MÁSTER: Gestión de Riesgos Financieros

CIBERSEGURIDAD Y RIESGO OPERACIONAL EN LAS ORGANIZACIONES

Autor: Noelia Martínez Landrove

Tutor: Mónica Hernáez Rollón

Trabajo Fin de Máster

Madrid

Agosto 2019

ÍNDICE

ÍNDICE FIGURAS

RESUMEN

El objetivo de este trabajo es dar luz de una forma sencilla y clara todos los problemas que tienen las organizaciones no financieras, pero sobre todo las financieras a la hora de enfrentarse a los ataques cibernéticos y de implementar la seguridad necesaria dentro de las corporaciones. Para poder realizarlo se ha realizado una tarea de búsqueda y de recopilación de información a través de distintos informes.

Durante el trabajo se ha aprendido acerca de los distintos ciberataques a los que se enfrenta una compañía, cómo se implementa las medidas de seguridad, los problemas a los que se enfrentan y las guías, reglamentos y leyes que se están aprobando para gestionar adecuadamente el riesgo cibernético.

Como conclusión de todo el estudio se puede decir que aunque las organizaciones, las instituciones y los gobiernos son cada vez más conscientes de la amenaza que supone un ciberataque aún queda un largo recorrido hasta alcanzar unas medidas de seguridad adecuadas.

PALABRAS CLAVES: Ciberataque, ciberseguridad, riesgo operacional, riesgo cibernético, organizaciones, instituciones financieras.

ABSTRAC

The objective of this work is to give light in a simple and clear way all the problems that non-financial organizations have, but especially financial ones when dealing with cyber-attacks and implementing the necessary security within corporations. In order to do this, a search and information gathering task has been carried out through different reports.

During the work we have learned about the different cyber-attacks that a company faces, how security measures are implemented, the problems they face and the guides, regulations and laws that are being passed to properly manage the risk cybernetic

As a conclusion of the entire study, it can be said that although organizations, institutions and governments are increasingly aware of the threat posed by a cyber-attack, there is still a long way to go to achieve adequate security measures.

KEY WORDS: Cyber-attack, cybersecurity, operational risk, cyber risk, organizations, financial institutions.

1. INTRODUCCIÓN

La llegada de las nuevas tecnologías ha supuesto grandes avances técnicos, que han generado grandes beneficios financieros como no financieros tanto a las personas como a las organizaciones. Pero la tecnología también ha ocasionado nuevos riesgos a los que las empresas se tienen que enfrentar. Estos riesgos se pueden englobar en el riesgo cibernético.

El objetivo de este trabajo es exponer los problemas que tienen las organizaciones al enfrentarse a los ataques cibernéticos y de implementar la seguridad necesaria dentro de las corporaciones. El motivo por el cual se ha realizado este tema es porque los riesgos cibernéticos cada vez está más presente en el día a día de las organizaciones y se espera que esta importancia aumente en el futuro, ya que los avances tecnológicos no paran de aumentar y con él las posibles amenazas.

La metodología del mismo ha sido la búsqueda y recopilación de documentación de diversos informes y se ha intentado demostrar a lo largo del trabajo todos los conocimientos adquiridos a través de la lectura de todos esos documentos. Aunque en un principio, al ser un tema tan actual parecería que es fácil el proceso de recopilación de información, por el mismo motivo, ha resultado ser todo lo contrario.

A continuación se va a explicar brevemente la estructura del trabajo. En el primer apartado, nos encontramos con las definiciones más básicas de ciberataque y de ciberseguridad, también con los tipos de ciberataques más importantes en la actualidad, los autores de los ciberataques y por último las tendencias que previsiblemente se van a tener que enfrentar las entidades.

En el siguiente apartado pasamos a encuadrar todo el apartado anterior dentro del riesgo cibernético y este a su vez en el riesgo operacional. Posteriormente, se realiza un análisis del riesgo operacional.

El tercer apartado se centrará en las medidas de seguridad que las empresas están tomando para protegerse de los ciberataques y también los problemas que tienen a la hora de incorporarlas principalmente debido a que los ciberataques siempre van un paso por delante de la ciberseguridad.

Lo anteriormente mencionado, nos lleva al siguiente apartado en el que se va a abordar el tema de las ciberamenazas desde un punto de vista más general, el del sector. Se va a hablar de las medidas,

la legislación y las guías que se están imponiendo ante los ciberataques. Y también se va a mencionar la situación de las entidades financieras en relación con este problema.

Por último, se encuentra la conclusión dónde se van a recoger las ideas fundamentales explicadas a lo largo del trabajo.

2. EN QUÉ CONSISTE LOS CIBERATAQUES Y LA CIBERSEGURIDAD

En la actualidad, la llegada de las nuevas tecnologías ha ocasionado una gran revolución tanto a nivel productivo como económico que ha revolucionado todas las industrias. Toda esto, aunque a priori ha supuesto grandes beneficios también ha acarreado ciertos problemas como es que ciertos individuos intenten aprovecharse de las vulnerabilidades tecnológicas y obtener un beneficio económico, este es el caso de los ciberataques.

En primer lugar, para tener una visión global y poder continuar con el trabajo, es necesario definir brevemente qué son los ciberataques y la ciberseguridad.

Un ciberataque es un intento premeditado de un individuo o de un grupo de atacar el sistema informático de otro individuo o de una organización para destruir medios electrónicos y obtener un beneficio económico. También se incluye los fraudes, robos y falsificación a través de un aparato electrónico.

La ciberseguridad consiste en proteger los sistemas informáticos de posibles ataques. Estos ataques tienen como objetivo obtener, modificar o eliminar datos de las compañías, buscando un beneficio económico.

2.1 TIPOS DE CIBERAMENAZAS. [1]

A continuación se van a describir los tipos de amenazas más frecuentes que se han dado durante el 2018.

1. Código dañino o malware. El código dañino hace referencia a cualquier ataque a un sistema informático para causar un daño en el sistema o intentar modificar el mismo. Aquí se engloban, los virus, spyware, ransomware o los troyanos. Y es una parte esencial en la mayoría de los ataques, ya que buscan una debilidad dentro del sistema para instalarse en él.

   Entre las acciones que realizan destacan:

   - Bloquear el acceso de componentes de la red, es el caso de los ransomware

[1] Datos obtenidos en su mayoría de: Centro Criptológico Naciona (2019). *Ciberamenazas y tendencias. Edición 2019*. Recuperado el 2 de julio del 2019 en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3776-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-edicion-2019-1/file.html

- Instalar malware o software dañinos

- Obtener información de datos del disco duro, es el caso de los spyware.

- Dejar el sistema inoperativo al infectar ciertas partes del sistema fundamentales.

Como se puede ver en la figura siguiente, el código dañino en los últimos años ha tenido un crecimiento exponencial.

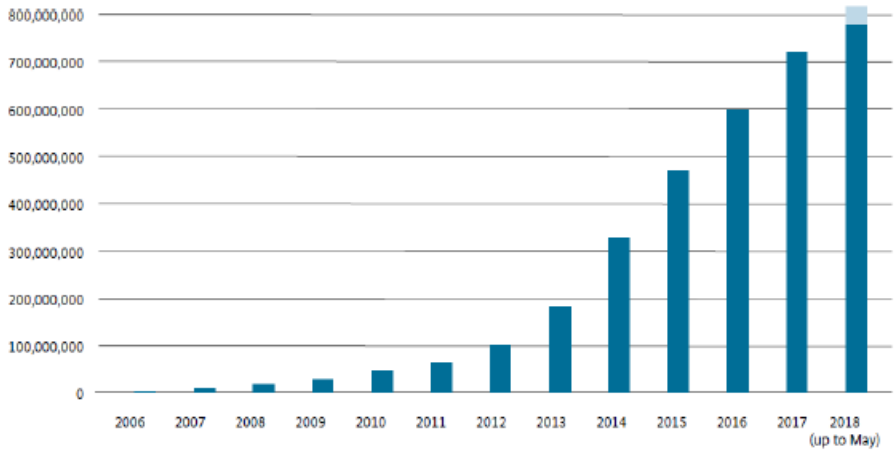

Figura 1 : Evolución de Código dañino en los últimos años.

Fuente: Ciberamenazas y tendencias. Edición 2019. Centro Criptológico Nacional.

2. Amenaza persistente avanzada (APT). Consisten en ciberataques dirigidos a instituciones y organizaciones lanzadas con el objetivo de obtener acceso a un sistema para poder robar información y propagar los ataques a otros sistemas.

   Para las primeras fases de este ataque, la forma más típica en la que se realiza este ataque es a través del secuestro de actualizaciones o archivos de instalaciones dañinos. Estos archivos se colocan en los servidores, de tal forma que cuando la organización vaya a descargar e instalar un programa también lo esté haciendo con el programa dañino. Es un método que está teniendo buenos resultados ya que las victimas están instalando el malware sin saberlo. A esta técnica también se le llama ataque en la cadena de suministro.

También se están usando de forma habitual para realizar este ataque los correos fraudulentos, con enlaces o archivos dañados.

Para las fases posteriores, se está utilizando la técnica de movimiento lateral que consiste en que una vez que se ha instalado el virus dentro del sistema intentan contagiar a otros sistemas.

3. Ciber-espionaje. Es una técnica que la están empezando a utilizar Estados y organizaciones, su objetivo principal es obtener y en ocasiones destruir cierta información confidencial tanto a nivel geopolítico, comercial o de propiedad intelectual y utilizarlo para mejorar su posición en el mercado frente a las víctimas.

4. Amenazas híbridas. Consiste en la utilización de varias técnicas coordinadas que van desde el ciberataque, métodos militares, presión económica o campañas en redes sociales realizadas con el objetivo de desestabilizar e influir en la opinión pública.

   Esta amenaza puede estar realizada tanto por agentes estatales como no estatales, utilizan el ciberespacio como herramienta para sus propósitos y juegan con la desinformación de las personas.

5. Correos electrónicos. Sigue siendo una de las técnicas más usadas para realizar la primera fase de un ciberataque. A través de esta técnica los atacantes acceden al sistema de las víctimas y pueden obtener la información que quieran o también analizar cómo está configurado el sistema para ir atacando más partes del mismo.

