. Sin embargo, las organizaciones tienen que proteger a sus trabajadores en términos de seguridad digital, ya que trabajar desde casa no es lo mismo que trabajar desde la oficina donde la red está protegida. El trabajo del Director de Seguridad de la Información (CISO) es establecer unas políticas sólidas que evalúen los riesgos del teletrabajo e implementen soluciones. Mientras tanto las empresas

llevan a cabo la capacitación que protege a los empleados informándoles y recordándoles las nuevas medidas de protección.

Esta situación es el escenario idóneo para los ciberataques que se benefician de la incertidumbre de la situación mediante estafas de *phising*. El teletrabajo representa una vulnerabilidad para la empresa y una oportunidad para los ciberatacantes. Por tanto, esta nueva forma de trabajar constituye un reto para las organizaciones que tienen que ejecutar la ciberseguridad e integrarla con la política institucional corporativa. El teletrabajo es un reto porque, por un lado, puede beneficiar a las organizaciones aportando mejores condiciones de trabajo para sus empleados, facilitando la conciliación de la vida laboral y familiar. Y, por otro lado, es un reto porque las organizaciones tendrán que digitalizarse con mayor rapidez porque los ciberataques se van a acentuar y van a representar una amenaza persistente. Las organizaciones deberán crear sistemas informáticos resistentes y poner al trabajador en el centro de la política de capacitación. Una de las directrices que tendrán que llevar a cabo es la de invertir en formación para sus trabajadores. El elemento humano es igual de importante que el técnico y permitirá a las empresas transformar una debilidad en una fortaleza.

Los *ransomware* van a tener mucha relevancia en el panorama de la ciberseguridad del futuro. Como ya hemos comentado con anterioridad un *ransomware* es un programa informático malicioso que pretende cifrar archivos, bloquear el acceso hasta que se pague un rescate. La tendencia creciente para ejecutar los *ransomware* son las exfiltraciones y la extorsión. Los ciberdelincuentes extraen la información confidencial la guardan en un lugar seguro, y luego cifran los datos para pedir un rescate a la víctima. Las acciones de los atacantes tienden a publicar o vender esta información. No obstante, las organizaciones están cada vez más preparadas gracias a las inversiones en inteligencia y en tecnología. En muchas ocasiones los ciberatacantes se encuentran con procesos resistentes de *backup* y restauración, lo que influye para que las empresas no paguen los rescates (ESET, 2020).

En conclusión, las tendencias en ciberseguridad y riesgos cibernéticos para los próximos años incluyen el aumento de la complejidad y frecuencia de los ataques, especialmente de

los *ransomware*. Por ello las empresas tienen que aumentar la inversión en prevención y remediación. No obstante, el personal cualificado será escaso y de alto coste.

4. Análisis y estudio de la ciberseguridad en las instituciones financieras

Las instituciones de servicios financieros son las más vulnerables a los ciberataques, ya que son el objetivo principal de los cibercriminales. La industria de los servicios financieros es de las más susceptible en recibir email malicioso, así como sus clientes. Como vemos en la Figura 5 a continuación, el robo o fraude financiero es uno de los delitos con mayor impacto y más ejecutados por los ciberatacantes en el sector bancario (Deloitte, 2014).

Figura 5. Mapa de calor de los actores e impactos de los ciberataques en el sector bancario[7]

	IMPACTS						
ACTORS	Financial theft/ fraud	Theft of intellectual property on strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life/ safety	Regulatory
Organised criminals	↑↑	→	↓	↓	↑↑	↓	↑↑
Hacktivists	↑	→	↑↑	↑	↑↑	↓	↑
Nation-states	↑	↑	↑↑	↑↑	↑↑	↓	↑↑
Insiders	↑↑	↑	↑	↑	↑	→	↑
Third parties	↑	→	→	→	↑↑	↓	↑↑
Skilled individual hackers	↑↑	↑	↑	↑	↑	↓	↑

↑↑ Very high ↑ High → Moderate ↓ Low

Fuente. (Deloitte, 2014)

[7] Estudio realizado en más de 250 organizaciones se servicios financieros de 39 países, principalmente EMEA, América Latina y Japón (Deloitte, 2014).

4.1. El Estado de la ciberseguridad en las instituciones financieras

El desarrollo de este apartado se basará en la encuesta[8] realizada por el Centro de Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC), junto con el Servicio de Riesgos Cibernéticos de Deloitte en 2018. Participaron tanto empresas grandes, con más de 2.000 millones de dólares de ingresos anuales, como empresas pequeñas, con menos de 500.000 de dólares de ingresos. Los encuestados procedían de todos los sectores financieros, aunque se inclinaban más hacia la comunidad bancaria.

En este análisis del sector financiero examinaremos los elementos en las operaciones de ciberseguridad de cada institución financiera encuestada, incluyendo cómo se organizan y gobierna, a quién reporta el CISO (*Chief Information Security Officer),* cuándo y dónde se abastece externamente de funciones de gestión de riesgos, así como las prioridades de inversión para mejorar las capacidades de ciberseguridad.