   Cabe destacar, que en un principio los objetivos eran individuos aleatorios o sin demasiada influencia dentro de las organizaciones. Actualmente, los ataques van dirigidos a personas con influencia dentro de las organizaciones para conseguir un mayor beneficio económico.

   La técnica principal de estos ataques es a través del spam. Esta técnica consiste en enviar correos no deseados ni solicitados, normalmente son de carácter publicitario. Esta técnica se divide en tres categorías:

4.1 Spam convencional. Se utiliza para promocionar ciertos productos o servicios que en algunas ocasiones pueden llegar a ser fraudes.

4.2 Malware Spam. Se mandan correos con malware dentro de un documento adjunto o de una imagen adjunta y se busca dañar el sistema de las víctimas de código dañino.

4.3 Phising o mensajes de suplantación de identidad. Los atacantes se hacen pasar por usuarios o empresas e incitan a la víctima a facilitarle cierta información comprometida.

Esta última técnica se ha convertido en la más popular, durante el 2018, aproximadamente el 90% de las infecciones de código dañino y el 72% de robo de datos en corporaciones ocurrieron debido a esta técnica.

6. Ransomware. Es un tipo de ciberataque que consiste en introducir cierto código dañino en los sistemas para obtener cierta información de las corporaciones y así poder exigir un rescate por la misma. Se podría decir que es un secuestro de datos.

Hay dos tipos de ransomware, el que bloquea el acceso al sistema y muestra un cuadro de diálogo en el equipo con la petición del rescate. Y el que bloquea los datos de la víctima y tras el pago del rescate, que generalmente se realiza en criptomoneda, el atacante da la clave para desbloquear los datos.

Estos ataques se pueden realizar a través de:

- Los correos electrónicos, los cuales contendrán un código dañino.

- Exploits drive-by, son ataques que buscan las vulnerabilidades en los sistemas que en un momento dado la organización ha anunciado y se activan cuando se accede a ciertos sitios webs y buscan un beneficio económico.

- Exploits-kits, es un ataque automático que al igual que el anterior explota las vulnerabilidades del sistema para su beneficio propio.

- Herramientas de administración remota (RAT), los atacantes aprovechan fallos en esta herramienta que les permite acceder al sistema deseado.

7. Criptojacking. Durante el 2018 se han detectado un aumento de ciberataque hacia las criptomonedas. La técnica consiste en obtener el beneficio a partir de la creación de la moneda.

   Como se puede ver en la siguiente figura el aumento de este tipo de técnicas ha ido aumentando exponencialmente.

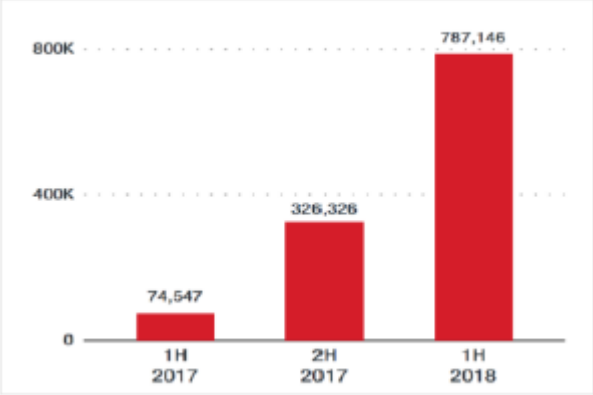

Figura 2: Evolución semestral de los Criptojacking

Fuente: Ciberamenazas y tendencias. Edición 2019. Centro Criptológico Nacional.

Hay que tener en cuenta aunque estos ataques en líneas generales están realizados por entidades externas a las compañías, puede ser que también se realicen por actores internos de las mismas.

8. Robo de identidad. Este ataque consiste en robar información personal de manera masiva, como cuentas bancarias, domicilio o registros contables. Está muy relacionado con los robos de datos de corporaciones.

   El nuevo Reglamento General de Datos (GDPR) de la Unión Europea, que posteriormente se explicará, define las normas que deben seguir los propietarios de información personal de terceros para la protección de los mismos. Entre las medidas se encuentra el cifrado de datos. El incumpliendo de estas normas puede llevar sanciones bastante elevadas.

9. Ataques basados en web. Este tipo de ataque compromete la explotación de navegadores a través del control del sistema informático. Durante el 2018, fue una de las amenazas más usadas. El objetivo principal de estos ataques es la obtención de información.

   Dentro de este ataque destaca el conocido como Man-in-the- middle que son ataques de espionaje, en este caso los atacantes interrumpen los flujos de información entre emisor y receptor para filtrar y robar la información. Una de las formas más fáciles de ataque es a través de las redes Wi-fi, cuando la víctima se conecta es el momento en el cuál el atacante aprovecha para introducirse en el dispositivo de la víctima y robar la información que necesite.

10. Ataques DDoS. Cuando algún sistema está dañado por este ataque no permite hacer las operaciones que habitualmente se realiza con ese sistema, por ese motivo a este ataque también se le conoce como ataques de denegación de un servicio.

    Es de los ataques más populares que se han realizado durante el 2018. Debido a esto, las organizaciones, sobre todo las relacionadas con el sector financiero, están invirtiendo para cubrirse de este ataque.

11. Botnets. El uso de esta herramienta permite el acceso a los sistemas informáticos de varias víctimas simultáneamente, para robar datos relevantes para las organizaciones.

Ha sido una de los ataques más usados durante el 2018, su objetivo ha sido principalmente el robo de información, ataques de denegación (DDoS) y el envío de correos electrónicos no deseados para otros usos.

12. Criptografía. En los últimos años se ha utilizado la criptografía como medida de seguridad para los sistemas informáticos. Como medida de seguridad impide que los atacantes, en el caso de que sean capaces de acceder al sistema, puedan obtener los datos que les interesen en su totalidad.

    Pero lo que no impide es que si los atacantes tienen acceso a la red puedan obtener información a través del análisis del comportamiento del equipo, como el uso de baterías, el tiempo que utiliza para hacer alguna tarea, etc. A estos ataques se les conoce como canal lateral.

    Y en los últimos años para realizar este ataque se están empezando a utilizar el machine learning como técnica para recolectar el comportamiento de un equipo.

13. Para finalizar, hay que mencionar la Ingeniería Social, que es una técnica cada vez más común que utilizan los ciberatacantes para conseguir sus objetivos. Es un conjunto de técnicas y habilidades sociales que los atacantes realizan para obtener cierta información útil para acceder a los sistemas informáticos. Hay distintos tipos según el nivel de interacción:

    - Pasivo, esta técnica consistiría en conseguir información a través de técnicas poco directas como la observación.
    - No presencial, consistiría en obtener información obteniendo la contraseña, accediendo al teléfono, cartas o chats.
    - Presenciales, consistiría en técnicas más directas para recopilar la información como buscar en la basura, mirar por encima del hombro, vigilar los edificios, etc.
    - Agresivo, está sería la más directa y recoge técnicas como la suplantación de identidad o el chantaje.

2.2 ¿QUIÉN REALIZA LOS ATAQUES?

En este apartado se mencionará los principales agentes de las amenazas cibernéticas a las que las organizaciones se tienen que enfrentar, es decir, qué grupos realizan los ataques cibernéticos.

En primer lugar, nos encontramos con los Estados, estos lanzan código dañino para explorar las vulnerabilidades de los sistemas de información de las estructuras críticas. Estos ataques se han detectado principalmente hacia objetivos europeos.

Su objetivo fundamental es conseguir información sobre las medidas de seguridad que tienen implantadas otras organizaciones.

También nos encontramos con los ciberdelincuentes, que es uno de los grupos con más actividad durante el 2018. Dirigen principalmente sus ataques a empresas, bancos e instituciones financieras.

Los métodos que más utilizan son los ciberataques a través de correos electrónicos o el phising, aunque hay que decir que esta última técnica se ha ido sofisticando a través de la ingeniería social y las innovaciones en la automatización.

Otros de los impulsores de las ciberamenazas es el ciberterrorismo, durante el 2018 no se ha encontrado ningún ataque destacable relacionado con grupos cuyos ataques tienen una motivación religiosa.

Pese a esto, los individuos que pertenecen a un grupo terrorista siguen utilizando las tecnologías legítimas, como las redes sociales que tienen a su alcance para obtener fondos o captar a gente nueva.

Los activistas son otro grupo que se dedican a la destrucción de páginas web, ataques DDoS y divulgación de información crítica para la corporación dañada.

Su objetivo principal es llamar la atención y reivindicar sus ideas. A diferencia de otros grupos, en líneas generales no busca obtener un beneficio económico por sus acciones.

Y, por último no nos podemos olvidar de los actores internos, este grupo lo forman personas que son usuarios de los sistemas de información o proveedores que de una forma negligente o premeditada abren una vía para que los ciberatacantes puedan acceder al sistema.

El motivo principal por el que se realiza este tipo de acciones es el beneficio económico. Aunque, como ya se ha mencionado antes, en ocasiones estos actos se ocasionan de forma negligente por parte de los propios empleados de la compañía los cuales no buscan ninguna recompensa.

2.3 TENDENCIAS DE LOS CIBERATAQUES Y DE LA CIBERSEGURIDAD.

Una vez analizadas las amenazas más comunes que se han dado durante el 2018 y los propulsores de las mismas, a continuación se va a explicar las tendencias en ciberataques y en ciberseguridad que se espera que se vayan a originar en los próximos años.

Si nos centramos en los ciberataques:

Es previsible que los ataques realizados por los Estados aumenten, estos podrían ser de todas las intensidades y muy probablemente se realicen en forma de advertencia hacia otros Estados o corporaciones.

Esto va a ser posible debido a la gran dependencia que tienen los sistemas de información a internet, siendo fundamental para el desarrollo de cualquier actividad. Con las nuevas tecnologías, esta dependencia se convierte en un posible ataque.

También se va a poder seguir viendo ataques dirigidos a cadenas de suministros, ya que los atacantes se están dando cuenta que la forma más fácil de atacar a grandes corporaciones es a través de sus proveedores.

Muchas organizaciones, siendo conscientes de su dependencia con sus proveedores y la amenaza que esto supone están empezando a gestionar este riesgo.

Por otra parte, se prevé que los atacantes modernicen sus ataques realizados con código dañino para que sean más eficientes, haciendo que sean más difíciles de detectar. Y, aumentará el uso de los ataques persistentes avanzados (APT).

También se cree que a medida que se vaya protegiendo los sistemas de una forma más eficiente, los atacantes se centraran en el eslabón más débil y aumentarán los ataques dirigidos a las personas, como el envío de correos electrónicos.

Aunque ya se están empezando a realizar ataques de criptojacking se espera que en los próximos años estos ataques aumenten. La técnica consiste en que los atacantes a través de código dañino toman el control de ordenadores para controlar esta moneda.

Si nos centramos más en la ciberseguridad:

Se prevé que el Consejo de Administración de las organizaciones vayan tomando conciencia de los problemas que suponen los ciberataques y que la mitigación de este riesgo y su gestión sean uno de los principales temas que se aborden en las juntas de dirección.

Siguiendo con las tendencias en seguridad, es previsible que las empresas más pequeñas empiecen a introducir las medidas en ciberseguridad que aplican las empresas de un mayor tamaño.

Este cambio se va a empezar a realizar por dos motivos principales, en primer lugar, tanto las empresas pequeñas como las grandes están expuestas a los mismos riesgos. Y también este cambio se debe a que el resto de empresas, clientes o proveedores van a exigir tanto a las pequeñas como a las grandes empresas garantías de ciberseguridad.

Por otro lado, se está empezando a utilizar las herramientas de machine learning que automatizan la detención y el bloqueo de las amenazas detectadas dentro de los sistemas. Esta técnica será fundamental para aquellas amenazas que intentan ocultarse dentro del sistema.

Se prevé que se siga aprobando nuevas normativas y legislaciones. La llegada de la ley de protección de datos implantada por la Unión Europea, de la que se hablará posteriormente, ha motivado que países de fuera de Europa empiecen implantar una normativa similar.

Es el caso de Canadá o Australia que han implantado una legislación similar a la europea o el caso de Brasil que lo empezará a implantar a partir del 2020.

Y para terminar, es necesario mencionar una nueva técnica que se va a ir implantando tanto para el envío de la amenaza como para la protección ante la misma. Esta nueva técnica es la inteligencia artificial.

Los atacantes lo utilizarán para conocer de una forma sencilla y rápida las debilidades en el sistema de sus objetivos. Por otro lado, las organizaciones lo empiezan a utilizarán para identificas las nuevas amenazas.

3. RIESGO CIBERNÉTICO.

Tanto los ciberataques como la ciberseguridad, suponen un coste económico y reputacional para las empresas, fundamentalmente las financieras. Para poder medir el alcanza, el impacto y predecir las pérdidas que tiene esta amenaza las organizaciones engloban lo anteriormente mencionado en el riesgo cibernético.

El riesgo cibernético es la posibilidad de pérdida tanto financiera como no financiera provocada por los posibles eventos digitales causados por agentes internos o externos a la compañía. Entre los eventos destaca el robo y el daño de información esencial para la empresa o la interrupción del negocio. Este riesgo se considera que es un tipo de riesgo tecnológico y está englobado en el riesgo operacional.

A continuación, se abordará con más profundidad el riesgo operacional centrándonos en las entidades bancarias, ya que estas organizaciones son más propensas a sufrir un ataque cibernético debido a la cantidad de información confidencial de la que disponen. Además, de que tienen una normativa más restrictiva para gestionar los riesgos que el resto de empresas.

Durante el 2019 se ha observado que una de las principales necesidades en las entidades financieras en relación con el riesgo operacional es la necesidad de adaptarse a las nuevas tecnologías y los avances digitales. Hay que mencionar que este riesgo está presente no solo de forma individual sino que afecta a otros riesgos operacionales. Y se ha convertido en la primera preocupación en relación a los riesgos operacionales.

3.1 ¿QUÉ ES RIESGO OPERACIONAL?

Seguidamente se va a pasar a definir qué es el riesgo operacional, este es un riesgo propio de cualquier negocio y afecta a todas las dimensiones de la entidad. Consiste en la posibilidad de pérdidas resultantes de una falta de adecuación o de fallo en los procesos, el personal, los sistemas internos o acontecimientos externos.

La preocupación por este riesgo ha crecido en los últimos años tanto para las entidades financieras como para los supervisores, principalmente porque se ha visto que es un riesgo que ha ido aumentando en los últimos años.

Es por ello, que ya en el acuerdo de capitales de Basilea II se reconoce que las entidades de crédito no sólo se ven afectadas por el riesgo de crédito o de mercado, sino por muchos otros como el riesgo de liquidez o el operativo.

Basilea II se divide en tres pilares:

1. Pilar I. Requerimiento de mínimo de Capital. Es una cuantía mínima que las entidades tienen que tener para cubrir su riesgo tanto de crédito de mercado y operacional. Estos se obtienen de forma ponderada a partir de la exposición que tenga la entidad a estos riesgos.

   En el caso del riesgo operacional, se introducen tres métodos de medición de este riesgo que buscan que las entidades desarrollen un sistema más avanzado en la gestión y el requerimiento mínimo de capital en función de sus estrategias, necesidades y perfiles de riesgos.

2. Pilar II. Autoevaluación. Se establece un proceso de autoevaluación del capital necesario, tanto para su asignación interna, como la revisión del proceso por el supervisor.

3. Pilar III. Disciplina de mercado, Busca que a través de la transparencia en la información que facilita las entidades, que la acción del libre mercado se convierta en un elemento externo incentivador que complete las acciones llevadas en el Pilar I y Pilar II.

Hay tres métodos para el cálculo de los requerimientos de capital para el riesgo operacional, estos son: Método del Indicador Básico (BIA); Método Estándar (SA); Método de Medición Avanzada (AMA). También se está promoviendo un nuevo método con el que se quiere empezar a sustituir a los demás, este es el nuevo método estándar (SMA).

Estos métodos clasifican las pérdidas ocasionadas por un riesgo operacional según el evento que haya ocurrido. Los tipos de eventos que se reconocen son:

- Fraude interno; es la pérdida ocasionada por cometer un fraude, apropiarse de bienes o evitar el cumplimiento de la legislación vigente realizado por cualquier empleado de la entidad.

- Fraude externo; es muy similar a la anterior con la diferencia que en esta ocasión la acción está realizada por alguien ajeno a la organización.

- Relaciones laborales y seguridad en el puesto de trabajo; pérdida provocada por hechos contrarios a la ley, acuerdos laborales o seguridad en el trabajo. También se encuentran las reclamaciones por daños personales, incluidas las relacionadas con casos de acoso.

- Clientes, productos y prácticas empresariales; pérdida obtenida por no haber cumplido las obligaciones acordadas con un cliente.

- Daños a activos materiales; pérdidas ocasionadas por daños en activos materiales provocados por desastres naturales u otros eventos.

- Incidencias en el negocio y fallos en el sistema; pérdida derivada de fallos en los sistemas o incidencias en el negocio.

- Ejecución, entrega y gestión de procesos; pérdidas obtenidas por errores en el procedimiento de alguna operación o en la gestión de procesos.

Hay que mencionar que los eventos tienen dos partes, la frecuencia y la severidad. La frecuencia es las veces que ocurre un evento y la severidad la pérdida que se tiene cuando este evento ocurre. Lo normal es que las empresas tengan eventos de mucha frecuencia pero poca severidad pero puede ocurrir que tengan eventos que tengan poca frecuencia pero mucha severidad.

Cabe destacar que la frecuencia de los eventos y la severidad de los mismos tiene una relación inversa, cuanto más frecuente es un evento menos severidad tiene, por lo tanto, las empresas deberían centrarse más en los eventos que tienen poca frecuencia pero mucha relevancia porque son los que si en un momento dado ocurren comprometerían la continuidad de la entidad.

Por otro lado, para poder utilizar estos métodos se debe dividir la actividad en líneas de negocios:

a. Financiación empresarial; engloba servicios relacionados con las operaciones de suscripción, asesoramiento en inversiones, estrategia industrial, asesoramiento en fusiones o adquisiciones y análisis financiero.

b. Negociación y ventas; está línea de negocio se encarga de la negociación por cuenta propia, intermediación en los mercados, recepción de órdenes de clientes, ejecución de órdenes en manos de clientes y gestión de sistemas multilaterales de negociación.

c. Intermediación minorista; en este caso, se realizaría las mismas operaciones que en el apartado anterior, siempre que sean operaciones realizadas por pymes o personas físicas.

d. Banca comercial; engloba actividades relacionadas con la concesión de préstamos, arrendamientos financieros, garantías personales y aceptación de depósitos.

e. Banca minorista; esta línea de negocio es igual que la anterior con la diferencia de que está orientado exclusivamente hacia pymes o personas físicas.

f. Pago y liquidación; se encuentran recogidas actividades tales como operaciones de pago, emisión y administración de medios de pago.

g. Servicios de agencia; en este apartado podemos observar actividades de administración de instrumentos financieros por cuenta de cliente y servicios conexos como la gestión de efectivo y de garantías.

h. Gestión comercial; en esta línea de negocio se engloba todas las actividades de gestión de activos.

Una buena gestión del riesgo operacional que permita controlar el mismo se divide en cuatro fases. Estas son:

1. Identificación; esta fase consiste en encontrar las vulnerabilidades de la compañía y conocer qué partes de la compañía tienen más exposición al riesgo.

Para ello, se crea un mapa de procesos, riesgos y controles dónde se recoge la exposición total que tiene la compañía al riesgo operacional.

Posteriormente, se tiene que implantar un mecanismo de evaluación de los riesgos, para obtener periódicamente el impacto y la frecuencia de los riesgos a los que se está expuesto.

Y por último, realizaría un plan de acción dónde se intenta identificar las mejoras que se puedan realizar para mejorar la eficiencia de los procesos y tomar medidas para mejorar los resultados obtenidos.

2. Medición. En esta fase se realizarían los métodos para el cálculo del capital que se han mencionado anteriormente.

3. Control y seguimiento. Aquí se intentará hacer un seguimiento de cómo evoluciona la exposición al riesgo operacional, para conseguirlo se realizan los KRIs o los indicadores clave de riesgos.

   Y por otro lado, se registra los eventos de pérdida que han ocurrido en un periodo de tiempo para analizarlas, hacer un seguimiento de las mismas y controlarlas de tal forma que no vuelvan a ocurrir.