En primer lugar, cada institución financiera se evaluó por un tercero para informar sobre su nivel de madurez en materia de ciberseguridad. Estos niveles de madurez de la ciberseguridad se dividen en cuatro, de menor a mayor madurez:

- Parcial: las prácticas de gestión del riesgo de ciberseguridad de la organización no están formalizadas. El riesgo se gestiona *ad hoc* y a veces de forma reactiva.

- Informado: las prácticas de gestión de riesgos son aprobadas por la dirección, pero no pueden establecerse como política para toda la organización.

- Repetible: las prácticas de gestión de riesgos de la organización se aprueban formalmente y se expresan como política.

[8] Encuesta realizada a 51 empresas procedentes de todos los sectores financieros, concretamente el sector bancario en EE. UU. (Eckenrode & Friedman, 2018).

- Adaptación: la organización adapta sus prácticas de ciberseguridad basándose en las lecciones aprendidas y los indicadores predictivos derivados de las actividades de ciberseguridad anteriores y actuales.

4.2. Características en función de los niveles de madurez

A continuación, veremos las características de la ciberseguridad en función de los distintos niveles de madurez. Es importante comprender que en muchas ocasiones la forma en la que se organiza y gobierna una entidad puede tener un impacto igual, si no mayor, que la cantidad que se gasta en relación con el presupuesto general del departamento de Tecnología Informática. De hecho, muchas empresas con asignaciones presupuestarias de ciberseguridad por debajo de la media consiguieron alcanzar un alto nivel de madurez del programa, mientras que algunas que tenían un gasto superior a la media estaban en realidad menos avanzadas. Este mecanismo nos podría ayudar a comprender los retos a los que se enfrentan las organizaciones más grandes a la hora de avanzar en sus capacidades, en comparación con organizaciones más pequeñas.

Si el dinero no es el único criterio de la eficacia de la ciberseguridad, ¿qué factores diferencian las prácticas de gestión de riesgos de los encuestados con capacidad de *adaptación*, aquellos que han alcanzado el nivel más alto de implementación, de sus homólogos de menor nivel de madurez?

Los miembros de los consejos de administración y de los comités de dirección de las empresas encuestadas estaban muy interesados en la estrategia global de ciberseguridad de sus empresas. Sin embargo, las empresas con capacidad de *adaptación* sugieren que los miembros de sus consejos se impliquen y profundicen en los detalles del presupuesto de ciberseguridad, las funciones y responsabilidades operativas específicas, así como la evolución del programa. Las empresas con nivel de madurez *informadas* explicaron que sus consejos de administración suelen estar menos interesados en revisar las amenazas actuales, el progreso del programa y los resultados de seguridad.

Tres cuartas partes de las empresas encuestadas tenían una función de ciberseguridad totalmente centralizada. A pesar de ello las empresas con capacidad de *adaptación* eran más propensas a favorecer un enfoque híbrido, con funciones centralizadas, pero con cada unidad de negocio dotada de capacidades de estrategia y ejecución y coordinada entre sí. De esta manera se demuestra que la responsabilidad compartida entre los trabajadores del departamento de ciberseguridad favorece la implicación y dedicación en el trabajo (Eckenrode & Friedman, 2018).

Otro pilar importante para la eficacia de la ciberseguridad es establecer líneas de defensa independientes las unas de las otras. Las empresas de *adaptación* tienen dos líneas de defensa en ciberseguridad separadas: la primera implica la seguridad en las unidades de primera línea, y la segunda son las operaciones de gestión de riesgos cibernéticos en toda la organización.

Asimismo, es fundamental que la exposición a los riesgos cibernéticos esté distribuida. Alrededor de la mitad de las empresas encuestadas de nivel de madurez *informada* explican que sus organizaciones no compraron ningún seguro para cubrir específicamente los riesgos cibernéticos. Mientras que dos tercios de las empresas con capacidad de *adaptación* dijeron que sus organizaciones habían contratado un seguro cibernético adaptado a los escenarios de pérdidas previstas.

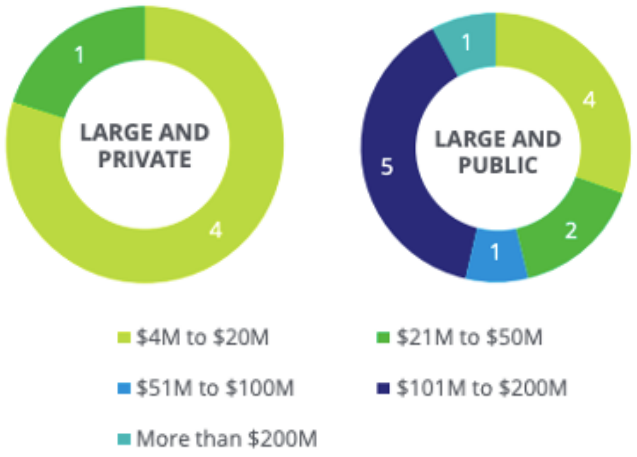
Las empresas con programas de seguridad menos maduros y potentes tienden a recurrir a fuentes externas para apoyar las funciones de seguridad con personal especializado en materia de ciberseguridad (Eckenrode & Friedman, 2018).