4. Mitigación. En esta fase se planeará cómo va a organizarse la corporación en el caso de que se produzca un evento de riesgo operacional que suponga pérdidas a la compañía.

   Principalmente hay dos planes que la compañía crea:

   - Plan de contingencia: se recoge las acciones y los recursos que se van a emplear en el caso de que se produzca algún evento.

   - Plan de continuidad de negocio: engloba las medidas, los recursos y los procedimientos para que en caso de que se produzca un evento la compañía pueda volver con su actividad habitual lo antes posible.

3.2 SITUACIÓN ACTUAL DEL RIESGO OPERACIONAL

Una de las partes cruciales a la hora de gestionar cualquier riesgo es su identificación y en el caso del riesgo operacional es una de las partes más complicadas a las que se enfrenta las entidades bancarias, es por ello que O.R.X crea el informe de Horizonte de Riesgo operacional[2], intentando dar luz sobre este tema. En este informe se analizan 377 riesgos operacionales y 282 riesgos emergentes.

Hay que aclarar que O.R.X es una plataforma creada para facilitar el intercambio de datos de riesgo operacional entre entidades bancarias. En su base de datos se recogen los eventos de pérdida operacional entre las empresas de servicios financieros. Actualmente está recogido 630.000 eventos de 96 bancos y recoge unas pérdidas de 400 mil millones de euros.

Lo primero que hay que mencionar que el riesgo operacional es un riesgo que engloba otros muchos que son muy distintos entre sí y que la amenaza va cambiando según va pasando el tiempo, por lo tanto las entidades bancarias tienen que ir mejorando su gestión constantemente para cubrir su riesgo operacional.

En los últimos años, el riesgo operacional está cada vez más en auge, convirtiéndose en una de las partes más importantes del perfil de riesgo de las entidades y se prevé que las categorías de riesgo van a ir aumentando en los próximos tres años.

Todo este cambio se debe en gran medida a los cambios tecnológicos y todos los riesgos asociados al mismo, como el riesgo en las infraestructuras de TI, seguridad informática, digitalización, etc. Aunque también hay que destacar que el cumplimiento normativo ocupa otra de las grandes preocupaciones de las entidades.

Dentro de la clasificación de los riesgos operacionales del informe, aparecen dos tipos los riesgos operacionales y los riesgos operacionales emergentes.

Los riesgos operaciones más importantes ordenados según importancia son:

[2] Datos obtenidos de: O.R.X. (2018). *Operational Risk Horizon2018.* Recuperado el 15 de julio del 2019 en: https://managingrisktogether.orx.org/research/operational-risk-horizon-2018

1. Riesgo conductual; consiste en que las entidades abusen de su situación de poder y se aprovechen de sus clientes.

2. Seguridad de la información y el riesgo cibernético; amenaza de ataques cibernéticos que aumenten la creciente dependencia de las entidades en los datos y tecnologías de la información.

3. Robo y Fraude; como su nombre indica son los robos y fraudes de individuos tanto internos como externos de la entidad.

4. Infraestructura de IT; gran dependencia a la tecnología antigua que no cubre las necesidades reales del mercado en el que se mueve las tecnologías.

5. Cumplimiento normativo; son las dificultades que pasan las entidades para cumplir con las exigencias normativas vigentes.

Como se puede observar el riesgo cibernético y la estructura IT son dos de los riesgos más importante, principalmente el riesgo cibernético que se queda en segundo lugar pero siguiendo muy cerca al riesgo conductual.

Se piensa que esto en los próximos tres años vaya cambiando ya la que la previsión es que los riesgos cibernéticos y la estructura IT sigan aumentando mientras que los riesgos conductuales se mantengan estables.

Los riesgos operaciones emergentes más importantes ordenados según importancia son:

1. Digitalización y desintermediación; es la posible pérdida por invertir en nuevas tecnologías e intentar adaptarse las constantes actualizaciones tecnológicas.

2. Riesgo cibernético.

3. Cumplimiento normativo.

4. Riesgo geopolítico; es la exposición que tienen las entidades ante cambios de gobierno o implantación de nuevas medidas.

5. Seguridad de la información y riesgo conductual.

Como se puede ver dentro de los riesgos emergentes las entidades centran su reputación en lo relacionado con la tecnología, la digitalización y el riesgo cibernético, que aunque ya en el 2016 resaltaban dentro de los riesgos cada vez están cogiendo más importancia y por otro lado las tensiones geopolíticas también están causando grandes preocupaciones.

Estas nuevas tendencias han hecho que aparezcan nuevas formas de amenaza y que aumente de esta forma las posibles pérdidas financieras y reputacionales. Creando la necesidad a las entidades de crear nuevos sistemas e implantar nuevas medidas para adaptarse, creando de esta manera nuevas exposiciones al riesgo.

3.3 PÉRDIDAS ACTUALES DEL RIESGO OPERACIONAL

Para tener una idea global del riesgo operativo es fundamental centrarnos en las pérdidas que ha ocasionado este riesgo a las entidades bancarias. Es por ello, que se ha seleccionado un informe de O.R.X[3] dónde se recoge las tendencias de pérdidas por riesgo operacional de 86 bancos entre el 2012 y el 2017 ambos incluidos.

Hay que aclarar que las pérdidas recogidas son a partir de 20.000 euros. Lo eventos se clasifican por el tipo de actividad, tipo de evento y la región.

Entre los años que analiza este informe, se han recogido un total de 358.669 eventos, con una pérdida bruta de 170.000 mil millones de euros. Aunque hay que destacar que a partir del 2008 y hasta el fin del estudio las pérdidas han ido disminuyendo paulatinamente.

El tamaño medio de un evento de pérdida en el 2017 es de 206.426 euros y en el 2012 era de 664.510 euros, muestra de que según ha ido pasando los años se ha ido reduciendo las pérdidas operacionales en la industria bancaria. Pero hay que mencionar que los eventos de pérdida se han mantenido constantes durante todo este tiempo, entorno a unos 60.000 eventos al año.

[3] Datos obtenidos de: O.R.X (2018). *Annual Banking Loss Report. Operational risk loss data for banks submitted between 2012 and 2017*. Recuperado el 2 de julio del 2019 en: https://managingrisktogether.orx.org/orx-loss-data/annual-banking-loss-report

Del informe podemos concluir que es la banca minorista dónde más eventos de pérdidas recoge dentro de las líneas de negocio de las entidades, provocado principalmente por el fraude externo, aunque también es muy importante la gestión de procesos.

En cambio, la pérdida bruta es más abundante para el tipo evento que está relacionado con el cliente para todas las líneas de negocio. Y llama la atención que entre los eventos que menos pérdida bruta reporta se encuentra el fraude interno.

Analizando en más profundidad la pérdida bruta, podemos decir que en el 2012 triplica la pérdida del 2017, aunque el número de eventos se mantienen igual, tal y como podemos ver en las figuras siguientes.

Year	Average loss size
2012	€664,510
2013	€522,309
2014	€575,407
2015	€465,502
2016	€422,783
2017	€206,426

Figura 3: Pérdida bruta entre 2012 y 2017.

Fuente: Annual Banking Loss Report. June 2018. O.R.X.

Year	Total number of reported events
2012	54,854
2013	59,773
2014	61,753
2015	64,195
2016	61,984
2017	56,110

Figura 4: Eventos entre 2012 y 2017.

Fuente: Annual Banking Loss Report. June 2018. O.R.X.

Al hacer un análisis trimestral, vemos que los eventos operacionales son bastante irregulares de un trimestre a otro, tienen una gran volatilidad, aunque hay que mencionar que estos picos de volatilidad se ven claramente entre el 2012 y el 2016, durante el 2017 la situación se estabiliza bastante. Como podemos observar en la siguiente figura.

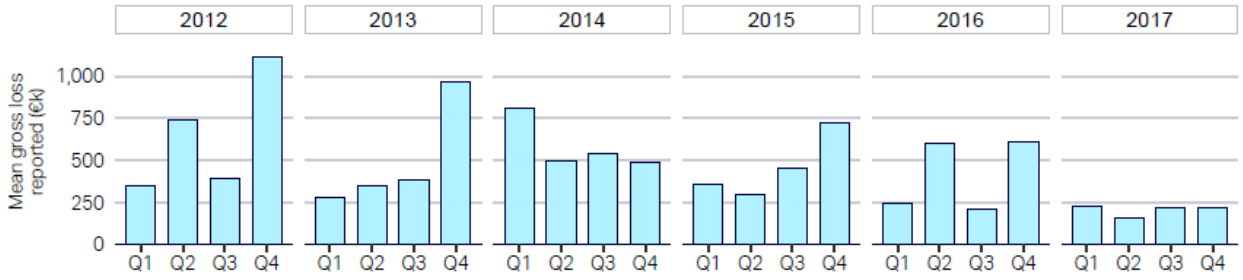

Figura 5: Pérdida bruta media entre 2012 y 2017.

Fuente: Annual Banking Loss Report. June 2018. O.R.X.

Como modo de conclusión se puede decir que durante los años del estudio, las entidades de crédito han ido estabilizando y reduciendo sus pérdidas paulatinamente, aunque los eventos a los que se han tenido que enfrentar no se han reducido. Por lo tanto, durante estos años las entidades han ido gestionando de una forma más adecuada el riesgo operacional al que se enfrentaban las entidades bancarias.

4. CIBERSEGURIDAD EN LAS EMPRESAS.

A pesar de las constantes inversiones en tecnología de seguridad cibernéticas, las amenazas cibernéticas están muy presentes en el día a día de las empresas y siguen siendo muy vulnerables a las mismas.

Por eso es necesario que las empresas centren sus esfuerzos en crear unas medidas de seguridad adecuadas para el nivel de riesgo al que se expone. En este apartado del trabajo es lo que se va a intentar abordar.

En la actualidad, los ciberataques representan un coste mundial cercano a los 600.000 millones de dólares. Esto se debe principalmente a la rapidez y facilidad con las que los ciberdelincuentes utilizan las nuevas tecnologías. También, al haber muchas más personas utilizando las tecnologías que tienen a su disposición brindan una ayuda a los atacantes para poder lanzar sus amenazas. Y por último, las nuevas técnicas ya mencionadas como el criptojacking, facilita, a los ciberdelincuentes, enormemente la obtención de beneficios con los ataques que realizan.

Por otro lado, en necesario añadir que los sistemas están cada vez más interconectados, hay más información fundamental para las empresas que no está controlada por ellas ya que la gestionan los propios empleados o terceros ajenos a las compañías, haciendo muy difícil la protección total de los mismos. Además, el uso de sistemas en la nube o servicios compartidos hace que los servicios estén fragmentados en sistemas dependientes uno de otros.

Por otro lado, cada uno de estos sistemas utiliza una metodología de protección diferente provocando que sea muy difícil tener un control adecuado y global de la seguridad.

4.1 CIBER-SEGURIDAD EN LAS EMPRESAS.[4]

El mundo empresarial aún está en el camino de abordar de una manera correcta los problemas relacionados con la ciberseguridad, este hecho hace que sea muy difícil que las compañías adopten una buena estrategia cibernética.

[4] Datos obtenidos en su mayoría de: Deloitte. *Beneath the surfaces of a cyberattack. A deeper look at business impacts.* Recuperado el 4 de abril del 2019 en: https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

Esto se ve claramente en cómo las empresas miden los riesgos y el impacto que tendría un ataque cibernético, ya que muchas veces las compañías solo se centran en el coste directo asociado a este, cuando también deberían prestar atención a los costes intangibles que están relacionados con estos ataques.

También deberían centrarse en cómo les va a afectar a medio y largo plazo un ataque y no quedarse solo con el impacto a corto plazo ya que muchos problemas derivados de un ciberataque solo se pueden observar cuando haya pasado un periodo de tiempo.

Por todo ello, cada vez las compañías están dando mayor importancia a la seguridad cibernética, intentando desarrollar una mayor capacidad de reacción en el caso de que haya un incidente cibernético.

Para poder realizar la defensa correctamente, en primer lugar las entidades tienen que estudiar los tipos de riesgos cibernéticos a los que se enfrentan y saber medir cuál es la probabilidad de que los mismos sucedan. Y por último, medir los impactos que pueden tener en el desarrollo de la actividad principal de la compañía. Para ello, se necesita tener un conocimiento amplio del modelo de negocio de la compañía, el nivel de madurez, la vulnerabilidad de la compañía, su presencia en el sector, etc.

A simple vista, se puede pensar que el principal impacto que puede tener una compañía ante un ataque cibernético es el robo de información de identificación personal y los costes relacionados con la notificación al cliente, junto con la posibilidad de enfrentarse a juicios y sanciones.

Pero hay que tener en cuenta que quizás el objetivo del ataque es otro como por ejemplo el robo de la propiedad intelectual, espionaje o la destrucción de datos y estos ataques pueden tener un mayor impacto que el anterior aunque sean más difíciles de medir.

Hay muchas formas de que un ataque cibernético impacte dentro de la compañía, pero se han identificado 14 impactos con los que la compañía tiene que trabajar para garantizar la seguridad de la compañía ante una posible amenaza cibernética.

Estos factores de impacto están presentes durante el tiempo que dura la respuesta de la compañía ante un ciberataque. La respuesta se puede dividir en tres fases y los impactos pueden aparecer en solo una de las fases o varias veces a lo largo de todo el proceso de respuesta de la compañía.

Las tres fases en las que se divide la respuesta ante el incidente son:

1. Triaje del incidente: Esta fase ocurre justo días después del ataque, es dónde se toman las decisiones de acción a corto plazo, se decide la forma de comunicarlo al exterior de la compañía, se crea una estrategia para garantizar la continuidad del negocio y se hace un análisis de lo ocurrido.

2. Gestión del impacto: Esta fase ocurre meses semanas después del ataque y consiste en hacer frente a las consecuencias más visibles y palpables del incidente. Reducir el daño con clientes, ajustar el proceso operativo a las necesidades de la compañía, realizar auditorías internas para comprobar la seguridad implantada y empezar con los procesos legales ligados con el ataque.

3. Recuperación del negocio: Esta fase se empieza a realizar meses después del ataque, se basa en reparar los daños causados a la compañía por el ataque y prevenir que vuelva a pasar. Incluye actividades como rediseñar los procesos del negocio, desarrollo de estrategias para mejorar la reputación y mejorar la seguridad y los sistemas de detención.

Cada uno de los catorce impactos tiene que ser enfocados de una determinada manera para estimar correctamente los costes. Principalmente se dividen en dos grandes grupos, los que se encuentran “sobre la superficie”, son los costes más tangibles y son más fáciles de calcular y los que se encuentran “bajo la superficie”, son los costes intangibles y más difíciles de cuantificar.

Los catorce impactos de un ciberataque son:

- SOBRE LA SUPERFICIE

a) Investigación técnica. Se encuentran los costes vinculados a esclarecer el motivo del ataque y ver qué parte de la organización ha fallado para poder localizar a los culpables.

b) Notificación al cliente del ataque. Se recogen todos los costes asociados con la comunicación del ataque a los clientes que se hayan visto perjudicados por el mismo.

c) Protección posterior al ataque del cliente. Son los gastos asociados con la detención de los daños sufridos y el intento de protección de los datos.

d) Cumplimiento normativo. Son las multas y las sanciones que la compañía tiene que pagar por haber sido atacada e incumplir la normativa de protección de datos entre otras.

e) Relaciones públicas. Son los costes asociados a la comunicación del daño cibernético a los agentes externos a la compañía.

f) Pago de abogados y litigios. Los gastos del asesoramiento jurídico y de empezar con las acciones legales para defender los intereses de la compañía.

g) Mejoras en la seguridad cibernética. Engloba los costes asociados al invertir en la mejora de controles de seguridad para evitar que vuelva a realizarse un ataque y la vuelta a la actividad habitual.

- BAJO LA SUPERFICIE

h) Aumento de los costes, prima de seguros. Al haber sufrido un ataque las pólizas de seguro asociado al riesgo cibernético aumenta.

i) Aumento del coste al aumentar la deuda. Al haber sufrido un ataque cibernético aumenta el riesgo de la continuidad del negocio, por lo tanto, se asocia a las empresas mayor riesgo de crédito y por lo tanto el tipo de interés asociado a los créditos y préstamos de la empresa aumentan.

j) Impacto de la interrupción de la actividad. Se asocian todos los costes que se va a tener que enfrentar la compañía al verse modificada su actividad habitual, al igual que los costes para volver a poner la actividad en marcha.

k) Pérdida de valor en las relaciones con los clientes. Se intenta cuantificar cuántos clientes se han perdido debido al ataque cibernético.

l) Devaluación del nombre comercial. Se intenta cuantificar la pérdida causada por la pérdida de reputación de la compañía, debido entre otras razones a que los ciberataques están teniendo más repercusión en los medios de comunicación.

m) Valor de las pérdidas por perder algún contrato. Se incluye la pérdida ocasionada por ingresos futuros que debido al ataque no se va a poder obtener y también la pérdida de oportunidades de negocio provocada por el ataque.

   Engloba el coste de oportunidad por no poder seguir con el negocio habitual después de un ataque, la reducción de producción y del valor de la compañía.

n) Pérdida de la propiedad intelectual. Es el coste asociado con la pérdida de control de cierta información como los derechos de autor, planes de inversión e información confidencial que pueden perjudicar a la rentabilidad de la empresa.

4.2 PROBLEMAS DE LA CIBERSEGURIDAD EN LAS EMPRESAS.

La única manera que tienen las organizaciones de defenderse frente a los ataques es incorporando medidas de seguridad adecuadas. Para poder cubrirse de una amenaza correctamente se deberá anticiparse a los ataques antes de que sucedan y poder planificar una estrategia a la altura de la amenaza.

Las organizaciones deben desarrollar una conciencia de su vulnerabilidad, que proporcionará una evidencia perceptible de las implicaciones del ataque y luego probar la eficacia de las medidas que se adoptan. Desgraciadamente la asignación de recursos solamente se produce, en la mayoría de las organizaciones, cuando una violación grave de seguridad ya se ha producido.

En los últimos años el método más rápido y rentable es la de subcontratar gran pate de la complejidad de la gestión de seguridad cibernética en un proveedor de servicios de seguridad.

También hay que añadir que no se da demasiada importancia al desarrollo de software seguros, ni a tener la última actualización de los software. En muchos casos, los planes de acción y los programas utilizados son antiguos y por lo tanto no protegen a los sistemas de los nuevos ataques. E incluso en

ocasiones las organizaciones no implementan las medidas mínimas que hubieran podido protegerlas de un ataque o reducir el impacto del mismo.

Otro problema al que se tienen que enfrentar las organizaciones es que no se dispone de suficiente información sobre los ciberataques y es por ello que se hace muy difícil crear un sistema de seguridad adecuado para gestionar este riesgo. Muchos de ellos ni si quiera están recogidos en la legislación vigente a nivel mundial.

Por este motivo y en líneas generales, las empresas solo se centran en amenazas ya ocurridas o se centran en las que son más comunes. De esta forma, sobrestiman su seguridad ante un ataque, no tienen en cuenta muchos fallos de la seguridad ni tampoco las posibles pérdidas tanto a corto como a largo plazo.

Según un artículo publicado en The Economist [5] una empresa tarda alrededor de 205 días en darse cuenta que se ha sido atacada, dejando un periodo de tiempo muy elevado para que los atacantes puedan infectar a otras entidades, poniendo en peligro a todo el sector. Esto demuestra que las pruebas de intrusión son muy importantes para intentar detectar cuánto antes un ataque y evitar el robo de información y que las medidas de seguridad puede que no estén bien implementadas.

En el 2016 salió a la luz que en los últimos meses habían aumentado los ataques, aunque hay que decidir que del número total de ataques solo el 20% ha conseguido robar fondos.

Y desde ahí, en los últimos años, ha habido un aumento de los mismos, sustrayendo mucha información confidencial de las empresas ocasionado pérdidas y pasando esta información y el conocimiento técnico a otras empresas o incluso a otros países.

Los principales problemas para la empresa con los ciberataques son:

- Los ciberataques pueden causar daño a cualquier escala y a cualquier lugar del mundo.
- Sin contar que el ataque se puede hacer desde cualquier parte del mundo lo que proporciona cierta ventaja a los ciberatacantes.