4.3. La importancia del tamaño en los programas de ciberseguridad

Las instituciones financieras podrían no estar asignando los recursos suficientes a la ciberseguridad. Según la encuesta de Deloitte, los datos parecen sugerir que los presupuestos de gestión de riesgos cibernéticos de las mayores instituciones financieras pueden oscilar entre el 5% y el 20% del total del presupuesto de Informática. La mitad de las grandes empresas del sector financiero declararon que el gasto en gestión de riesgos cibernéticos era de 20 millones de dólares o menos. Esto significa que la mitad de las empresas gastan un 1% o menos de sus ingresos en ciberseguridad. Esta cifra no es suficiente teniendo en cuenta los riesgos de interrupción de las operaciones, el daño reputacional, los costes de investigación y los gastos de reparación que podrían surgir (Eckenrode & Friedman, 2018).

El gasto en materia de ciberseguridad puede estar muy relacionado con el tipo de propiedad de las instituciones financieras. Las empresas con titularidad pública tienden a invertir más en ciberseguridad que aquellas que son privadas, como se observa en la Figura 6 (Eckenrode & Friedman, 2018). Las instituciones financieras públicas tienen más en cuenta su sistema de ciberseguridad ya que la existencia de problemas en materia de ciberseguridad puede preocupar a sus inversores, accionistas y analistas, así como afectar a la capitalización del mercado.

Figura 6. Presupuestos de gestión de riesgos cibernéticos por tamaño de la Institución Financiera



Fuente. (Eckenrode & Friedman, 2018).

Más de un tercio de las instituciones encuestadas gastan sus presupuestos de ciberseguridad en actividades operativas, frente a menos de un tercio en iniciativas de transformación como la cibervigilancia. Más de la mitad de las empresas gastan su presupuesto de tecnología en el funcionamiento del negocio. Este es un punto clave para la ciberseguridad en las instituciones financieras, deben invertir más presupuesto en iniciativas transformacionales ya que la ciberseguridad es un tema que evoluciona rápidamente y requiere de gran capacidad de adaptación por parte de las empresas (Eckenrode & Friedman, 2018).

El tamaño de las instituciones financieras es un factor explicativo de la estructura de ciberseguridad. Más de la mitad de los CISO, director de Seguridad de la Información, de empresas pequeñas responden directamente ante un director ejecutivo. Estas relaciones son sinónimo de una estructura de organización plana. Mientras que, en las empresas más grandes, el CISO responde ante el director de información (CIO), al director de operaciones (COO) o al director de riesgos (CRO). Estas relaciones demuestran que la información que transmite el CISO es recibida y tratada por profesionales más especializados en las grandes empresas que en las pequeñas. Esta situación puede ser más beneficiosa para las empresas grandes que podrán analizar en profundidad la información y tomar decisiones en base a ella.

Las principales prioridades de innovación que establecen las empresas encuestadas en torno a las capacidades de ciberseguridad son la adopción de los móviles, la nube y los datos en sus empresas. Asimismo, la integración de las ciberdefensas es una prioridad a nivel empresarial. La tecnología y la innovación son los asuntos más importantes en materia de innovación para los CISO (Eckenrode & Friedman, 2018).

4.4. Áreas de mejora

Las instituciones financieras han reforzado su espectro de madurez de la gestión del riesgo en todo el sector. Es clave que encuentren el equilibrio entre el riesgo y la innovación. Para ello, tienen que involucrar a la junta directiva de forma proactiva, proporcionando informes detallados a los miembros del consejo para involucrarlos en la consecución de objetivos.

Igualmente es importante implicar a toda la organización en la ciberseguridad, ya que no solo depende de los trabajadores de ese departamento, sino que depende de todos los empleados. Es clave formar a los empleados para que entiendan y acepten su papel y responsabilidades en el mantenimiento de una buena ciberseguridad para evitar intrusiones. Implicando a todo el personal en la ciberseguridad la empresa consigue establecer varias líneas de defensa, mejorando la gestión de los riesgos cibernéticos. Para ello la concienciación y la responsabilidad compartida son fundamentales.

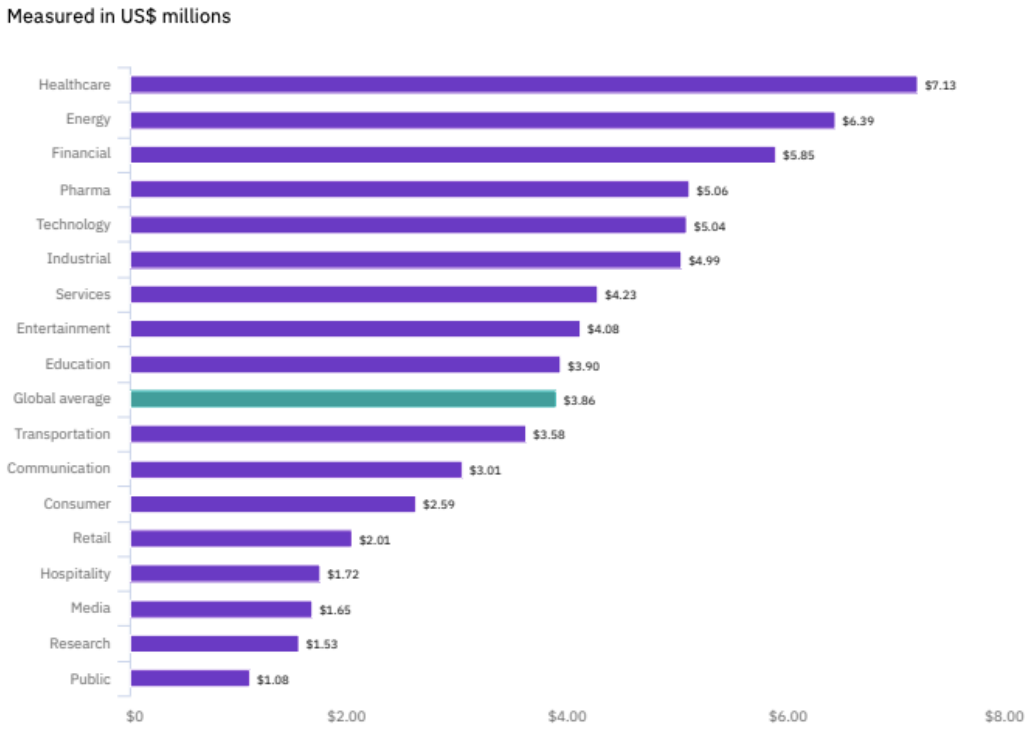
Por lo general, los CISO se centran en tareas tácticas y funciones tradicionales como la de tecnólogos. Sin embargo, a medida que los temas de ciberseguridad han cogido importancia, los CISO deberán enfocar su tiempo en tareas de estrategia para complementar y apoyar al consejo de administración.

La ciberseguridad en las instituciones financieras se presenta como un reto continuo ya que las amenazas siguen evolucionando. La ciberseguridad es una función integral de las empresas, por ello deben ir adaptándose para prevenir los posibles ataques. Para ello es importante que las instituciones financieras permanezcan seguras, vigilantes y resistentes frente al panorama cambiante al que se enfrentan. La colaboración entre empresas del sector es fundamental para mejorar sus ciberdefensas y su gestión del riesgo cibernético.

5. Desafíos para la ciberseguridad en el futuro

El desafío para las instituciones financieras se concreta en cómo favorecer el crecimiento y mejorar la rentabilidad mediante el uso seguro de las nuevas tecnologías. Según previó el Foro Económico Mundial, los riesgos tecnológicos más recurrentes son los ciberataques, los fallos de la infraestructura informática crítica y los fraudes de datos. Las pérdidas financieras relacionadas con robo de datos y dinero fueron de 82% en 2019 (Castellanos, 2019). Esto es una consecuencia de que los cibercriminales han aumentado los objetivos potenciales. Como se ha visto en el capítulo anterior, las instituciones financieras son uno de los principales objetivos de los ciberataques por la naturaleza de los datos que contienen. Como vemos en la Figura 7, el sector financiero tuvo que hacer frente a un alto coste por filtraciones de datos, siendo la tercera industria con mayor coste (IBM Security, 2020)[9].

Figura 7. Coste total medio de filtraciones de datos por industria



Fuente. (IBM Security, 2020).

[9] Estudio realizado a partir de una muestra de 524 organizaciones de 17 industrias y 17 países, cuyas principales áreas geográficas son EE. UU., América Latina, Europa, Asia y Oceanía (IBM Security, 2020).

5.1. Factor técnico

Como se ha explicado a lo largo del trabajo los ciberataques son una amenaza que ha venido para quedarse, sobre todo en el sector financiero. El riesgo cibernético supone la tercera prioridad para las entidades financieras, mientras que la ciberseguridad tan solo supone su duodécima prioridad (Deloitte, 2014). Este desajuste de prioridades para las entidades financieras supone un reto que deben resolver en el corto plazo. La existencia de un riesgo debe implicar automáticamente la activación de un mecanismo de defensa, para ello las entidades financieras deberán asignar más fondos y recursos al desarrollo de barreras de ciberseguridad.