[5] Información obtenida de: Economist (2015). *The cost of inmaturity* . Recuperado el 18 de julio del 2019 en: https://www.economist.com/business/2015/11/05/the-cost-of-immaturity

- No se necesita para ejecutar el ataque ningún material muy técnico salvo acceso a internet y un ordenador por lo que cualquiera lo podría realizar.

- Tiene una gran repercusión social y los medios de comunicación dan mucho eco a los mismos.

- Pueden aparecer de diferentes maneras, haciendo muy difícil su detención.

Aunque si se llega a estimar las pérdidas ocasionadas por un ciberataque, es muy complicado calcular las pérdidas reales ocasionadas, ya que hay que tener en cuenta muchas cosas a la vez como los daños colaterales, la vuelta en marcha de la actividad, trabajar para que los medios de información se enteren lo más tarde posible, etc.

4.3 CIBERSEGURIDAD Y LA JUNTA DE DIRECCIÓN.

Las empresas cada vez están más digitalizadas y tienen una mayor dependencia tecnológica, siendo un rasgo diferenciador entre las empresas que están ya digitalizadas y las empresas que comienza con la digitalización. Debido a la dependencia tecnología que las nuevas tecnologías han creado es más fácil sufrir un ciberataque en todas las compañías.

Por otro lado, aunque la seguridad de los datos es algo fundamental, también es necesario tomar medidas para poder continuar con las operaciones normales del negocio ya que en el caso de que una entidad fuera atacada su actividad se paralizaría.

Todas las medidas que se van a realizar para la protección de la entidad antes los ciberataques tienen que estar alineadas con la tolerancia al riesgo de la empresa y los objetivos estratégicos de la misma.

El buen funcionamiento de la ciberseguridad se basa en tres pilares fundamentales: personas, procesos y tecnología. Aunque las medidas tecnológicas son clave también es fundamental que las personas que trabajan y los procesos estén alineados.

No sirve de nada cumplir con las restricciones legales que hay si luego no se aplican en el día a día de la compañía. Además, todos los empleados tienen que tomar conciencia del peligro que supone

ser atacados cibernéticamente ya que cualquier puesto que esté conectado con el exterior supone una amenaza.

Es por todo ello fundamental, que las juntas de dirección empiecen a tomar conciencia de las complicaciones derivados de los ciberataques y comiencen a abordarlo como uno de los problemas principales a los que se tiene que enfrentar una compañía en la actualidad.

Según un estudio realizado por EY, el problema de la ciberseguridad en muchas empresas no se aborda desde la junta de dirección, sino que se sigue organizando desde el departamento informático.

También en este estudio se asegura que los presupuestos para este problema están aumentando año a año en las empresas. Hecho que confirma que cada vez las organizaciones están siendo más conscientes de la importancia que supone estar bien protegidos frente cualquier amenaza.

5. SECTOR FINANCIERO Y LOS CIBERATAQUES

El sector financiero está en peligro frente a las ciberamenazas tanto es España como en el resto de los países. Tanto es así que se ha convertido en un asunto de seguridad nacional.

Como ya se ha visto anteriormente, las nuevas tecnologías han ofrecido grandes innovaciones, tanto dentro como fuera del sector financiero. En estos años han aparecido nuevos productos y proveedores dentro del sector financiero que han redefinido las bases del mismo, pero paralelamente aparecen una serie de amenazas que ponen en jaque la estabilidad financiera hasta ahora conocida.

Cada vez los riesgos cibernéticos son más sofisticados haciendo que sean más peligrosos y diversos entre sí y sea más sencillo interrumpir en cualquier sistema financiero y en las instituciones que apoyan al sistema. Por otro lado, al estar en un entorno cada vez más global, los ciberataques se han convertido en una amenaza para el mundo en general, ya que se propagan muy fácilmente de unas infraestructuras a otras.

Los ciberataques pueden tener un objetivo más individual y lanzar una amenaza para su beneficio propio, aunque la tendencia más actual es un poco más sofisticada y consiste en lanzar una amenaza para atacar el sistema financiero directamente.

Estos están en constante cambio y evolución, por este motivo, la ciberseguridad se ha convertido en una de las prioridades para las infraestructuras financieras. Se hace fundamental el intercambio de información entre las infraestructuras, los gobiernos y las empresas sobre los ataques que se han sufrido y las medidas que se han tomado.

5.1 MEDIDAS, GUÍAS, RECOMENDACIONES Y LESLACIÓN.

Ante todos los problemas a los que se enfrenta el sector financiero en relación con los ciberataques, muchos de los supervisores a nivel internacional y nacional se han dado cuenta del riesgo que supone los ciberataques y han ido poniendo medidas para intentar paliarlos lo máximo posible.

Es el caso del BCE[6], que al ser consciente que los ataques cibernéticos pueden ocasionar que desapareciera la confianza de los clientes depositada en las entidades. Junto con la necesidad de que los mercados estén conectados de una manera segura y eficaz, ha reunido a los gobernantes de los países que forman el G-7.

En esta reunión del G-7 se ha intentado mitigar los impactos que tienen los ciberataques, han intentado alinear una estrategia de seguridad cibernética a nivel internacional y han creado ocho elementos primordiales de ciberseguridad para el sistema financiero. Estos elementos se han diseñado para entidades tanto públicas como privadas del sector financiero.

Estos elementos sirven como guía para que las entidades puedan diseñar su estrategia de ciberseguridad y decidan cómo se va a implementar operativamente en las entidades. El diseño de la estrategia está guiado por el apetito al riesgo de cada entidad.

También, se puede utilizar cómo una guía para evaluar las estrategias ya implantadas en las empresas e intentar mejorarlas. Para el sector público, estos elementos están orientados para guiar las políticas públicas y mejorar el proceso de supervisión que deben hacer a las entidades, mejorando de esta forma la seguridad cibernética global del sistema financiero.

Los ocho elementos son:

1. Estrategia de Ciberseguridad.

   Esta fase consiste en definir la estrategia de ciberseguridad y el marco dónde se va a aplicar para intentar identificar, prevenir y reducir los riesgos cibernéticos de una manera global. Las entidades para ello deben tener en cuenta su perfil de riesgo y su cultura.

2. Gobernabilidad.

   En esta fase se definirá de forma más concreta la estrategia, se marcarán las funciones concretas y las responsabilidades del personal, además de supervisar y medir la eficacia de la estrategia de seguridad cibernética.

[6] BCE: Banco central europeo.

Para ello, se necesita un gobierno eficaz que defina claramente los objetivos que además estén en consonancia con la misión y con la tolerancia al riesgo que tenga cada la entidad y fomente la comunicación y la colaboración entre los equipos.

3. Riesgo y evaluación de control.

En esta fase se definirá las funciones, las actividades, se evaluará los riesgos cibernéticos a los que se enfrenta la entidad, se identificaran los controles que se van a realizar y todo ello teniendo en cuenta la tolerancia al riesgo que tiene la entidad.

Dentro de esta fase, lo primero que se ha de realizar es la evaluación del riesgo cibernético, para ello se debe analizar la tecnología que tiene la entidad, los procesos y el personal que se puede ver afectado por las amenazas cibernéticas. Posteriormente, se deberá identificar y evaluar los controles que se van a implantar. Y por último, también mencionar que es necesario que se fijen también en los riesgos cibernéticos de otras entidades y del sector financiero en particular.

4. Seguimiento.

Aquí, se establecen una serie de seguimiento de las actividades para detectar una amenaza en el menor tiempo posible y medir la eficacia de los controles internos. Esta fase ayuda a encajar mejor la estrategia seguida con la tolerancia al riesgo.

Todo esto se realizará a través de pruebas y auditoria interna, que deberían ser realizadas de forma independiente de las personas responsables de la gestión de programa de seguridad cibernética.

5. Respuesta.

Una vez detectada la amenaza, en esta fase se analiza el impacto del incidente cibernético, se intenta reducir el impacto del mismo, se comunica el incidente a todas las partes interesadas y se realiza una respuesta conjunta al mismo.

Al igual que pasaba con otras fases la planificación es fundamental, y por lo tanto, las entidades deberían implementar una serie de políticas que llevar a cabo en caso de amenaza y tener claro qué controles se van a implantar para que la respuesta ante esta sea lo más eficiente posible.

6. Recuperación.

Su objetivo sería una vez controlada la amenaza volver a la realización de la actividad de una forma habitual, para ello se deberá eliminar el posible peligro restante de la amenaza sufrida, restaurar el sistema y los datos a la normalidad, identificar y corregir todas las vulnerabilidades que provocaron la amenaza y la comunicación de la misma tanto externamente como internamente.

Para esta fase, sería idóneo que las entidades antes de que surgiera la amenaza realizasen un plan de contingencia, dónde se recogiese los planes de acción para poder seguir con la actividad habitual una vez sufrida la amenaza.

7. Intercambio de información.

En esta fase se intercambiará información sobre seguridad cibernética entre partes interesadas tanto dentro como fuera de la entidad.

Entre la información intercambiada se comunica de las amenazas sufridas, las incidencias que se han recogido, las partes en las que se es más vulnerable y las respuestas de la entidad ante esa amenaza.

Todo esto, permite a las entidades que estén al día de todos los métodos que utilizan los atacantes para irrumpir en cualquier entidad y de cómo estas entidades se defienden ante estas amenazas, dando una imagen global de la situación.

8. Aprendizaje.

El objetivo principal es revisar la estrategia se ha tomado anteriormente. En este análisis se debe incluir el riesgo, el control que se ha llevado del mismo, la respuesta que se ha dado

ante alguna amenaza y la estrategia de recuperación que se ha llevado a cabo ante la amenaza.

De esta forma, se podrá mejorar la estrategia tomada hasta ese momento, identificar los puntos débiles e incorporar partes nuevas a la estrategia que no se habían tenido en cuenta. Y adaptarse a la constante evolución ya no solo de los riesgos cibernéticos sino del sistema financiero provocados por los avances tecnológicos.

Por otro lado, en marzo del 2017 se aprobó la estrategia del Eurosistema para la vigilancia de la resiliencia cibernética para las infraestructuras de los mercados financieros. Cuyo objetivo es estandarizar la forma de reaccionar ante un ataque cibernético.

Anteriormente, en junio del 2016 el CPMI[7] y el IOSCO[8] crean un guía de ciberresiliencia para las infraestructura de mercado, en las que se indican las medidas a tomar para mejorar la ciberseguridad.