La evolución del panorama cibernético ha desencadenado un cambio más dinámico en el enfoque de las capacidades de ciberseguridad. Las estrategias de ciberseguridad han de ser, en primer lugar, seguras, es decir que mejoren los controles prioritarios de riesgo para protegerse contra las amenazas conocidas y emergentes. En segundo lugar, las estrategias de ciberseguridad tienen que desarrollar la característica de vigilante, para detectar infracciones y anomalías mediante un mejor conocimiento en todo el entorno. Por último, las estrategias de ciberseguridad tienen ser resistentes estableciendo la capacidad de volver rápidamente a las operaciones normales y reparar los daños de la empresa.

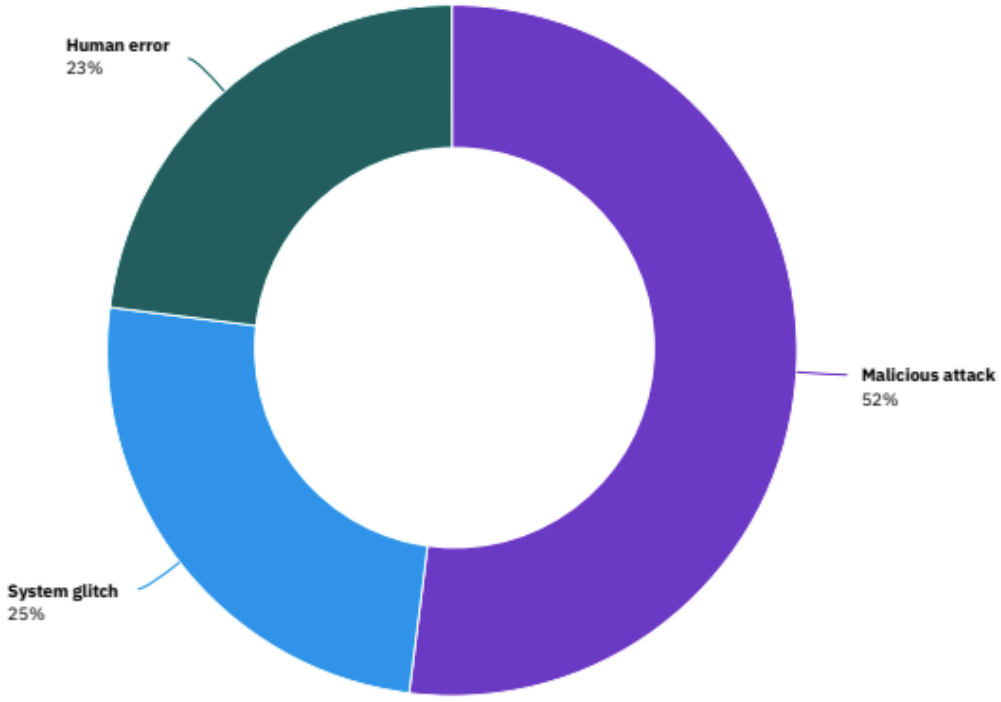
Invertir grandes cantidades en ciberdefensa de la organización es clave, aunque siempre con una planificación y respondiendo a los ciberdelitos más recurrentes. Los programas de defensa han de ser preventivos e inteligentes en materia de riesgos para construir una defensa en profundidad con diferentes capas de seguridad. Los sistemas de ciberseguridad tienen que ser revisados y actualizados con cierta frecuencia, para lograr las tres capacidades esenciales explicadas previamente, ser seguros, vigilantes y resistentes.

Invertir en prácticas de ciberseguridad es una parte fundamental, pero tiene que ir acompañado de la formación de los empleados.

5.2. Factor humano

El aumento de la inversión en herramientas y tecnologías para evitar que estos ataques tengan éxito no siempre garantiza la mejora de la ciberseguridad. Es importante tener en cuenta el factor humano, ya que la falta de concienciación y respuesta a las amenazas sugiere que las tecnologías más preventivas son, por sí solas, probablemente inadecuadas. Como se ve en la Figura 8, el error humano representa la tercera causa de filtraciones de datos en instituciones financieras (IBM Security, 2020). Por ello, las instituciones financieras tienen que considerar un sistema de formación a sus empleados para tratar de disminuir los errores humanos en sus organizaciones. Estos sistemas de formación pueden materializarse en sistemas de capacitación para instruir a los empleados y dotarles con las herramientas necesarias para que sepan localizar las ciberamenazas. Algunas iniciativas podrían ser establecer un correo de consultas, organizar charlas de formación, crear una guía de buenas prácticas entre otros.

Figura 8. Principales causas de las filtraciones de datos

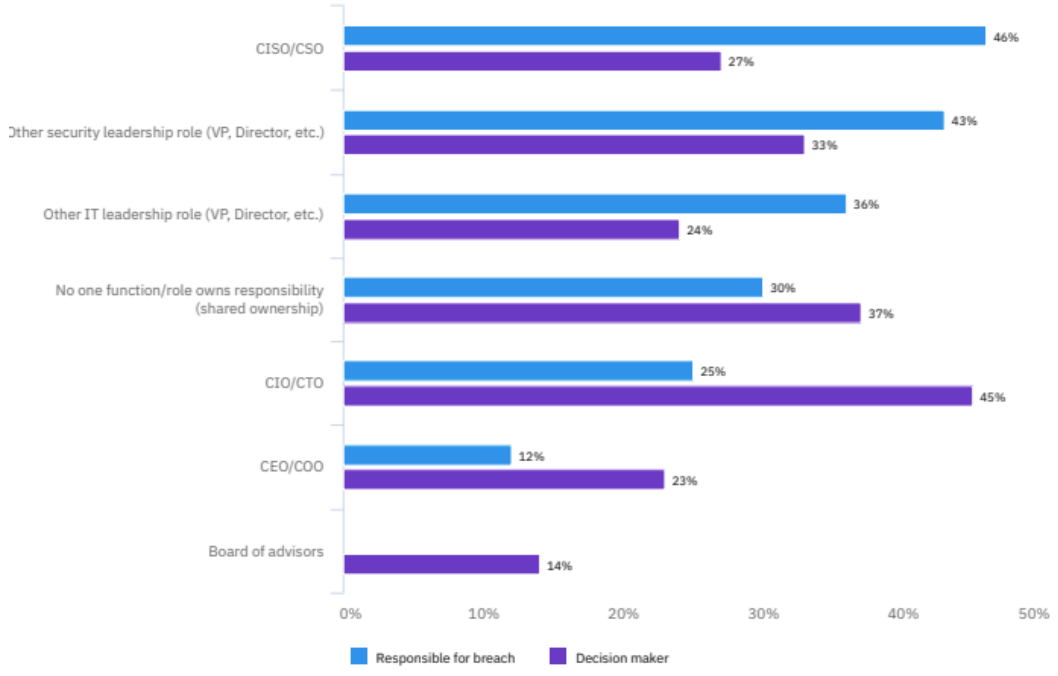


Fuente. (IBM Security, 2020).

5.3. Retos para el CISO

El CISO es el director de la seguridad de la información de la empresa. Es importante que este profesional esté técnicamente preparado y tenga las habilidades necesarias para adaptarse a las características cambiantes de la ciberseguridad. El CISO debe tener las tres características que han de tener los sistemas, es decir que ha de ser seguro en sus decisiones, estar vigilante al nuevo panorama cibernético y ser resiliente en los cambios. Como vemos en la Figura 9, el 46% de los encuestados dirían que el CISO es responsable en caso de brecha de seguridad (IBM Security, 2020). Sin embargo, solo el 26% de los encuestados atribuye al CISO la responsabilidad de la toma de decisiones tecnológica y de la política de ciberseguridad. Claramente hay una incongruencia de objetivos, ya que las responsabilidades del CISO deben de ir alineadas con la toma de decisiones, que hasta ahora se le atribuye en un 45% al CIO/ CTO, director de información y tecnología (IBM Security, 2020).

Figura 9. Responsables de las decisiones tecnológicas, las brechas y la política de ciberseguridad



Fuente. (IBM Security, 2020).

Uno de los grandes retos que tendrá el CISO de cara al futuro será el de implementar la cooperación entre los equipos de red y seguridad. El trabajo en equipo será fundamental para compartir la información y llegar a resultados mejores a través de las sinergias. Será retador implementar esta metodología de trabajo debido al incremento del trabajo en remoto. Asimismo, el CISO y su equipo tendrán que trabajar codo con codo con los proveedores de seguridad en una relación de confianza y colaboración plena. La unión de fuerzas será un factor clave para el éxito de la ciberseguridad en el futuro.

El CISO será el encargado de alinear la estrategia corporativa con las prácticas de protección de datos que contemplan las nuevas regulaciones. Los datos serán tratados en la nube lo que ayudará a cumplir la regulación.

También es importante mencionar que el CISO tendrá que adaptarse a nuevas tecnologías como la Inteligencia Artificial y el aprendizaje automático, ya que van a ser fundamentales para desarrollar nuevos modelos de detección y prevención de ciberamenazas. Estas tecnologías serán la clave de las nuevas ciberamenzas, por ello es bueno conocerlas y saber cómo van a atacar los agentes en un futuro.

Las funciones que lleva a cabo un CISO, director de seguridad de la información, son cuatro. Por un lado, un CISO hoy en día desempeña principalmente la función de *guardián,* es decir, se encarga de proteger los activos del negocio entendiendo el panorama de amenazas y gestionando la efectividad de los programas de ciberiesgo. Por otro lado, la segunda función que desempeña es la de *tecnólogo* que consiste en evaluar e implementar las tecnologías de seguridad para mejorar las capacidades de la organización. Estas funciones contribuyen a crear un profesional preparado y al corriente de los detalles técnicos. Sin embargo, el CISO también tiene que desarrollar un perfil *estratega* capaz de dirigir el negocio y la estrategia de ciberseguridad motivando un cambio transicional en la gestión del riesgo. Asimismo, el CISO también tendrá que ser *asesor* integrándose en el negocio para asesorar e influir en las decisiones con implicaciones sobre el riesgo cibernético.