Antes de continuar explicando qué se recoge en esta guía hay que definir la ciberresiliencia. Es la capacidad de las entidades de prevenir, resistir y recuperarse de un ataque cibernético.

En esta guía de ciberesilencia[9] se recogen una serie de acciones para protegerse de los ciberataques tanto a los reguladores como a las infraestructuras. Estas acciones se basan en tres pilares.

1. Preparación de la infraestructura del mercado financiero. En este primer apartado, se busca la mejora en la seguridad de la infraestructura del mercado financiero ante unos ciberataques cada vez más específicos y sofisticados para garantizar su correcto funcionamiento.

2. Resiliencia del sector. El objetivo es mejorar la seguridad cibernética del sector mejorando la colaboración entre autoridades y todas los integrantes de compartiendo información entre los participantes del sector.

   Como el sector financiero está tan conectado entre sí, cualquier pequeña amenaza puede afectar de manera global al sector financiero. Es por ello que se está promoviendo la colaboración para mejorar la comunicación y los procedimientos en un momento de crisis.

[7] CPMI: Comité de pagos e infraestructura del mercado.
[8] IOSCO: Organización Internacional de comisiones de valores.
[9] Datos obtenidos de: Banco de España (2017). *Memoria anual sobre vigilancia de las infraestructuras de los mercados financieros.* Recuperado el 18 de julio del 2019 en: https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaAnualSistemasPago/17/MAV2017.pdf

3. Foro estratégico de la industria y los reguladores. El ECRB[10] se encarga de promover iniciativas conjuntas de concienciación sobre los riesgos cibernéticos.

   Se propone crear un foro en el que se reúnan los reguladores y las entidades, en el que se colabore conjuntamente para mejorar las capacidades del sector en relación con los ciberataques.

A nivel internacional destaca el caso de Estado Unidos, que entre otras muchas medidas, la CFTC[11] publicó en 2015 un documento consultivo que buscaba mejorar la normativa actual en ese momento proponiendo cinco tipos de pruebas de ciberseguridad. A partir del 2016 se ha ido aplicando a todas las entidades.

También en Estado Unidos, la SEC publicó en el 2011 una guía sobre la divulgación de riesgo cibernético, que se actualizó en el 2018, en la que se indica cómo y cuándo las empresas deberían revelar su información acerca de los ataques cibernéticos a sus inversores.

En Reino Unido, se creó una iniciativa entre el tesoro, el Banco de Inglaterra y la FCA[12] con el objetivo de recolectar información sobre la resistencia y la continuidad después de un ataque del sector financiero.

A nivel nacional, desde 2013 se creó un Plan Estratégico de Ciberseguridad creado por el Consejo de Seguridad Nacional. Los objetivos que se buscan son:

- Conseguir que los sistemas de información y telecomunicación utilizados por el Estado estén totalmente cubiertos de los riesgos cibernéticos.

- Promover la seguridad de los sistemas de información y telecomunicación en las compañías.

- Concienciar de los riesgos cibernéticos.

- Potenciar la prevención, análisis y recuperación ante los ataques cibernéticos.

- Intentar mejorar la ciberseguridad con nuevas aportaciones.

- Adquirir los conocimientos y las capacidades tecnológicas necesarias para proteger a todo el territorio español de cualquier ciberataque.

[10] ECRB: Consejo de Ciberresilencia del Euro para las infraestructuras financieras Panerupeas.
[11] CFTC: Commoditty Futures Trading Commision
[12] FCA: Financial Conduct Authority.

Por otro lado, IOSCO creó una guía en el 2016 dónde aunque reconoce que los ciberataques están dentro del riesgo operacional, hay ciertos aspectos que se debe tener en cuenta:

1. Los ciberataques más sofisticados son difíciles de detectar, son persistentes en el tiempo y pueden propagarse por otras infraestructuras antes de ser eliminados.

2. Puede que los planes de contingencia creados por la compañía no sean suficientes para eliminar del sistema el ataque haciendo que sea muy difícil volver a la actividad con normalidad, después de un ciberataque.

3. Hay muchos puntos de entrada para un ataque y las infraestructuras están conectadas entre sí.

También es importante mencionar de esta guía que recomienda que la protección ante un ciberataque englobe a toda la entidad y no solo a los puestos que tenga más relación con la tecnología. Y, que desde cualquier puesto puede interrumpir en la organización el ataque por lo tanto es fundamental que toda la compañía esté informada y concienciada con estos temas.

Y por último, destaca la necesidad de la cooperación internacional entre infraestructuras, entre las medidas necesarias que propone destacan:

- Apoyar a los países emergentes para que su legislación se iguale a los países ya desarrollados en temas de ciberseguridad.

- Fomentar el intercambio de información sobre los ciberataques recibidos, pudiendo crear una base de datos sobre las medidas tomadas.

- Desarrollar una guía que poder seguir en caso de ciberataque, tanto a gran nivel como a un nivel más bajo.

- Definir claramente los principios a seguir para protegerse de los ciberataques que esté muy ligada con las leyes sancionadoras del momento.

Hasta ahora, solo se ha hablado de guías y estrategias que se han ido creando e incorporando para intentar combatir de la mejor forma posible las amenazas que se enfrenta actualmente el sector financiero, pero también hay que añadir ciertas leyes que se han incorporado tanto a nivel nacional como internacional para combatir los ataques cibernéticos.

Durante el 2018 se han ido aprobando nuevas normativas, entre otras muchas cabe destacar: [13]

- A nivel internacional

El Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo, del 27 de Abril de 2016. Este reglamento busca la protección de las personas físicas y el tratamiento de datos personales. (GDPR), su plena aplicación comenzó en mayo del 2018.

Esta ley obliga a las empresas a informar de un ataque o un incumplimiento en la protección de datos de los clientes al órgano de supervisión en las siguientes 72 horas. Su incumplimiento tendría unas multas bastante elevadas, hasta 20 millones de euros o el 4% de la facturación anual.

- A nivel nacional

Orden PCI/870/2018 del 3 de agosto del 2018, en la que se publica el Acuerdo del Consejo de Seguridad Nacional. En este acuerdo se recogen la estrategia creada para la ciberseguridad nacional.

Real Decreto- ley 12/2018 de seguridad de las redes y sistemas de información. Este decreto se realiza para cumplir la Directiva de la Unión Europea 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016.

Cabe destacar el Real Decreto 3/2010, 8 de enero por el que se regula el Esquema Nacional de Seguridad. La Ley 8/2011 de 28 de abril por la que se establece medidas para la protección de las Infraestructuras Críticas. Y la Ley 36/2015 de 28 de septiembre, de Seguridad Nacional. Todas ellas conforman el Real Decreto-ley 12/2018, mencionado en el párrafo anterior.

Para finalizar, hay que nombrar la Ley orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales. Esta ley se ha creado a raíz de la incorporación de la ley GDPR, anteriormente mencionada, aunque aún no está aprobada.

[13] Datos obtenidos en su mayoría de: Centro Criptológico Nacional (2019). *Ciberamenazas y tendencias. Edición 2019.* Recuperado el 15 de julio del 2019: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3776-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-edicion-2019-1/file.html

Para finalizar es importante mencionar que tanto los reguladores como las entidades forman un papel fundamental en la resiliencia cibernética del sector financiero y por ello, es fundamental que trabajen conjuntamente para resolver las posibles amenazas y compartir información.

5.2 SITUACIÓN DE CIBERSTAQUES EN LAS ENTIDADES BANCARIAS.

A raíz del análisis realizado de las instituciones financieras, es importante analizar brevemente la situación actual de las entidades de crédito y es lo que se va a explicar en el siguiente apartado.

Los primeros ataques financieros aparecieron sobre el 2003 cuando empezaba a popularizarse la banca online y las medidas de seguridad eran muy básicas. Esta era una forma rápida y cómoda de estar conectado al cliente, utilizando las nuevas tecnologías. Que si no se protegía adecuadamente daba la oportunidad a los hacker de realizar los robos de dinero de una forma fácil y discreta.

Los primeros ataques se basaban principalmente en phising, correos electrónicos que simulaban que era enviados de las entidades. Pocos años después comenzaron los troyanos bancarios, su objetivo era al igual que en el phising, robar la identidad de la víctima para engañar al banco.

Las entidades financieras recogen una gran información sobre los clientes y en los ataques cibernéticos los atacantes pueden obtener una retribución económica mayor. Por otra parte, los ciberdelincuentes cada vez cuenta con más medios tecnológicos para evolucionar y paulatinamente los ataques cibernéticos se han ido sofisticando. Es por ello que el principal objetivo de los ataques ha dejado de ser los clientes de las entidades para ser directamente las instituciones financieras.

Para intentar paliar esta situación, la Unión Europea quiere realizar pruebas, parecidas al stress test para comprobar que los bancos cuentan con medidas de seguridad suficientes para responder a las amenazas. También, las Autoridades Bancarias Europeas van a implantando medidas para intentar mitigar lo máximo posible los efectos de un ataque cibernético a cualquier banco, como la ley de protección de datos ya implantada (GDPR).

Aunque no hay que olvidar que se continúan realizando los ataques tradicionales como el Phising o los troyanos bancarios, que van dirigido más particularmente al cliente.

Entre los últimos ataques cibernéticos realizados a una entidad financiera en sí y no a sus clientes destacan tres:

- Bangladesh Bank: En el 2016 el Banco Central de Bangladesh sufrió un ataque cibernético cuando un malware intento realizar una transferencia de 951 millones de dólares. Finalmente solo se pudo robar 81 millones de dólares ya que el resto de transferencias se bloquearon a tiempo.

- Tien Phong Bank: es un banco vietnamita que sufrió un ataque en el 2015, es un caso muy similar al anterior en el cuál, se intentó robar a través de transferencias per el banco se dio cuenta y gracias a ello la pérdida solo fue de 1 millón de dólares.

- Banco del Austro: la dinámica fue la misma que en las anteriores aunque en este caso se consiguió robar 9 millones de dólares.

Como se puede observar, en los tres ejemplos se utilizó un malware y se utilizó la red SWIFT ya que es un plataforma que utiliza para realizar transferencias la gran mayoría de entidades financieras a nivel global. También hay que añadir que ambos ataques están realizados por el mismo grupo y hacker.