Hoy en día, el perfil del CISO ya no tiene que ser meramente de tecnólogo, sino también tiene que impulsar la estrategia comercial. Mantener una vía de comunicación entre el departamento de seguridad y la junta es vital para tener habilitado un canal de información que favorezca la toma de decisiones. Hasta ahora el CISO está desempeñando funciones de *tecnólogo* y *guardián*, sin embargo, tiene que desarrollar nuevas funciones como las de *estratega* y *asesor*, para alinear el negocio con la estrategia de riesgos. Además de *tecnólogo* el CISO tiene que ser *estratega* y entender las consecuencias globales que conlleva un ataque cibernético para la organización. Las pérdidas económicas asociadas a ataques cibernéticos a veces no son significativas para la cuenta de resultados de las empresas. No obstante, el verdadero impacto potencial está en la confianza de los clientes y de los inversores. El riesgo de reputación supone riesgos importantes para las empresas de servicios financieros.

6. Conclusiones

Este trabajo ha permitido dar luz sobre el concepto de ciberseguridad, que es un tema muy en tendencia por la cantidad de ciberataques que reciben regularmente las empresas, concretamente las instituciones financieras. Mientras se redactaba este trabajo se dieron una serie de ciberataques contra los ministerios de Economía, Educación y Justicia español y el Instituto Nacional de Estadística (INE). Esta noticia reafirma la pertinencia de este tema y confirma las razones de su elección. Es un tema de creciente importancia que va a dar lugar a muchos puestos de trabajo, ya que se demandarán expertos en ciberseguridad.

La ciberseguridad nace como consecuencia de los usos que se hacen de Internet. Desde entonces el panorama cibernético ha cambiado bastante, suficiente como para que la ciberseguridad se tenga que adaptar a nuevas ciberamenazas. La cuestión que se presenta en este trabajo trata de plasmar los retos y desafíos de la ciberseguridad en los próximos años. De esta manera se han marcado unas pautas que determinan una gestión exitosa de los sistemas de ciberseguridad en las instituciones financieras.

Como se ha ido viendo a lo largo del trabajo, las máquinas han de estar protegidas física y cibernéticamente por programas especializados. Esta fase es en la que más recursos se dedican y por ello la más controlable. Sin embargo, cuando los sistemas están protegidos, los ciberatacantes se aprovechan de las vulnerabilidades de las personas. De ahí que uno de los principales retos de la ciberseguridad es la de formar técnicamente a todos los empleados para que no exista ningún eslabón débil. También es interesante hacer una auditoría de ingeniería social para ver hasta qué punto los empleados son vulnerables.

Este trabajo muestra que uno de los elementos de mejora en la ciberseguridad del futuro es la formación de las personas. Los humanos son la variable exógena más complicada de controlar en una gran empresa, de ahí que sea el eslabón más débil de las organizaciones y por ende el principal objetivo de los ataques. El reto para las instituciones financieras es formar a todos los empleados por igual, desde el CEO hasta el último empleado, ya que todos suponen una oportunidad de entrada a un ciberataque.

Establecer las políticas de formación técnica y llevarlas a cabo forma parte del rol del CISO. El CISO tiene que estar muy bien formado y tener los conocimientos técnicos actualizados en materia de ciberseguridad, pero también es clave que tenga una visión del negocio global. Por ello, el perfil del CISO es complicado ya que debe ser muy completo y versátil. Tiene que ser flexible y capaz de adaptarse a los cambios del entorno.

Esta investigación aporta unas líneas directrices de las claves para gestionar correctamente la ciberseguridad en una institución financiera. Al tratarse de un entorno cambiante, el estudio de investigación tenderá a quedarse atrasado en cuanto cambien las condiciones del entorno. En pocos años la ciberseguridad habrá avanzado enormemente, por ello este trabajo responde a los retos de la ciberseguridad planteados en el momento actual, y no será aplicable en cualquier momento del futuro.

En cuanto a posibles líneas de investigación, se podrían llevar a cabo otros estudios en relación con la ciberseguridad en el futuro, por ejemplo, cómo se adaptarán las instituciones financieras a las nuevas ramas de la inteligencia artificial, como al aprendizaje automatizado. Al fin y al cabo, la tecnología va a continuar avanzando y con ella las ciberamenzas y los sistemas informáticos se irán desarrollando. Sería interesante analizar esa "carrera" por adaptarse al entorno cambiante y a las nuevas tecnologías y ver quienes lo logran con mejor resultado, si las empresas o los ciberatacantes.