Otro ataque que está en auge, aunque este sí que afecta directamente al cliente y no a las instituciones financieras en sí son los atracos a la TPV para robar información de las tarjetas de crédito.

Otro ejemplo de ataque financiero es el ocurrido en el banco Nacional de Blacksburg, Virgina en el 2016. El banco descubrió que había sufrido dos ataques de phising en menos de 8 meses, con una pérdida de 2.4 millones de dólares.

Este ataque fue lanzado desde Rusia y consistió en mandar correos al banco y desde allí acceder e intentar infectar a diferentes partes de la compañía.

Y el último ejemplo a mencionar sería el ocurrido en Agosto del 2018 en el banco Cosmos Cooperative Bank en la India. En este caso se atacó el sistema de tarjetas de débito de la compañía

(ATM) y el sistema interbancario de SWIFT y estos hechos provocaron una pérdida de 13.5 millones de dólares. Este caso se atribuye que los atacantes actuaron desde Corea del Norte.

Como modo de conclusión se puede decidir que aunque las entidades están tomando medidas para mejorar la seguridad y comprobar de una forma más eficaz la identidad de los clientes, no hay ningún método para evitar un ataque cibernético.

Pero para intentar protegerse de la mejor manera, en primer lugar se debería contratar un buen seguro e invertir en políticas, estrategias y planes de acción para responder de una forma rápida y correcta a los ciberataques dentro de la compañía.

Por último, una forma de protegerse más eficazmente ante un ataque cibernético consistiría en no centrarse en proteger los documentos, activos y datos importantes si no basar la estrategia de seguridad en las posibles amenazas.

6. CONCLUSIÓN

Como modo de conclusión se puede añadir que aunque la llegada de las tecnologías ha ocasionado muchos beneficios tanto financieros como no financieros. También han aparecido los ciberataques que buscan obtener un beneficio económico aprovechando las vulnerabilidades de los sistemas informáticos.

Esta nueva amenaza a la que se tienen que enfrentar las empresas se clasifica dentro del riesgo operacional, convirtiéndose en la mayor preocupación a la hora de gestionar este riesgo. Las empresas cada vez centran más esfuerzos en protegerse del riesgo operacional y de esta manera del cibernético. Muestra de ello es que en los últimos años aunque se ha mantenido el número de eventos de pérdida en relación con este, las pérdidas obtenidas son cada vez menores.

Las empresas son cada vez más conscientes del riesgo que suponen los ciberataques, tanto es así que la gestión de este riesgo está empezando a ser gestionado por la junta de dirección y no por el departamento informático de las compañías como se ha estado haciendo hasta ahora.

Aun así, las compañías siguen siendo muy vulnerables a los mismos debido a que los ataques son cada vez más sofisticados, gracias a la rapidez y facilidad con la que los ciberdelincuentes se adaptan a las nuevas tecnologías.

Por esto es necesario que las empresas centren sus energías en anticiparse a las amenazas antes de que ocurran. Para ello, están creando medidas adecuadas para protegerse del riesgo al que se exponen y desarrollar un plan de acción en el caso de que haya un incidente cibernético.

Para poder crear una buena defensa deberán conocer ampliamente el modelo de negocio y el sector dónde actúan, conocer los riesgos cibernéticos a los que se pueden enfrentar y medir los impactos que pueden acarrear en el caso de que algún riesgo, al que están expuestos, se materialice.

El problema viene cuando los recursos asignados no son suficientes para poder crear unas medidas de seguridad adecuadas. Sin contar con que en muchos casos no se dispone de demasiada información sobre los nuevos ataques, provocando que las empresas solo se centren en amenazas pasadas.

Ante todos los problemas a los que se enfrentan las empresas, pero sobre todo el sector financiero,, en relación con los ciberataques, los gobiernos y los supervisores, tanto nacionales como

internacionales, están implantando medidas para controlarlos, convirtiéndose la ciberseguridad en un asunto de seguridad nacional.

Estos, han creado guías, aprobado reglamentos y leyes para intentar paliar las amenazas lo máximo posible, es el caso de ley de protección de datos (GDPR) ya implantada en la Unión Europea.

Para finalizar se puede decir que aunque las empresas y los gobiernos son cada vez más conscientes del riesgo que supone sufrir un ataque cibernético, no hay ningún método infalible para evitar un ataque.

Es por ello, que aún hay mucho camino que recorrer para que los ciberataques no supongan una amenaza real para las organizaciones. Camino que deberán recorrer conjuntamente los reguladores y las compañías.

7. BIBLIOGRAFÍA

Banco de España (2017). *Memoria anual sobre vigilancia de las infraestructuras de los mercados financieros.* Recuperado el 18 de julio del 2019 en: https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaAnualSistemasPago/17/MAV2017.pdf

B.D.O (2018). *Cyber threat insights. Special focus: Recent cyber events in the financial instituions industry.* Recuperado el 4 de abril del 2019 en: https://www.bdo.global/en-gb/insights/advisory/cybersecurity/bdo-cyber-threat-insights-2018-3rd-quarter-report

B.D.O. *The need for a more proactive cyber defence.* Recuperado el 2 de julio del 2019 en: https://www.bdo.global/getmedia/6c07c065-5858-4066-86e0-acc5be34bfdf/The-Need-for-a-More-Proactive-Cyber-Defence_24-05-2017.pdf.aspx?ext=.pdf&disposition=attachment

Centro Criptológico Nacional (2018). *Ciberamenzas y Tendencias 2018.* Recuperado el 15 de julio del 2019 en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2856-ccn-cert-ia-09-18-ciberamenazas-y-tendencias-2018-resumen-ejecutivo-2018/file.html

Centro Criptológico Nacional (2019). *Ciberamenazas y Tendencias. Edición 2019.* Recuperado el 2 de julio del 2019 en*:* https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3776-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-edicion-2019-1/file.html

Cisco (2018). *Annual Cybersecurity Report.* Recuperado el 30 de julio del 2019 en: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

Cisco (2019). *Defensa contra las amenazas más graves de la actualidad.* Recuperado el 18 de julio del 2019 en: https://www.cisco.com/c/dam/global/es_es/assets/pdfs/es_cybersecurityseries_thrt_01_0219_r2-2.pdf

Cisco. *Effective Security for financial Services organizations.* Recuperado el 18 de julio del 2019 en: https://www.cisco.com/c/m/en_us/solutions/industries/financial-services/security-fsi.html

Cisco. *What are the most common cyber-attacks?* Recuperado el 2 de julio del 2019 en: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Cisco. *What is cybersecurity?* Recuperado el 2 de julio del 2019 en: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Comisión Nacional del Mercado de Valores. (2017). *Ciberseguridad en las infraestructuras de los mercados.* Recuperado el 18 de julio del 2019 en: https://www.cnmv.es/DocPortal/Publicaciones/Ciberseguridad/Ciberseguridad_Infraestructuras_Mercados.pdf

Deloitte. *Beneath the surfaces of a cyberattack. A deeper look at business impacts.* Recuperado el 4 de abril del 2019 en: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf

Deloitte. *Focus on: The board´s-eye view of cyber crisis management.* Recuperado el 4 de abril del 2019 en: https://www2.deloitte.com/es/es/pages/risk/articles/Ciberataques-el-nuevo-foco-de-atencion-de-los-directivos.html

Economist. (2015). *The cost of inmaturity*. Recuperado el 18 de julio del 2019 en: https://www.economist.com/business/2015/11/05/the-cost-of-immaturity

Ernest & Young (2018). *Recuperando la ciberseguridad: prepárese para enfrentar los ataques cibernéticos.* Recuperado el 10 de julio del 2019 en: https://www.ey.com/Publication/vwLUAssets/EY-recuperando-la-ciberseguridad/$File/EY-recuperando-la-ciberseguridad.pdf

European Central Bank. *Cyber resilience and financial market infraestructures.* Recuperado el 15 de julio del 2019 en: https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html

European Central Bank (2018). *Cyber resilience oversight expectations for financial market infraestructures.* Recuperado el 15 de julio del 2019 en:

https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

European Central Bank. *Cybersecurity for the financial sector*. Recuperado 10 de julio el 2019 en: https://www.ecb.europa.eu/paym/pol/shared/pdf/qa_cybersecurity.pdf

European Central Bank. *G7 Fundamental elements of cybersecurity for the financial sector*. Recuperado el 18 de julio del 2019 en: https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

European Central Bank. *What is cyber resilience?* Recuperado el 18 de julio del 2019 en: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html

European Central Bank (2018). *Why is cyber resilience important?* Recuperado el 18 de julio del 2019 en: https://www.ecb.europa.eu/explainers/tell-me/html/cyber-resilience.en.html

Instituto Español de Estudios Tecnológicos (2015). *Ciberataques, la mayor amenaza actual.* Recuperado el 4 de abril del 2019 en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

International Monetary Fund (2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.* Recuperado el 15 de julio del 2019 en: https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx

O.R.X. (2018). *Annual Banking Loss Report. Operational risk loss data for banks submitted between 2012 and 2017*. Recuperado el 2 de julio del 2019 en: https://managingrisktogether.orx.org/orx-loss-data/annual-banking-loss-report

O.R.X (2018). *Operational Risk Horizon 2018*. Recuperado el 15 de julio del 2019 en: https://managingrisktogether.orx.org/research/operational-risk-horizon-2018

O.R.X. (2019). *Operation Risk Horizon 2019 Summary*. Recuperado el 15 de julio del 2019 en:

https://managingrisktogether.orx.org/news-and-blogs/digital-continues-dominate-operational-risk-landscape

O.R.X. (2019). *ORX CISR Initiative: Definitions.* Recuperado el 15 de julio del 2019 en: https://managingrisktogether.orx.org/research/cyber-and-information-security-risk-definitions

O.R.X. (2019). *ORX launches cyber risk initiative*. Recuperado el 2 de julio del 2019 en: https://managingrisktogether.orx.org/news-and-blogs/orx-launches-cyber-risk-initiative

Panda Security (2018). *Guía de supervivencia contra ciberatracos millonarios*. Recuperado el 4 de abril del 2019 en: https://www.pandasecurity.com/spain/mediacenter/seguridad/ciber-riesgos-banca-online/