7. Bibliografía

Banco de España. (2018). *Memoria Anual sobre la Vigilancia de las Infraestructuras de los Mercados Financieros 2018*. ISSN: 2605-1893 (edición electrónica). https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaAnualSistemasPago/18/MAV2018.pdf

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%20risk%2026-feb-2019.pdf

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

CISCO. (2020). *Protección para el presente y el futuro. 20 consideraciones de ciberseguridad para el futuro.* Serie de informes sobre la ciberseguridad de Cisco de 2020. Estudio Comparativo sobre CISO. https://www.cisco.com/c/dam/global/es_es/solutions/ES-CISO-Benchmark-Report-2020.pdf

Deloitte Advisory, SL. (2013). *Ciberseguridad es su negocio.* https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte_ES_GRC_Ciberseguridad.pdf

Deloitte. (2017). *¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?* https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte-ES-GRC-Informe-WannaCry.pdf

Deloitte. (2014). *Transforming cybersecurity in the Financial Services Industry. New approaches for an evolving threat landscape.* [Figura 5] https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_Transforming_Cybersecurity_05122014.pdf

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).* [Figura 6] https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Deloitte-Risk-Cybersecurity-Financial-Institutions.pdf

ESET. (2020). *Tendencias en Ciberseguridad para el 2021: Mantenerse seguro en tiempos de incertidumbre.* https://www.welivesecurity.com/wp-content/uploads/2020/12/Cybersecurity_Trends_2021_ES.pdf

Financial Stability Board (FSB). (October 2018). *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices.* https://www.fsb.org/wp-content/uploads/P131017-2.pdf

Fundación Telefónica. (2016) *Ciberseguridad, la protección de la información en un mundo digital*. Editorial Ariel, S.A. https://publiadmin.fundaciontelefonica.com/index.php/publicaciones/add_descargas?tipo_fichero=pdf&idioma_fichero=es_es&title=Ciberseguridad%2C+la+protecci%C3%B3n+de+la+informaci%C3%B3n+en+un+mundo+digital&code=531&lang=es&file=Ciberseguridad.pdf

Gaidosch, T. (2018, julio). La industrialización de la ciberdelincuencia, *Finanzas y desarrollo,* 22-25. https://www.imf.org/external/pubs/ft/fandd/spa/2018/06/pdf/gaidosch.pdf

Granados Franco, E., (2020). *The Global Risks Report 2020*. World Economic Forum in partnership with Marsh & McLennan and Zurich Insurance Group. [15th edition] [Figura 4] https://www.marsh.com/ve/es/insights/research/global-risks-report-2020.html

IBM Security. (2020). *Cost of a Data Breach Report.* [Figura 2-7-8-9]. https://www.ibm.com/downloads/cas/RZAX14GX

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.pdf

Instituto Nacional de Ciberseguridad (INCIBE). (2017). *Decálogo de Ciberseguridad en empresas. Una guía de aproximación para el empresario.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

Interreg (Cooperación Territorial Europea). (2020). Manual de Seguridad Informática en la Empresa. https://www.google.com/search?q=Interreg%282020%29.+Manual+de+Seguridad+Inform%C3%A1tica+en+la+Empresa.&sxsrf=ALeKk00SWqc-Dbo3gcxCwf0_KbyXyQ_JWw%3A1619691377828&ei=cYeKYPjhMY_5gQbe9bKABg&oq=Interreg%282020%29.+Manual+de+Seguridad+Inform%C3%A1tica+en+la+Empresa.&gs_lcp=Cgdnd3Mtd2l6EANQ5IACWOSAAmCuigJoAXACeACAAZ4BiAGXApIBAzAuMpgBAKABAaoBB2d3cy13aXrAAQE&sclient=gws-wiz&ved=0ahUKEwi43uHJnKPwAhWPfMAKHd66DGAQ4dUDCA4&uact=5#

KPMG. (2015). *Un año de Unión Bancaria*. https://assets.kpmg/content/dam/kpmg/pdf/2015/12/Union-Bancaria-091215.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. [Edición 1178]. [Figura 3]. https://www.asobancaria.com/wp-content/uploads/semana-economica-edicion-1178.pdf

Morán Blanco, S. (2017). La ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. *Revista Española de Derecho Internacional.* REDI, vol. 69, 196- 221. http://www.revista-redi.es/wp-content/uploads/2017/08/8_estudios_moran_blanco_ciberseguridad.pdf

PriceWaterhouseCoopers (PwC). (2020). *Fighting fraud: A never-ending battle. PwC's Global Economic Crime and Fraud Survey* [Figura 1] https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

PriceWaterhouseCoopers (PwC). (2019). *Unión Bancaria, reto de ser digital y regulado.* https://www.clubgestionriesgos.org/wp-content/uploads/Union-Bancaria_2019.pdf

PriceWaterhouseCoopers (PwC). (2018). *Pulling fraud out of the shadows: Global Economic Crime and Fraud Survey 2018* https://www.pwc.es/es/publicaciones/deals/assets/encuesta-mundial-fraude-delito-economico-2018.pdf

Urueña Centeno, F. J. (2015, 16 de enero). *Ciberataques, la mayor amenaza actual*. Instituto Español de Estudios Estratégicos (ieee) http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf