ICADE Business School

La gestión de los riesgos tecnológicos (ICT)

Autor: Guillermo Martín Rodríguez

Director: Julián Carlos Oliver Raboso

Madrid

27 Agosto 2018

Guillermo Martín Rodríguez

La gestión de los riesgos tecnológicos (ICT)

Dedicado a mi familia y a mi novia por todo el apoyo dado durante este año, a mi tutor por el gran asesoramiento recibido y a la directora del Máster por su inestimable ayuda durante todo el curso.

Contenido

RESUMEN

El fin de este trabajo es comprobar la importancia de la gestión de los riesgos tecnológicos tanto en la actualidad como en el futuro, enfocando el estudio en los ciberriesgos. Para ello se ha realizado una amplia tarea de investigación en las principales revistas tecnológicas y documentos de literatura del riesgo cibernético.

Mediante el estudio realizado se han adquiridos unos conocimientos acerca de los ciberriesgos: nomenclatura, consistencia, sistematización, mitigación, agentes, vectores de ataque, tendencia, relevancia en las entidades financieras y volumen de pérdidas generado.

Los resultados alcanzados evidencian la fundamental importancia de la gestión de los riesgos tecnológicos y más concretamente en este caso la gestión de los ciberriesgos en las entidades financieras.

Palabras clave: Ciberriesgo, ciberseguridad, gestión de riesgos, riesgo, tecnología, coste, tendencia.

ABSTRACT

The goal of this work is to document the importance of technological risk management in the present and in the future with a focus on cyber risks. In order to do it a wide research has been done in specialized technological papers and magazines.

Cyber risk knowledge has been acquired through the research carried out; nomenclature, consistency, systematization, mitigation, agents, attack vectors, tendency, relevance for financial institutions and loss volumes have been understood and analyzed.

Among other results we show in detail the fundamental importance of the management of technological risks in general and the management of cyber risks in financial institutions in particular.

Keywords: Cyber risk, cyber security, risk management, risk, technology, cost, trend.

1. Introducción.

La finalidad de este trabajo es tratar de evidenciar la creciente importancia de la gestión de los riesgos tecnólogos en las entidades financieras en el presente y futuro, centrando el estudio en los ciberriesgos. Es un tema que merece ser estudiado debido a su gran relevancia y a que hasta ahora no ha sido muy tratado. Esa es la razón por la cual yo decidí realizar este tema de trabajo, ya que considero que es un tema que ya tiene gran importancia en el presente, pero que adquirirá un importancia transcendental en el futuro.

Con la elaboración de este trabajo esperaba incrementar mis conocimientos en riesgos tecnológicos, conociendo tanto los diferentes tipos de riesgos como los principales métodos de mitigación de los mismos.

Para ello busqué entre los principales documentos de literatura del ciberriesgo y las publicaciones más relevantes de las revistas tecnológicas de la actualidad, mostrando así en diferentes apartados los conocimientos adquirimos tras las diferentes lecturas. Esta búsqueda no fue sencilla debido a que el tema a tratar es relativamente nuevo y no había mucha información sobre el mismo.

El trabajo está organizado de la siguiente forma.

En el primer apartado se pone en conocimiento qué es el ciberriesgo, para ello:

- Se realiza una breve definición de los ciberriesgos.
- Se realiza un análisis de los mismos.
- Se explica quiénes son los principales agentes de los riesgos cibernéticos y cuáles son sus objetivos.
- Y finalmente se muestra el conjunto de ciberriesgos mostrando para cada tipo de subriesgo sus principales características, vectores de ataque y métodos de mitigación.

En el segundo apartado se muestra cómo ha sido la evolución de la tecnología, de los ciberriesgos y de los sistemas de detección de intrusos hasta el año 2018. Posteriormente se exponen las tendencias de las amenazas en ciberseguridad y los principales retos en esta materia. Para finalizar el apartado se muestra la evolución de los sistemas de detección de intrusos, qué son, sus métricas más relevantes y las ventajas e inconvenientes de los mismos.

En el tercer apartado se pone en evidencia la importancia de los riesgos cibernéticos en las entidades financiares ya que la finalidad principal de los ciberataques no es otra que los motivos económicos. Esto tiene por consecuencia que las entidades financieras sean el objetivo principal de los mismos.

El cuarto apartado muestra diferentes formas de mitigar los ciberriesgos, exponiendo 4 alternativas:

- Mediante el uso de herramientas propuestas por el CNI.
- Mediante la contratación de seguros cibernéticos.
- Mediante el uso de la ciberinteligencia.
- Y mediante el intercambio de información relevante en materia de ciberriesgos.

Para finalizar el trabajo en el quinto apartado se exponen las diferentes conclusiones que permite alcanzar la elaboración del mismo.

Personalmente con la elaboración de este trabajo he aprendido a sistematizar los riesgos cibernéticos, su nomenclatura, su consistencia, sus principales métodos de mitigación y el importante volumen de pérdidas reales que genera este riesgo.

2. El ciberriesgo.

En este apartado se explicara de forma concisa qué es el ciberriesgo, cómo es su análisis, cuáles son sus agentes y qué diferentes subriesgos le componen. Comencemos.

2.1. ¿Qué es el ciberriesgo?

Es la posibilidad de incurrir en pérdidas como consecuencia de la realización de actividades usando medios informáticos o telemáticos sin conexión o bien a través de internet y/o redes de telecomunicaciones.

Este riesgo viene dado por la utilización de las nuevas tecnologías, tanto a nivel profesional como personal, y que puede hacer que se vean afectados tanto el correcto funcionamiento de los sistemas informáticos como la privacidad de las personas físicas y la información confidencial de las personas jurídicas.

El ciberriesgo puede provocar diferentes daños tanto materiales como intangibles, e incluso provocar daños a terceros.

Frecuentemente las personas piensan que los objetivos de estos ataques cibernéticos son solo las grandes entidades, pero esto no es así, todos somos un objetivo, es más, los hackers establecerán sus objetivos en empresas o individuos cuya seguridad sea más débil independientemente de su tamaño.

Es el riesgo más subestimado por las entidades, actualmente no se está reconociendo la gran importancia de este riesgo y por lo tanto no se están tomando las medidas necesarias para mitigarlo, esto puede dar a lugar a situaciones realmente trágicas. Especialmente se está subestimando el impacto que genera la interrupción del negocio desencadenado por un ciberataque. Cada día más empresas dependen de la tecnología, por lo tanto, su nivel de exposición está aumentando y volviéndose realmente significativo, sobre todo en los siguientes sectores: financiero, telecomunicaciones, transporte, fabricación y logística.

2.2. Análisis de los ciberriesgos.

Las ventajas del uso del ciberespacio son numerosas ya que permite la creación de nuevas capacidades en las comunicaciones, en la investigación científica, en la gestión de conocimientos o en los procesos industriales. Pero esta revolución tecnológica también trae consigo una serie de desafíos como son la protección de datos y la recuperación de infraestructuras críticas ante los ataques en el ciberespacio.

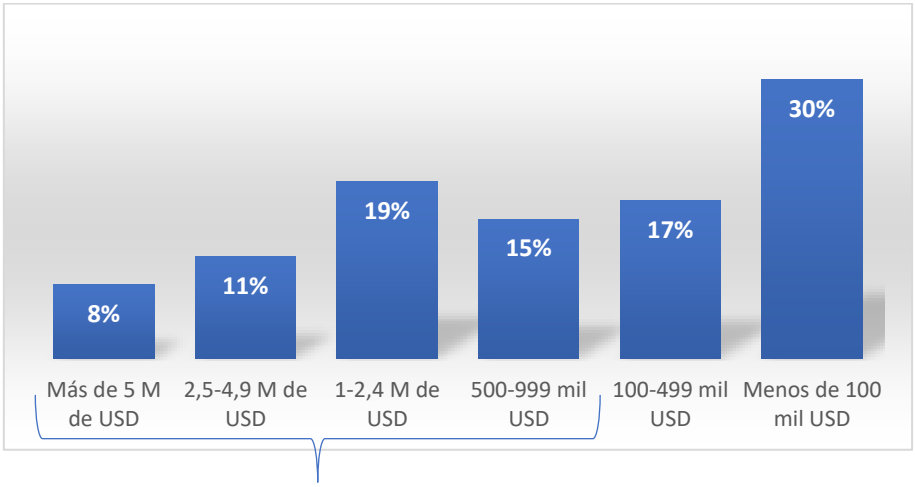
El ciberespacio también hace que se desdibujen las fronteras tradicionales de los países a la hora de determinar las responsabilidades de estos, debido a la dificultad de atribución de las responsabilidades y a la deslocalización de los ciberataques.

La reducción en los costes y los avances en las comunicaciones están generando una red en la que todos los elementos están conectados incluso los objetos de uso cotidiano.

Ante este escenario y con el objetivo de hacer frente a los desafíos del uso del ciberespacio se han realizado diferentes medidas de planteamiento estratégico de la seguridad, de creación de estructuras organizativas y técnicas, y de carácter político.

Los ciberatacantes están evolucionando de una forma más rápida que los responsables en ciberseguridad. Para los atacantes el coste de realizar un ataque cada vez es más barato y aumenta el daño realizado con el mismo; por el contrario, los sistemas de seguridad y prevención no dejan de ser cada vez más sofisticados y de mayor coste. Esto no hace más que aumentar la rentabilidad de los ciberataques, sobre todo cuando los beneficios de los mismos no dejan de aumentar:

Gráfico 2.1: El coste de los ciberataques.



Fuente: Elaboración propia con los datos del informe anual de 2018 de ciberseguridad del fabricante de equipos de telecomunicaciones CISCO

Como podemos observar en el gráfico, más de la mitad de los ataques han supuesto unas pérdidas mayores al medio millón de dólares por ataque. Esto nos hace ver la gran importancia de una adecuada gestión de los ciberriesgos en la actualidad.

Tabla 2.1: Países con un mayor coste en ciberataques.

País	Coste de los ciberataques como % del PIB	Coste estimado (millones de $)
Alemania	1,60%	59.000
EE. UU.	0,64%	108.000
China	0,63%	60.000
Brasil	0,32%	7.700
India	0,21%	4.000
Reino Unido	0,16%	7.700
Francia	0,11%	3.000
Rusia	0,10%	2.000
Italia	0,04%	900
Japón	0,02%	980

Fuente: Elaboración propia con los datos del World Bank (2013).

La tabla anterior muestra el ranking de países con un mayor coste en ciberataques como porcentaje de su PIB, apreciándose que los países más afectados son Alemania, Estados Unidos y China. Es destacable los casos de Japón y Reino Unido, dos de los países con un mayor número de transacciones mundiales y que sin embargo no son de los más afectados, esto puede ser debido a que tengan unos buenos sistemas de prevención frente a los ciberataques.

2.2.1. Comparación con otros riesgos globales.

Es interesante comparar la importancia de la gestión de las ciberamenazas en comparación con otros riesgos globales, para ello hay que fijarse en el Foro Económico Mundial que publica un estudio de riesgos globales en el que muestra el impacto y la probabilidad de estos.

Los riesgos globales más importantes en función de su impacto y probabilidad según el estudio de riesgos globales[1] son: los riesgos económicos (como las crisis y el alto desempleo), la inestabilidad social y los ciberataques. Los riesgos emergentes con mayor relevancia son el cambio climático, la desigualdad económica y el aumento de la ciberdelincuencia.

En concreto los ciberataques se encuentran en la cuarta posición por debajo de la negativa al tratamiento del cambio climático, la crisis del agua y las migraciones involuntarias. En cambio, se encuentra por encima de riesgos tan importantes como el desempleo y los conflictos internacionales. Esto refleja la gran importancia de la gestión de las ciberamenazas debido a su alta probabilidad y su elevado impacto en comparación con el resto de los riesgos globales.

Otro aspecto destacable del mencionado Informe de Riesgos Globales es la conexión directa de los ciberataques con otros riesgos, tanto tecnológicos, como económicos, como geopolíticos.

[1] MARSH&McLENNANCOMPANIES (2018). Informe de riesgos mundiales. Recuperado el 31 de julio de 2018 de http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=10&sid=22eeadff-be7c-4fac-95cf-1f27bb1a8e57%40sessionmgr4010.

2.2.2. Principales factores para el análisis de las ciberamenazas.

Los elementos esenciales que hay que tener en cuenta a la hora de realizar un análisis eficaz de las ciberamenazas son los siguientes:

- Intereses: objetivo al que va dirigido el ciberataque en contra de los sistemas de seguridad, ya sea la de confidencialidad, de trazabilidad, de la integridad, de la disponibilidad o de la autenticidad.
- Amenazas: tipos de actividades que podría realizar el ciberatacante para conseguir su objetivo.
- Resiliencia: medida de acierto de los sistemas de defensa frente al ciberataque, así como de las medidas adoptadas para hacerle frente. Por lo tanto, no se trata de la ausencia de vulnerabilidades en la defensa sino precisamente de la eficacia de las medidas adoptadas para fortalecer los sistemas frente a las agresiones.

Gráfico 2.2: Factores de los ciberataques.

Fuente: Elaboración propia.

2.3. Agentes de los ciberriesgos.

Los principales encargados de la realización de ciberdelitos y por tantos los responsables de las ciberamenazas son:

Actores estatales

Para valorar el impacto de la seguridad mundial es importante conocer la posición como elemento activo o pasivo de un Estado en los ciberataques ya que sus respuestas, compromisos, y actitudes serán diferentes en función de su posición.

En mayor o menor medida todos los países occidentales son objeto de ciberataque, debido al interés para la obtención de información de relevancia militar, económica o geoestratégica.

Debido a que permite la obtención de enormes beneficios en comparación con su bajo coste, que existe una gran dificultad para determinar sus actores y que limita los riesgos asumidos, los ciberataques son uno de los sistemas de acción más utilizados.

Los estados con gobiernos autoritarios o formas de estado no democráticas, esta importancia se hace mayor, debido a que gozan de ventajas frente al resto de estados. Estas ventajas se deben a que en estos estados se prestan poca atención al cumplimiento de las normas jurídicas, permitiendo así, utilizar ataques sin ningún control que tienen como consecuencia acciones realmente eficaces.

Los elementos comunes en los ataques realizados por estados son:

- El primer objetivo de ataque es la obtención de información estratégica.
- El segundo objetivo de ataque son las agresiones individuales dirigidas a persona o instituciones con algún interés.
- El tercer objetivo de ataque consiste en manipular las implementaciones técnicas de sus víctimas.
- Y finalmente el cuarto objetivo de ataque es la manipulación selectiva de los equipos informáticos.

Para finalizar este punto, cabe destacar el significativo número de países que ya están desarrollando sistemas para realizar operaciones militares en el ciberespacio.

Terrorismo y ciberyihadismo

El objetivo del terrorismo es provocar cambios políticos y/o ideológicos a través del pánico, generando terror en la sociedad. A pesar de que la actividad terrorista en el ciberespacio se está incrementando, todavía no es una gran amenaza debido a sus limitados conocimientos tecnológicos. Es por eso, que hoy en día los ataques terroristas se han limitado a actividades que no requieren unos grandes conocimientos o infraestructuras.

Los grupos yihadistas cuelgan en la red información y vídeos con el objetivo de formar en materia de ciberseguridad a yihadistas potenciales y también han comenzado a utilizar internet para realizar ataques contra gobiernos e instituciones occidentales. Son numerosos los casos recientes que muestran que el ciberejército yihadista está aumentando tanto en número como en sofisticación.

Para realizar estas tareas necesitan financiación, los terroristas se financian a través de la recaudación de fondos directa o con tácticas similares a los ciberdelincuentes, es decir, a través de *phising* para obtener datos de tarjetas de crédito robadas.

Todas estas señales nos muestran que las capacidades del ciberyihadismo no han hecho nada más que empezar, en el futuro se esperan ciberataques más sofisticados, más destructivos y más numerosos.

Profesionales del ciberdelito

Su objetivo es la obtención de beneficios económicos y se caracterizan por realizar ataques con una ejecución inmejorable, una brillante organización y una formidable sofisticación técnica.

Las organizaciones criminales están invirtiendo grandes cantidades de dinero para realizar sus acciones de una forma cada vez más creativa. A demás, las herramientas para la realización de ciberataques son cada vez más accesibles, lo que da a lugar a un incremento del número de ciberdelincuentes y, en consecuencia, de sus acciones.

Los métodos utilizados varían en función de si son usuarios privados u organizaciones. Los usuarios privados se decantan por el uso del correo basura o *spam*, el código dañino para el robo de identidad, los correos electrónicos de *phising,* y la utilización de *ransomware*. Mientras que las organizaciones utilizan métodos como la extorsión o la infección por código nocivo para terminales de punto de venta.

Como consecuencia de que algunas organizaciones criminales ofrecen sus servicios y capacidades a otras organizaciones, se ha creado un mercado de la ciberdelincuencia, en el que se ofrecen todo tipo de métodos de ataque, vulnerabilidades y se garantiza un resultado satisfactorio del ataque.

Ciberdelincuentes.

Se trata de individuos que poseen grandes conocimientos técnicos y que realizan sus acciones con el único objetivo de demostrar públicamente que son capaces de hacerlo.

Hacktivistas

Son personas o grupos más o menos organizados, que realizan sus actos por motivos ideológicos. Frecuentemente sus acciones se dan en lugares donde se han producido hechos que a su entender han sido desproporcionados o injustos.

Actores internos

Los denominados actores internos son personas que trabajan o han trabajado en la organización y no se mueven por motivos económicos, sino por negligencias o despecho.

Ciberinvestigadores

Buscan la vulnerabilidad de las TIC con el objetivo de garantizar la protección de los sistemas bajo investigación.

Es necesario tener en cuenta que muchas veces estos investigadores son contratados por otros agentes, especialmente estados y empresas dedicadas al ciberespionaje con el objetivo de la exfiltración de información o para la infección de una red objetivo.

2.4. Subriesgos.

En este apartado se muestran los diferentes subriesgos que componen el ciberriesgo permitiendo de esta forma hacernos una idea de la realidad de las ciberamenazas mostrando sus principales características.

2.4.1. *Malware*.

Es la ciberamenaza más frecuente, cuyo progreso en periodicidad se ha estancado, pero en sofisticación y diversidad ha continuado. Es una modalidad de *software* malicioso cuya finalidad es infectar un dispositivo tecnológico. Diariamente se detectan 4.000.000 de amenazas[2] por este subriesgo. Es la ciberamenaza que más veces se detecta y tiene una tendencia estable o ligeramente decreciente.

[2] ENISA (2017). ENISA Threat Landscape Report 201715 Top Cyber-Threats and Trends. Recuperado el 2 de Julio de 2018 en https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

El vector de ataque más utilizado por esta amenaza es el *phising*[3] (90-95%). Por esta razón es fundamental concienciar al usuario debido a que la debilidad de este vector de ataque se encuentra en el vínculo humano.

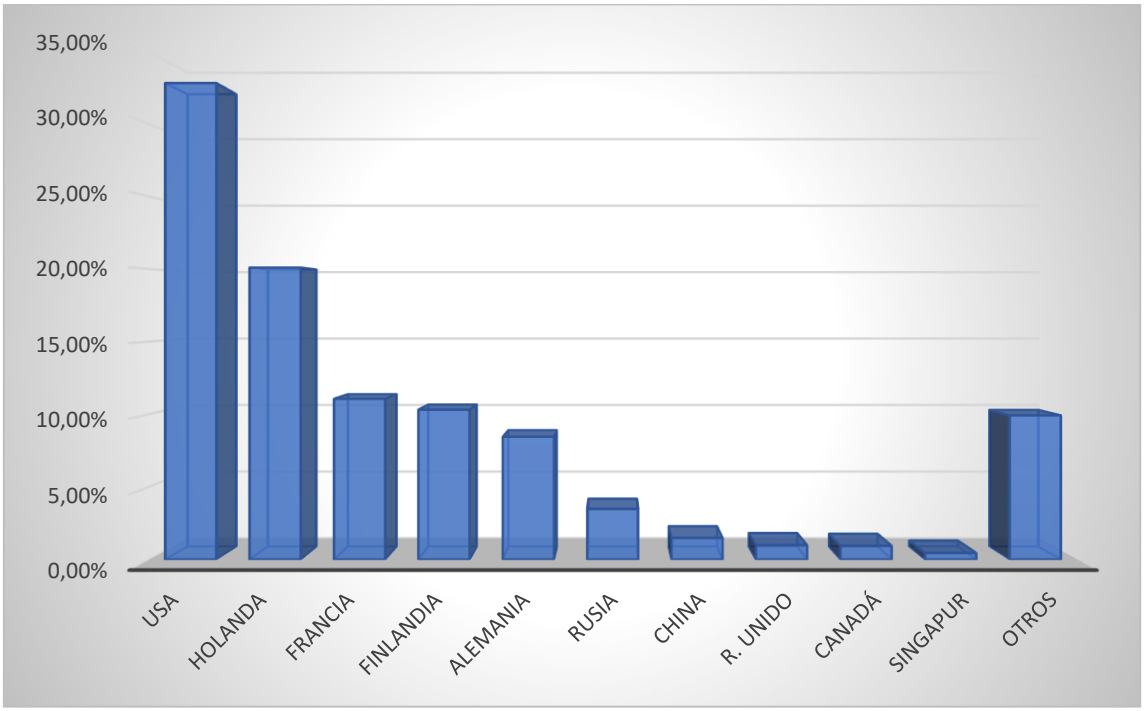
Para mejorar la seguridad ante este ciberriesgo hay que establecer sistemas de detección en todos los canales tanto de salida como de entrada de todos los dispositivos.

2.4.2. Ataques a la web.

La tendencia general de este riesgo es de aumentar. Son agresiones están enfocadas contra navegadores, componentes de TI, y webs. Ha sido uno de los ataques más frecuentes en el año 2017 y como consecuencia de la importancia de la web en la actualidad, se espera que su relevancia continúe. Este tipo de ataques se suele combinar con el anterior subriesgo y su número de actividades detectadas ha aumentado de tal forma que está a punto de igualar las cifras de ataque que posee el anterior ciberriesgo. De entre todas las posibles formas de introducir las ciberamenazas, el medio más utilizado es a través de la web, este método fue utilizado en el 48% de los casos[4].

[3] ENISA, op. cit. (2017). Pg 29.
[4] ENISA, op. cit. (2017). Pg32.

Gráfico 2.3: Distribución de los ciberataques.



Fuente: Elaboración propia con los datos de ENISA Threat Landscape Report 2017

A simple vista en el gráfico no aparece nada fuera de lo normal, los países con un mayor número de ciberataques son aquellos que más riqueza tienen o que realizan un mayor número de transacciones. Vuelve a destacar el caso de Reino Unido, caso peculiar debido a que todo parecería indicar que estaría entre los países con un mayor número de ciberataques, sin embargo está entre los más bajos, esto puede ser debido a que adopte unas mejores medidas en ciberseguridad que el resto de los países.

Los principales vectores de ataque a la web son:

- *Exploits*: código malicioso que aprovecha debilidades del navegador.
- Descargas de *drive-by*: descarga automática del virus al entrar en una página web insegura.
- URL maliciosas: creadas exclusivamente para la descarga directa de *malware*.
- *Water-holing*: el ciberatacante observa los sitios web más comunes de su víctima y los infecta.

Las principales recomendaciones en materia de ciberseguridad para este riesgo son evitar el uso de extensiones web innecesarias, mecanismos de protección del navegador, filtrado de la web, y actualización regular del navegador.

2.4.3. Ataques en aplicaciones.

La finalidad de estos ataques es abusar de las APIs, que son un conjunto de procedimientos o funciones que permiten a un módulo de *software* interactuar con otro, incorporadas en las aplicaciones. Es un método muy utilizado y de tendencia alcista debido a su alto grado de exposición por el acceso público a las aplicaciones. Los objetivos más apetecibles son las aplicaciones financieras y gubernamentales. El 90% de estos ataques[5] está cometido por organizaciones delictivas con una finalidad económica.

La media diaria de este tipo de ataques se encuentra en los 1.800 millones[6] y los países receptores de este tipo de ataque son EE. UU. (cerca del 35% de los ataques de este tipo), China (poco más del 10%), Brasil (entorno al 8%) y Holanda (entorno al 6%).

Las principales medidas de seguridad son elaborar políticas de seguridad, instalar de cortafuegos, usar mecanismos de autorización, realizar pruebas de vulnerabilidad, y reparar/fortalecer estas.

2.4.4. *Phising*.

Es un ataque que se basa en la suplantación de la identidad. Cada vez es más difícil de detectar como consecuencia del aumento de su sofisticación y especificación que se ha producido en este ciberriesgo. Este método es el más exitoso para la consecución de la infección y por esta razón esta relacionado con el resto de los ciberataques.

[5] ENISA, op. cit. (2017). Pg 37.
[6] ENISA, op. cit. (2017). Pg 37.

El elevadísimo ritmo de creación de nuevos sitios web de phising (1 millón[7] al mes), hace imposible el bloqueo de estos, más aún si como es en el caso de este ciberataque su vida media es de 4 a 8 horas[8]. La tendencia de esta amenaza es a aumentar.

Al contrario que en el anterior método en cual los ataques estaban muy concentrados en un país, en éste sus objetivos están muy diversificados por numerosos países encabezando la lista China, Vietnam, EE. UU. e India.

Las principales recomendaciones en seguridad son el aumento de la educación del personal en correos maliciosos, la utilización de filtros en el correo, evitar enlaces y descargas de origen dudoso (especialmente los enlaces cortos de las redes sociales), evitar compartir excesiva información personal, no hacer clic en "habilitar contenido", utilizar una contraseña consistente y en las transacciones económicas comprobar dos veces la cuenta corriente del receptor.

2.4.5. *Spam*.

Es un método que tiene una tendencia al alza. Esta amenaza proviene del comienzo de internet y es una de las más frecuentes y persistentes. El *spam* o correo no deseado representa el 50% del volumen de correo electrónico[9] y es el medio más utilizado para la infección del *malware*. A lo largo de su vida este método ha reducido el número de envíos, pero ha ganado calidad con la utilización de nuevas y mejores técnicas.

Algunos de los datos más destacados es que del total de correos *spam*[10] el 88% proviene de *botnets* (robots informáticos que se ejecutan de manera automática), y que el 66% de los correos no deseados tienen relación con productos farmacéuticos. No se centra en ningún país en concreto está bastante diversificado siendo los países más afectados Vietnam, EE. UU., China e India, los mismos que por *phising* pero con distinta relevancia.

[7] ENISA, op. cit. (2017). Pg 42.
[8] ENISA, op. cit. (2017). Pg 42.
[9] ENISA, op. cit. (2017). Pg 46.
[10] ENISA, op. cit. (2017). Pg 46.

El principal método para prevenir esta amenaza es la educación a los usuarios debido a que se basa en el abuso de la confianza de la gente, otros métodos recomendables es el filtrado de correo y la utilización de bloqueos autoejecutables.

2.4.6. Negación de servicio.

Es un ataque de especial importancia para las empresas que trabajan en línea. Consiste en imposibilitar el acceso a la red o sistemas computacionales a los usuarios. Es el responsable de los ataques más grandes de la historia en lo que se refiere a ancho de banda.

Los principales países involucrados[11] en este método de ataque son China, que como atacante, supone el 60% de los ataques y EE. UU. que como víctima, recibe el 90% de los ataques. Debido a la gran censura cibernética existente en China es fácil deducir que es el Estado el que realiza esos ataques y en el caso de Estados Unidos también es fácilmente deducible que sea el principal objetivo de este ataque debido a que la gran mayoría de las webs tienen su origen en este país[12].

Es destacable que el 80% del volumen[13] se centra en la industria de los videojuegos. También es destacable, que los ataques son contra los sectores financiero, energético, y de transporte.

Es un método con una tendencia creciente y los principales mecanismos de defensa son la creación de una política de seguridad DoS/DDoS, realizar una evolución y documentación de los sistemas de protección, y desarrollar los sistemas de identificación de este tipo de ataques.

[11] ENISA, op. cit. (2017). Pg 51.
[12] CIA, The World FactBook (2012). Recuperado el 14 de Agosto de 2018 en https://www.cia.gov/library/publications/the-world-factbook/rankorder/2184rank.html.
[13] ENISA, op. cit. (2017). Pg 51.

2.4.7. Ciberespionaje.

Es considerada una de las amenazas más importantes por las organizaciones mundiales. Se realiza a través de las APT (Amenazas Persistentes Avanzadas) que permiten infiltrarte en el objetivo durante un periodo de tiempo con la finalidad de obtener información relevante.

La tendencia de este riesgo es de aumentar; actualmente el 20% de las organizaciones[14] reconoce que el ciberespionaje es su riesgo más temido.

El vector de ataque utilizado en algunas ocasiones es un *malware* completo pero el método más utilizado es el *phising*.

Las principales medidas de seguridad contra este riesgo son el conocimiento de la exposición al mismo, el uso de filtros para la entrada y salida de los canales, el establecimiento de políticas de seguridad, las evaluaciones de vulnerabilidades y fortalecimiento de estas, y la elaboración de una lista con las actividades críticas.

2.4.8. *Exploit Kits*.

Este método consiste en la detección de las vulnerabilidades de los objetivos y explotarlas automáticamente. Es un método muy utilizado en ingeniería social.

Se está observando una caída en el uso de este método y es muy probable que su uso siga cayendo en un futuro.

Las principales recomendaciones para mejorar la seguridad frente a este tipo de ataque son la implementación de sistemas de detección, la realización de actualizaciones periódicas de las vulnerabilidades y la utilización de filtros en el correo.

[14] ENISA, op. cit. (2017). Pg 88.

2.4.9. Filtrados de información.

Son una de las principales amenazas de la actualidad consistente en la publicación de información reservada y que a pesar de que todo parecería indicar que la forma de conseguir la información es mediante la violación de la seguridad, actos hostiles o fallos tecnológicos, en la mayoría de las ocasiones es porque alguien de dentro de la organización facilita la información.

Estos casos de fuga de información han aumentado tanto en frecuencia como en tecnificación y volumen, se estima que más o menos el 78% de los usuarios[15] que abandonan las redes sociales lo hace por temor a estos filtrados de información. Es un método de ataque con tendencia al alza y sobre todo en el caso de la publicación de archivos privados provenientes de dispositivos móviles.

Como se ha apuntado anteriormente el principal vector de ataque es por filtrado de alguien perteneciente a la organización, otros métodos son por vulnerabilidades o errores.

Los principales métodos de prevención para este ciberriesgo son no tener información expresada de forma clara, identificación del personal con acceso a los diferentes documentos, instalación de herramientas para evitar la fuga de datos, clasificación de la información almacenada y la realización de análisis de debilidades y fortalecer las mismas.

2.4.10. *Ransomware*.

Es un método que se caracteriza por la obtención de rentabilidad de una forma rápida y directa. Es un tipo de *malware* que bloquea el sistema informático para posteriormente exigir un rescate a cambio de recuperar el acceso al mismo, concretamente es el más utilizado, el 60% de los *malware*[16] son *ransomware*.

[15] ENISA, op. cit. (2017). Pg 71.
[16] ENISA, op. cit. (2017). Pg 56.

Se prevé que las pérdidas mundiales por este tipo de ataque alcancen los cinco mil millones de dólares y que el más del 70% de las entidades afectadas[17] no puedan recuperar los datos en periodo mínimo de dos o tres días. Es una forma de ataque cibernético que tiene una tendencia a continuar creciendo.

El principal país en el que se concentran este tipo de ciberataques es EE. UU.[18] que detecta un 29% del total de estos ataques, el resto de los países apenas llegan al 5%, se encuentran entre un 3% un 4%.

Los vectores de ataque más utilizados por este método son los correos *spam* o los *Exploit Kits*.

Las principales medidas de ciberseguridad que se recomiendan son establecer un filtrado de contenidos no deseados, antivirus, políticas de control de los dispositivos externos, copias de seguridad, educación a los usuarios y elaboración de listas de puntos débiles.

2.4.11. *Botnets*.

Es un grupo de ordenadores infectados cuyo control lo tiene de forma remota el atacante. Está considerado el segundo ciberriesgo más importante, concretamente el *botnet* del "Internet de las cosas" (interconexión de los objetos cotidianos con internet), su importancia que viene dada por el gran desarrollo que se ha producido en este ámbito (en 2017 se conectaron otros 8.400 millones de dispositivos[19] al denominado "Internet de las cosas"). Por esta razón, este tipo de riesgo tiene una gran tendencia a incrementar su importancia.

Los países más infectados por este tipo de riesgo en 2017 fueron: China, India, Rusia, Vietnam, Argentina, Tailandia, EE. UU. e Indonesia.

[17] ENISA, op. cit. (2017). Pg 56.
[18] ENISA, op. cit. (2017). Pg 56.
[19] ENISA, op. cit. (2017). Pg 61.

Ese mismo año en Twitter se descubrieron más de 350 mil cuentas falsas[20] relacionadas con este método de ataque.

Para incrementar la seguridad frente a este riesgo se recomienda instalar un correcto antivirus, un filtro para el tráfico de datos relevantes, sistemas de detección, creación y mantenimiento de listas negras, y realizar una continua actualización de los sistemas de seguridad.

2.4.12. Amenaza interna.

Este riesgo consiste en que una persona perteneciente a la empresa utilice su acceso autorizado para hacer daño a la entidad ya sea de forma voluntaria o involuntaria. Este tipo de amenaza se da desde hace muchos años y en el presente continúa siendo importante.

Como la mayoría de los sistemas de seguridad se centran en el exterior, el vector de ataque, que es una o varias personas de dentro de la organización, hace que sea un riesgo de una importancia transcendental.

El 75% de las organizaciones[21] cree que los costes asociados a este ciberriesgo pueden llegar al medio millón de dólares por entidad y además, el 25% piensa que puede superar ese coste.

Estos datos nos muestran la situación real de la economía: que tan solo el 29% de las entidades[22] tiene sistemas de seguridad frente a amenazas internas.

Es recomendable establecer unas políticas de seguridad frente amenazas internas, usar la ciberinteligencia, implementar auditorías y monitoreo, realizar actividades de sensibilización de los trabajadores y controles del acceso de la información de cada trabajador, para incrementar la seguridad frente a esta ciberamenaza.

[20] ENISA, op. cit. (2017). Pg 61.
[21] ENISA, op. cit. (2017). Pg 20.
[22] ENISA, op. cit. (2017). Pg 20.

2.4.13. Manipulación/daños/pérdida/robo físico.

A pesar de que no es muy común todavía sigue teniendo una gran relevancia en los ataques cibernéticos sobre todo en el robo de datos. Este tipo de riesgo tiene una tendencia a disminuir y consiste en el uso de la fuerza física para conseguir los diferentes fines anteriormente mencionados.

Los datos[23] recientes muestran una tendencia decreciente de la acción física en los ciberataques, actualmente un 8%. Los dispositivos medios que pierde una persona en la actualidad son de 1,24 de los cuales menos de la mitad son recuperados. Si haces una encuesta a la población el 7, 5 % de ellos perdió su ordenador portátil en los últimos 10 meses.

Las principales recomendaciones en materia de seguridad son el cifrado de los dispositivos y documentos, mejorar las políticas de seguridad, establecer límites a determinados archivos de información, contratar un seguro y establecer una guía de uso de dispositivos móviles y buenas prácticas.

2.4.14. Violación de datos.

Este riesgo tiene la característica de que nos damos cuenta que se ha producido el ataque cuando ya ha sido realizado con éxito, además, se dan mucho más casos de los que llegamos a conocer. Consiste en el acceso por parte de personas no autorizadas a datos confidenciales. En los últimos años ha habido un esfuerzo importante por parte de las empresas para aumentar la seguridad frente a la violación de datos.

Los encargados de la defensa deben de estar preparados para las amenazas conocidas como para las nuevas que todavía aún no se conocen, además, de tener establecidos un plan de acción y recuperación frente a las mismas.

Este tipo de ataque aumento[24] un 25% en 2017 y su tendencia es creciente.

Debido a la gran cantidad de vectores de ataque que pueden llevar a cometer una violación de datos es difícil establecer un sistema de prevención de

[23] ENISA, op. cit. (2017). Pg 69.
[24] ENISA, op. cit. (2017). Pg 71.

garantías, pero este mismo debe tener soluciones ante las pérdidas previstas, cifrados de datos, reducción del acceso a los datos, desarrollo e implementación de nuevas políticas de seguridad, establecimiento límites de información almacenada, establecimiento de planes de recuperación de datos y creación de conciencia de seguridad dentro de los empleados de la entidad.

2.4.15. Robo de identidad.

Este método se basa en la obtención por parte del atacante de información confidencial de la víctima mediante el hurto de la identificación de la misma.

El ritmo de este ciberataque es por ejemplo en Reino Unido de casi 500 al día[25], esta frecuencia unida a los bajísimos precios de la información de la identidad en la "*dark web",* es una parte de la web donde hay contenidos ocultos a los sistemas de búsqueda convencionales utilizando direcciones IP enmascaradas y que sólo es accesible con un navegador web especial, hacen que sea de muy fácil acceso y por lo tanto de vital importancia.

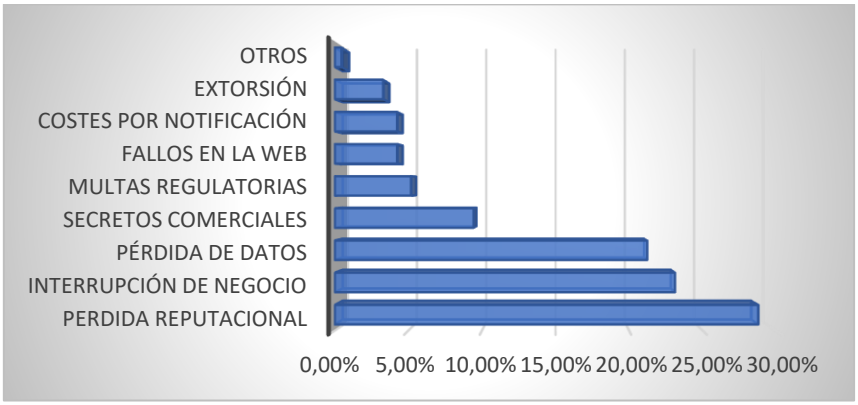
Este tipo de ataque tiene una tendencia a aumentar en los próximos años, tan sólo en el primer trimestre de 2017 se incrementó un 5% el número de casos[26].

El vector de ataque más común de este ciberriesgo es el factor humano, ya que muchas personas ponen a disposición su información personal sin saberlo.

Para aumentar la seguridad en esta materia es recomendable aumentar la protección de todos los documentos personales y sus copias, no divulgar datos personales, proteger mediante códigos las informaciones más relevantes, evitar las redes Wi-Fi públicas, verificar las transacciones bancarias y mejorar los sistemas de almacenamiento de información.

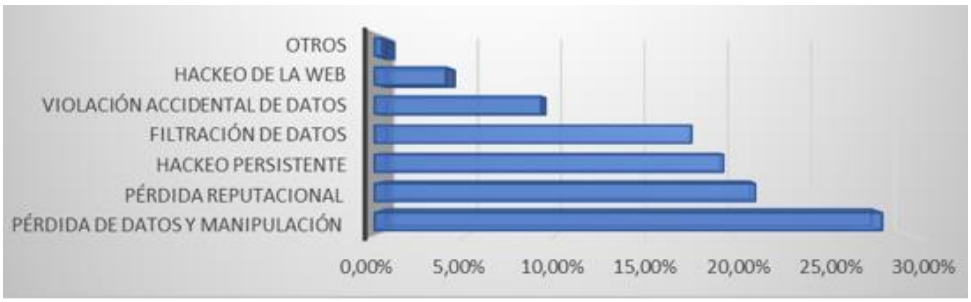
[25] ENISA, op. cit. (2017). Pg 76.
[26] ENISA, op. cit. (2017). Pg 76.

Gráfico 2.4: Pérdida económica por ciberriesgo.



Fuente: Elaboración propia con los datos del Barómetro de riesgo de Allianz.

Gráfico 2.5: Riesgos cibernéticos temidos por las empresas.



Fuente: Elaboración propia con los datos del Barómetro de riesgo de Allianz.

Como se ha expuesto anteriormente de forma individual y como se puede observar ahora de manera conjunta en los gráficos, los principales subriesgos que provocan las mayores pérdidas económicas son la pérdida reputacional, la interrupción de negocio y la pérdida de los datos y los ciberriesgos más temidos por las entidades son la pérdida de datos, la pérdida reputacional y el hackeo.

3. Evolución tecnológica.

Actualmente nos encontramos en un punto en el que todavía se esperan mayores tasas de crecimiento tecnológico, es decir, nos encontramos muy lejos del denominado punto de saturación de las TIC.

Si te descuidas en innovación hay un enorme riesgo de quedarte fuera del mercado. Esto se traduce en un aumento de la presión por situarse por encima de la competencia lo que provoca que en muchas ocasiones no se concilie de forma correcta la seguridad con los intereses económicos. Las empresas buscan sacar al mercado nuevos productos de una forma rápida dejando de lado la seguridad de los mismos.

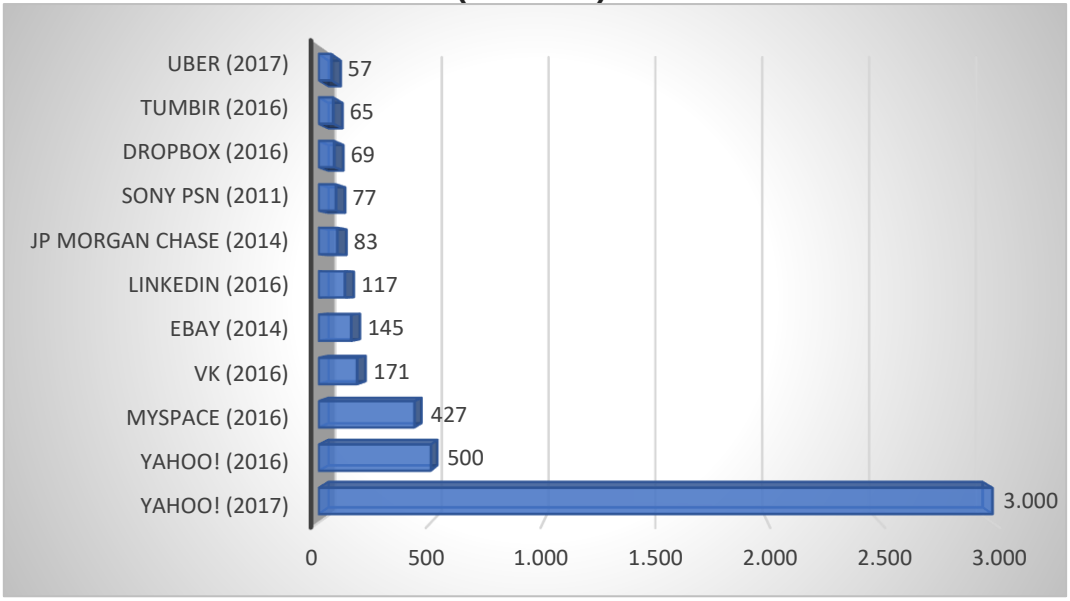
Utilizar productos modernos, seguros y compatibles es una tarea de una enorme dificultad, debido a que la incorporación de la seguridad a las tecnologías es un proceso lento.

La utilización de las TIC se ha generalizado, se utilizan en numerosos ámbitos, en la vida cotidiana, en la sanidad, en los medios de transporte, entre otros. La penetración de las TIC en la vida política, social, administrativa o económica de un país hace que desaparezcan de una forma más veloz las alternativas analógicas, esto hace que confiera especial importancia los sistemas TIC, sistemas que son mucho más complejos que sus antecesores y que están conectados a Internet lo que hace que aumente su riesgo.

El denominado “Internet de las cosas” tendrá una importancia transcendental. Las estimaciones apuntan que en 2020 estarán conectados más de 30.000 millones de dispositivos[27]. Estas nuevas tecnologías crean nuevas vulnerabilidades que los ciberdelincuentes pueden explotar. Pero no sólo las nuevas tecnologías generarán esas debilidades, sino que también los dispositivos más antiguos que continúen utilizándose, debido a que estarán obsoletos y utilizarán *softwares* incompatibles.

[27] OBS Business School (2015). Estudio Big Data 2015. Recuperado el 31 de julio de 2018 en https://www.obs-edu.com/es/noticias/estudio-obs/en-2020-mas-de-30-mil-millones-de-dispositivos-estaran-conectados-internet.

Gráfico 3.1: Número de cuentas hackeadas en plataformas tecnológicas (millones).



Fuente: Elaboración propia con los datos de statista.

Como se puede observar en el gráfico los mayores hackeos de la historia se han cometido recientemente, esto nos permite verificar la importancia creciente de la ciberseguridad. Otro aspecto a destacar es el caso de la entidad Yahoo!, empresa que se ha sido multada recientemente por ocultar la brecha de ciberseguridad que poseía durante el plazo de dos años, de ahí que sea la plataforma tecnológica con un mayor número de cuentas hackeadas.

3.1. Evolución de los ciberriesgos.

Como se ha venido recogiendo a lo largo del trabajo la cuestión ya no es si se va a producir un incidente cibernético, sino cuándo. Actualmente las empresas se han convertido más dependientes de la tecnología que nunca. Antes era más sencillo protegerse ante los ciberataques debido a la cantidad relativamente pequeña de dispositivos que estaban expuestos, ahora el fuerte avance de la evolución tecnológica hace que el número de objetivos aumente considerablemente.

La evolución de los ciberataques ha llevado a un aumento de la demanda de los ciberseguros y ha puesto en evidencia la necesidad de una adecuada gestión de los ciberriesgos.

3.1.1. Tendencias en 2018.

Los hechos anteriores hacen indicar que en el año 2018 se producirán una serie de acontecimientos[28]:

- Existencia de un mercado caracterizado por su elevada competitividad.
- Incremento del número de seguros cibernéticos globales.
- Disminución de las primas en las organizaciones que hayan mejorado sus políticas de ciberseguridad.
- Asociación entre aseguradoras y empresas especializadas en análisis de datos para optimizar los datos de exposición al ciberriesgo.
- Creación de nuevos productos de seguridad que cumplan el nuevo Reglamento General de Protección de Datos.
- Aumento de la capacidad en algunos mercados (EE. UU., Reino Unido y Asia).
- Continuación de la preocupación de la concentración de los riesgos por parte de las aseguradoras.
- Creación de productos de seguros a medida (personalizados).

3.1.2. Tendencias de las amenazas globales en ciberseguridad.

Las amenazas cibernéticas que más preocupan para el futuro debido a su alto grado de probabilidad de ocurrencia son:

Ciberespionaje (muy probable)

Es una medida que ha aumentado mucho debido a su eficiencia y su dificultad de atribución. Las principales características del ciberespionaje son:

- Tiene su origen en los estados, industrias o empresas.

[28] Willis Update (2018). Tendencias en Ciber Riesgo 2018. Recuperado el 06 de junio de 2018 de https://willisupdate.com/tendencias-en-ciber-riesgo-2018/.

- Están dirigidos contra el sector público y el privado.
- Tienen una enorme dificultad de atribución.
- Persigue obtener ventajas económicas, políticas, estratégicas o sociales.

Por ello, se han establecido una serie de recomendaciones como consecuencia de la peligrosidad de las campañas de espionaje:

- Aumentar la vigilancia en redes y sistemas.
- Establecer herramientas de gestión centralizada de registros, incluyendo la correlación de eventos y la monitorización.
- Diseñar una adecuada política de seguridad corporativa.
- Utilización de redes y equipos certificados, seguros.
- Incrementar y automatizar el intercambio de información entre los equipos de repuesta a los ciberataques.
- La Dirección debe asumir que existen riesgos y establecer políticas de seguridad para los mismos.
- Formar y sensibilizar a los miembros de la organización para que tomen conciencia de la exposición al riesgo y tomen las medidas adecuadas.
- Cumplir con la legislación y buenas prácticas vigentes.
- Trabajar como si la organización estuviera o fuera a ser inminentemente atacada.

Ataques como servicio (muy probable)

Consiste en la contratación de un grupo de personas con conocimientos y capacidad técnica para la realización delitos de forma eficaz.

Fusión de tácticas, técnicas y procedimientos utilizadas en ciberataque y ciberdelincuencia (muy probable)

En los últimos años ha habido un aumento sustancial del número de ataques consistentes en una fusión de código dañino y método propio y que tiene como objeto a las entidades financieras para el robo de dinero de diferentes formas:

- Manipular los sistemas informáticos para ordenar transferencias.

- Control remoto de los cajeros automáticos.
- Realización de transferencias de las cuentas de los clientes.

Ataques Hacktivistas (muy probable)

Se espera una continuación en los ataques de esta serie de grupos.

Herramientas de ataque a dispositivos móviles (probable)

Además de las actuales amenazas se espera que aumenten el número de vulnerabilidades especialmente graves en dispositivos móviles, plataformas y aplicaciones.

Ransomware (muy probable)

Actualmente se está asistiendo a una expansión de estos ataques consistentes en solicitar a los atacados una elevada cantidad de dinero a cambio de descodificar la información que le había sido previamente cifrada por los atacantes. Ahora se está empezando a pedir una menor cantidad por los rescates y se está empezado a liberar la información de verdad no como antes, esto está haciendo que los ingresos por este ciberataque hayan aumentado cuantiosamente.

Ataques a cajeros automáticos (probable)

Es probable que se produzca un aumento de los ataques a cajeros automáticos debido a que se ha evidenciado que estos dispositivos son muy vulnerables.

Amenazas a dispositivos móviles (muy probable)

Como consecuencia de la gran comercialización de nuevos accesorios para los dispositivos móviles con medidas de seguridad más avanzadas la tendencia en los ataques parece indicar que serán de una forma más compleja, avanzada y profesional.

Ataques contra infraestructuras críticas (posible)

Son especialmente vulnerables debido a que combinan tecnologías antiguas con una superficie de ataque cada vez mayor. Los objetivos más probables para los ataques son las redes de energía eléctrica y las grandes cadenas de fabricación.

Ataques contra el "Internet de las cosas" (probable)

A pesar de que los ataques contra el "Internet de las cosas" no han sido muchos, a medida que un mayor número de estos dispositivos estén conectados su seguridad será menor y en concreto su privacidad.

3.1.3. Retos en materia de ciberseguridad.

Uno de los principales desafíos es continuar el camino establecido por el Gobierno español durante los últimos años, basado en continuar adaptándonos a la gobernanza de la UE en materia de ciberseguridad, compartir información entre las entidades afectadas tanto privadas como públicas, gestionar la crisis y mejorar la cultura de ciberseguridad.

La ciberseguridad se tiene que caracterizar por la gestión del talento, la organización y la innovación. Hay que hacer frente de una forma correcta a los ciberatacantes ya que esto es la clave para determinar quién gana o quien pierde en un futuro inmediato.

Existe una gran necesidad de mejorar la notificación de los incidentes de ciberseguridad. La notificación de los sucesos es fundamental, pero el proceso no debe de ser un proceso rígido donde se tenga que notificar en muchas ventanillas con diferentes baremos, eso no lo hace ágil, hay que compartir la información de una forma que esta no sea una crisis en sí misma, hay que basarse en la confianza. Notificar es bueno, pero hay que decidir qué notificar debido a que cada entidad lo mide de una forma distinta.

También es muy necesario un proceso bien definido para la clasificación de los eventos y mucha cooperación entre las organizaciones.

3.2. Evolución de los sistemas de detección de intrusos.

En los últimos 20 años los sistemas de detección de intrusos (IDS) se han convertido en uno de los elementos fundamentales de la arquitectura de la seguridad de una red informática.

El periodo en el que se inicia públicamente el tratamiento de las tecnologías de sondeo de las intrusiones es en 1987 con la publicación del artículo de D. E. Denning[29].

Los Sistemas de Detección de Intrusos (IDS) a pesar de estar muy relacionados con las investigaciones universitarias, surgieron principalmente en el ámbito militar. No es hasta finales de los años 80 cuando muchas universidades comenzaron a realizar proyectos centrados en la detección de intrusos.

A comienzos de los noventa internet sale del contexto puramente académico y militar y se convierte en la estructura informática más grande del planeta, dejando en un segundo lugar el problema de la seguridad como consecuencia de su gran usabilidad y de que la gran mayoría de los ataques estaban encaminados hacia una élite exclusiva debido a que todavía no estaba a disposición de todo el mundo.

Con el tiempo los ataques se convirtieron en más difíciles de detectar, más fáciles de realizar y más accesible para todos. Se comienza a hacer visible el fracaso de la seguridad utilizando solo un dispositivo y los IDS comienzan a convertirse en elementos fundamentales en la seguridad.

La tecnología IDS comienza a actualizarse y aparecen unos primeros sistemas que integran el *firewall* (sistema encargado de bloquear el acceso no autorizado) al IDS, lo que hace que la línea de separación entre los sistemas de detección y los de contramedidas se haga más fina. Los IDS comienzan a responder directamente a los ataques convirtiéndose así en sistemas de prevención.

[29] Denning, D. E (1987). An Intrusion Detection Model. IEEE Transactions on Software Engineering, Vol SE- 13, No. 2, 222-232.

Los primeros años del 2000 se caracterizan por estancamiento en la investigación y el desarrollo de los IDS, comienza a haber serias dudas de la validez de estas tecnologías. Otro de los factores que afectan negativamente a la implantación de los IDS es su coste, no basta solo con comprar e instalar la tecnología, sino que además hay que tener un grupo interno encargado del monitoreo. Los costes se convierten en insostenibles a no ser que poseas un IDS y un equipo propio.

Hoy en día lo más demandado es un todo en uno, que integre en una sola aplicación el IDS, el *firewall* y el antivirus. Se pasa de los sistemas de detección pasivos a los sistemas de detección activos (IPS) que actúan a la vez en los 2 y 3 niveles de secuencia protocolaria.

En el año 2003 ya se hace evidente que los sistemas tradicionales de IDS no son siempre adecuados y que estos mismos requieren un proceso de actualización de forma continua.

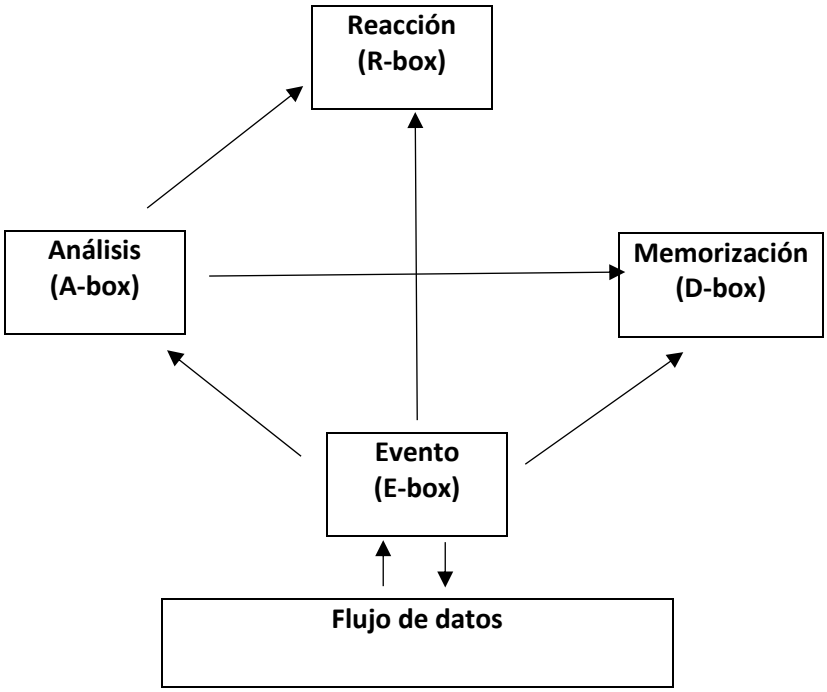
Ahora los IDS ya no son considerados una tecnología innovadora, ahora son considerados unos productos maduros. Los IDS requieren un mayor trabajo respecto a otros equipos de seguridad, debido a que su puesta en marcha de una forma desorganizada puede llevar a generar numerosos hechos inútiles.

Las métricas más relevantes a la hora de valorar un IDS son:

- Número de falsos positivos: son hechos que el IDS considera que son significativos pero que por el contrario no tienen ningún efecto.
- Número de falsos negativos: son hechos que el sistema no logra identificar y que son dañinos para la entidad.
- Capacidad de carga: mide la eficiencia, valora el máximo de carga que puede soportar el IDS manteniendo de forma intacta su capacidad de análisis.

Un IDS está compuesto por 4 elementos esenciales:

Gráfico 3.1: Elementos esenciales de in IDS.



Fuente: Elaboración propia.

- E-Box: es el sensor encargado de realizar la interfaz con el sistema de modo pasivo con el fin de capturar todas las informaciones relevantes para el análisis.
- A-Box: es el elemento principal de la realización del análisis y determina si se ha cometido o no el ataque.
- D-Box: es el sistema encargado de almacenar todo aquello que ha ocurrido.
- R-Box: es el sistema que se encarga de reaccionar frente a la amenaza pudiendo emitir una señal al personal de monitoreo o ejecutando el mismo una acción frente al ataque identificado

Desde los años noventa las innovaciones en el ámbito militar y académico en los productos de seguridad comenzaron a implantarse directamente en el ámbito comercial, pero este paso suele generar problemas. Para dar solución a los mismos todo sistema de seguridad es apoyado con varias tecnologías específicas que intentan reducir la incidencia de los falsos positivos y negativos.

El problema más drástico en el contexto de los IDS son los falsos negativos ya que hace posible modificar de un modo más o menos arbitrario la forma de ataque sin variar el quid del ataque.

Otro gran problema de los IDS es que si no están bien configurados tienden a generar un gran número de alarmas. Una posible solución a este problema sería el análisis del protocolo que hace reducir el número de falsos positivos eliminando las alarmas que no son admisibles. Otra posible solución al problema de los falsos positivos es la utilización de sistemas multiniveles que contrasten las informaciones obtenidas con el IDS con otras fuentes.

A partir del año 2003 las actividades de investigación y desarrollo se han encaminado hacia 3 proyectos:

- EAGLE: proyecto centrado en la creación de prototipos de nuevas tecnologías caracterizadas por su flexibilidad y escalabilidad utilizadas para ámbitos tradicionales.
- RDS: proyecto relacionado con los problemas de la red *backbone*, pone el énfasis en los posibles ataques sobre la infraestructura, en concreto, en los procesos de encaminamiento.
- *Network*: proyecto dedicado a garantizar la seguridad de las redes inalámbricas.

4. Los ciberriesgos en las entidades financieras.

Los peligros de los ciberriesgos para las entidades financieras que antes se tomaban como una exageración, ahora son toda una realidad. En el año 2015 el número de robos a las entidades financieras a través del *malware*[30] aumentó un 80%. Este mismo año otro estudio reveló que las entidades con un mayor número de pérdidas por estos robos han sido el sector financiero, seguidos de los servicios públicos y del sector energético.

La mayoría de los ataques a las entidades financieras no suelen ser denunciados para no dañar su reputación, debido a que la confianza es un

[30] Camilo, M. (2017). Cybersecurity: Risks and management of risks for global Banks and financial institutions. Journal of Risk Management in Financial Institutions, 10 (2), 196-200.

elemento esencial en este sector. El primer caso público en el que los afectados eran directamente los clientes como consecuencia de un ataque informático se da en diciembre de 2016 en un banco inglés, en este caso, el dinero fue aparentemente robado de las cuentas de los clientes, inmediatamente el banco congeló las transacciones y se comprometió a reembolsar las pérdidas ocasionadas a los clientes.

Las entidades no quieren que se haga público el ataque y quieren la más absoluta confidencialidad, es por eso, que uno de los mayores desafíos es la llamada "*dark web*", una red cuyas principales características son que es un sitio oculto y de muchísima dificultad a la hora de rastrear quien la utiliza. En esta web es donde se suele publicar la información robada para los distintos fines ya sea para su venta, para dañarla imagen de la entidad, o para otros propósitos.

Para las entidades financieras la seguridad cibernética tiene que ser una preocupación vital.

Como consecuencia del aumento de la importancia del ciberriesgo en las entidades financieras, el Banco Central Europeo (BCE) ha elaborado unos nuevos exámenes destinados a las entidades financiaras de la zona euro con la finalidad de mejorar la resistencia y resiliencia ante los ciberataques.

Esta decisión que todavía no tiene fecha de partida, se basará en la perpetuación de unos test voluntarios a las entidades bancarias que consideren las diferentes entidades supervisoras de cada país. Lógicamente el BCE remarcará la importancia de realizar dichos test en determinadas entidades antes que en otras.

Los dos principales objetivos que tiene esta medida en fomentar la colaboración transfronteriza en materia de ciberamenazas y mejorar la resistencia ante las mismas.

La prueba consiste en tres fases:

- En la primera se prepara a la entidad para el test de ataque.
- En la segunda se realiza dicho test de ataque.
- En la tercera se elabora un informe con los resultandos alcanzados.

Los resultados que proporcionen estas pruebas no serán los de un aprobado o un suspenso, sino que más bien permitirán a las entidades conocer sus principales fortalezas y debilidades frente a las ciberamenazas.

Los principales riesgos que afectan a las entidades financieras son:

- **Robo de información:** es uno de los principales peligros, implica la sustracción de información acerca de datos confidenciales sobre su estructura, clientes, facturación, modelo de negocio, entre otros.
- **Filtrado de la información:** son conocidos como fugas de información o *leaks*. El filtrado de información sensible puede llevar a ocasionar grandes pérdidas económicas y reputacionales.
- **Secuestros de información:** son conocidos como *ransomware,* se basa en cifrar todos los documentos de los dispositivos con una sola clave que solo conocen los atacantes, y por la cual, solicitan un rescate económico.
- **Daños en la imagen y reputación de la entidad:** se trata de ataques encaminados a dañar la imagen de una organización, son conocidos como *defacement*.

Como consecuencia de la gran cantidad de datos que maneja una entidad financiera el robo de estos causaría una inconmensurable pérdida reputacional. Y debido a que un banco hoy en día es imposible que trabaje sin tecnología, sufre una elevadísima exposición a una enorme pérdida económica como consecuencia de la interrupción de su negocio (*Business Interruption* o BI). Además, si esta interrupción se produce en la nube encargada de la provisión de servicios, el problema se agrava, ya que provoca que cientas de entidades se vean afectadas.

El riesgo más temido por las entidades financieras es el de interrupción de negocio cuyo crecimiento es el más rápido de entre todos los ciberriesgos y cuyo impacto es muy difícil de medir. Esta dificultad de estimación se debe a que no se puede realizar a través de datos históricos como se haría en el caso una violación de datos, sino que los costes de este riesgo dependen de varios factores:

- Detalles del evento cibernético.

- Modelo de negocio de la entidad.
- Respuesta de la entidad a la interrupción.

Ante este tipo de evento, un análisis de escenarios permite generar una base de datos hipotéticos permitiendo así calcular el coste resultante. El análisis de escenarios para cuantificar la pérdida por BI se basa tres puntos claves:

- Estimar de forma precisa la probabilidad y severidad de la BI en la entidad financiera.
- Establecer las opciones de mitigación del riesgo.
- Determinar las opciones de transmisión del riesgo. Las opciones de mitigación y transmisión tienen que ser complementarias y estar perfectamente coordinadas.

Centrarse en el logro de estos tres puntos permitirá a la entidad desarrollar una gestión del riesgo de interrupción de negocio de una forma eficaz.

5. Medidas de prevención

La mayoría de las personas no son conscientes del número de perfiles y cuentas que tenemos abiertas en internet y que constituyen nuestra identidad digital.

El aumento del riesgo de sufrir un ciberataque es tal que la UE ha redactado una Directiva[31] que obliga a los países miembros a tomar medidas para el control y el intercambio de información sobre los ataques cibernéticos.

Los gobiernos están tomando medidas de seguridad para proteger la información de sus actividades estratégicas.

La ciberseguridad no es un problema aislado como lo era antes, ya no es un tema que solo concierne a ciertas unidades especializadas sobre sectores específicos, sino que es un problema para toda la sociedad. Todo el mundo se puede ver afectado por un ciberataque.

[31] DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

El mayor peligro para las organizaciones hace diez años venía de un hacker con ganas de aprender nuevos conocimientos o técnicas, pero, actualmente, la principal motivación de los ciberataques es el lucro económico. Hoy en día, las acciones delictivas que se realizan en la red suponen el 0,8% del PIB mundial[32].

En los últimos años ha aumentado el número de noticias en los medios de comunicación acerca de ciberataques. Ataques cometidos por organizaciones criminales contra la banca y grandes organizaciones de alto perfil no han sido publicadas y se ha detectado que han estado bajo ataques encubiertos durante años. Este aumento de los ataques y el conocimiento de que algunas organizaciones han sido pirateadas durante periodos largos de tiempo sin saberlo han llevado a una necesidad de reevaluar los sistemas de seguridad del pasado.

En la actualidad, el ataque está garantizado, la cuestión ya no es si van a atacar o no, sino cuándo. Se hace evidente que la seguridad cibernética necesita evolucionar ya que los recientes ciberataques han sido operaciones activas durante casi una década. Por estas razones es muy importante no sólo aprender de los ataques pasados sino mirar hacia los ataques futuros.

La ciberseguridad necesita una reestructuración total de arriba debajo de cómo la información está administrada y protegida.

La actual seguridad cibernética se caracteriza por un aprendizaje continuo ya que existe un conflicto permanente con unos ataques en constante evolución. Además, el coste de los ciberataques no deja de caer, a diferencia de la seguridad cuyo coste no deja de aumentar. Ahora tiene una menor importancia la protección de la información y se le da más importancia al control operacional y la confianza de los sistemas.

En España en el año 2006 se creó el CCN-CERT con el fin de gestionar los incidentes cibernéticos que afectan al sector público y a las entidades de interés estratégico del país. Es el centro nacional encargado de recibir las

[32] Agencia EFE (2016). El ciberdelito mueve el 0,8 por ciento del PIB mundial al año, según Intel Security. Recuperado el 17 de julio de 2018 en https://www.efe.com/efe/america/tecnologia/el-ciberdelito-mueve-0-8-por-ciento-del-pib-mundial-al-ano-segun-intel-security/20000036-2877620.

alertas y dar respuesta ante los ciberriesgos. Ofrece apoyo operativo y técnico en las diferentes etapas del proceso (detección, análisis, notificación, respuesta, tratamiento y erradicación), facilitando una respuesta rápida y eficiente frente a las ciberamenazas, de esta forma contribuye a la mejora de la ciberseguridad española.

El país con una mayor conciencia de riesgos cibernéticos es EE. UU., donde existen estrictas leyes sobre protección de datos. Otros países que también tienen una fuerte regulación son Hong Kong, Singapur y Australia. En la Unión Europea la legislación es muy estricta pero cambia en función del país, si bien cabe destacar que existe una tendencia general en crear reglas más estrictas para reforzar la seguridad. Existen propuestas para establecer multas entre el 2% y el 5% de volumen total de negocio de las entidades[33], ante infracciones graves en protección de datos.

En materia de seguridad es muy recomendable tener establecido previamente un plan de contingencia para ser utilizado en el momento en el que se produzca el ataque, de esta forma se conocerá perfectamente qué hacer y cómo.

Realizando una adecuada gestión de los ciberriesgos es estimado que el 80% de los ciberataques[34] puede ser prevenido o mitigado.

A continuación, se muestran los principales sistemas de prevención frente a los ciberriesgos.

5.1. Herramientas del CNI[35].

El CCN-CERT ha realizado un transcendental esfuerzo para la integración y el desarrollo de herramientas propias que faciliten a toda la comunidad la gestión de la ciberseguridad.

[33] Allianz Global Corporate & Specialty (2015). A Guide to Cyber Risk. Recuperado el 14 de Junio de 2018 en https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.
[34] Allianz Global Corporate & Specialty, op. Cit. (2015). Pg 14.
[35]Centro Criptológico Nacional (2015). Informe de Actividades. Recuperado el 07 de julio de 2018 en https://www.ccn-cert.cni.es/documentos-publicos/2160-memoria-de-actividad-2015-2016-version-paginas-enfrentadas/file.html.

Existen diferentes herramientas en función de la etapa del proceso y su finalidad.

Gráfico 5.1: Herramientas de gestión de ciberriesgos.

Fuente: Elaboración propia.

CARMEN

Herramienta creada en el año 2013 que permite capturar y detectar el tráfico de datos que circulan por la red de una forma anómala. En el año 2016 ya estaba siendo utilizada por más de 25 entidades, permitiendo detectar 45 incidentes categorizados como críticos o muy peligrosos.

CLARA

Herramienta de auditoría desarrollada en el año 2014 que permite de una forma continuada la valoración del nivel de seguridad de los sistemas. Esta herramienta solo funciona para sistemas Windows.

CLAUDIA

Herramienta de auditoría encargada de mejorar las técnicas de seguridad de los entornos clasificados. Su orientación es la explotación y almacenamiento de datos de auditoría, permitiendo también el almacenamiento de otro tipo de información sin ningún perjuicio.

INES

Esta herramienta tiene como finalidad facilitar los procesos de todos los organismos en el momento de evaluar regularmente el estado de seguridad de los sistemas.

LORETO

Instrumento de compartición encargado del almacenamiento virtual de datos, aplicaciones, archivos e intercambio de información con los mismos colaboradores.

LUCIA

Creada en el año 2015, esta herramienta se encarga exclusivamente de la gestión de los incidentes cibernéticos de las entidades del ámbito de aplicación del Esquema Nacional de Seguridad.

MARIA

Permite el análisis de todo tipo de *malware,* para ello utiliza líneas de comando de diferentes motores de antivirus y de antimalware.

MARTA

Herramienta de análisis que se encarga del estudio automatizado de diversos tipos de ficheros que podrían tener algún efecto dañino.

Sus principales ventajas son:

- Permite una detección precoz de las amenazas derivadas de código dañino.
- Mediante un sistema de etiquetas permite una organización más ágil y visual de los ficheros, reglas y análisis.
- Creación de un lugar seguro y centralizado en el cual poder almacenar las muestras de *malware* con un instrumento de búsqueda avanzada y de un modo organizado.

PILAR

Creada en el año 2006 se encarga del análisis y la gestión de los riesgos. Existen diferentes variedades:

- PILAR: versión íntegra del instrumento.
- PILAR Basic: versión más sencilla dirigida a pymes y Administración local.
- μPILAR: versión reducida, destinada a la ejecución de análisis de riesgos muy rápidos.
- RMAT (Risk Management Additional Tools): personalización de instrumentos.

REYES

Desarrollada en el año 2016 con la finalidad de agilizar las tareas de análisis e investigación de ciberataques y compartir información sobre los mismos. Este instrumento facilita el acceso a cualquier base de datos relacionadas con incidentes de ciberseguridad. Gracias a esta herramienta se ha producido una mejora sustancial en el intercambio de información entre organismos públicos, entidades de interés estratégico y sistemas similares de otros países.

ROCIO

Se crea para el análisis de las configuraciones de los *routers*, dispositivos de red y conmutadores Cisco. Esta herramienta permite seleccionar distintos paquetes de reglas, crear informes de cumplimiento y almacenar configuraciones.

VANESA

Es una plataforma de retransmisión de vídeo en directo desarrollada para facilitar la tarea de formación y sensibilización con la comunidad de referencia. Con la retransmisión en directo se consigue una reducción de los desplazamientos, tanto en reuniones, como en cursos de formación.

5.2. Ciberseguros.

El comienzo de la preocupación por la ciberseguridad comenzó con la idea que se tenía sobre el gran fallo informático que se iba a producir en el año 2000, lo que hizo que muchas entidades comenzaran a valorar el potencial daño que causaría el ciberriesgo en sus negocios.

Las empresas comenzaron a ser más conscientes de sus exposiciones cibernéticas y comenzaron a asegurar los posibles accidentes mediante coberturas.

El siguiente paso en el desarrollo del ciberseguro se produce en EE. UU. con una mayor legislación en materia de protección de datos, lo que hizo que se comenzaran a comercializar productos enfocados a cubrir las posibles infracciones en materia de privacidad. Estas políticas se desarrollaron y comenzaron a incluir la gestión de crisis y la respuesta experta en el seguro.

Actualmente se está produciendo el tercer paso con el desarrollo de un mercado de ciberseguros cohesionado, se está produciendo una creciente toma de conciencia internacional en ciberriesgos y ya no se está limitando exclusivamente a EE. UU.

Hoy en día se estima que el mercado de la seguridad cibernética tiene un valor cercano a los 2.000 millones[36] de dólares en primas en todo el mundo, a pesar de que sólo un 10% de las empresas[37] compran productos de este tipo. Pero esto no acaba aquí, se espera un crecimiento anual de dos dígitos que supondría que en los próximos 10 años se llegara a la cifra de los 20.000 millones[38] de dólares.

Los sectores en los que es más probable que se adquiera este tipo de servicios son los que trabajan con grandes volúmenes de datos personales y aquellos que tienen un alto grado de digitalización (salud, banca, consultoría, telecomunicaciones, venta minorista…). También hay un interés creciente como consecuencia de los problemas que genera la interconectividad de sectores como el energético, el financiero, el transporte y los servicios públicos.

El mercado de los ciberseguros continuará creciendo, pero se tendrá que enfrentar a numerosos conceptos y expresiones que aún están por conocer.

Los seguros ofrecen coberturas ante:

- Responsabilidades de terceros, tanto legales como regulatorias, así como los costes asociados a la respuesta ante esa violación.
- Litigios derivados de la difamación en una web o red social.
- Violación de datos almacenados.
- Delitos cibernéticos, incluidos el robo y la extorsión.
- Interrupción de negocio.

Este último es uno de los grandes avances en ciberseguridad como consecuencia de su importancia. Es posible contratar un seguro tanto para exclusivamente la interrupción de negocio como para la misma y a demás la violación de los datos, que cubra la interrupción total o parcial frente a un ataque cibernético, fallo técnico u operacional. Cualquier paralización en el negocio, incluso la más leve de un minuto, puede causar graves impactos en el balance de cualquier empresa.

[36] Allianz Global Corporate & Specialty, op. Cit. (2015). Pg 24.
[37] Allianz Global Corporate & Specialty, op. Cit. (2015). Pg 24.
[38] Allianz Global Corporate & Specialty, op. Cit. (2015). Pg 24.

El fin de la póliza de seguro cibernético es otorgar amparo respecto determinados actos dolosos de terceros cometidos contra el cliente asegurado que resulten en pago, transferencia o entrega de bienes o dinero.

Para la contratación de estos seguros es necesario realizar un proceso de suscripción y selección de riesgos por parte de las aseguradoras, consistente en la realización de test de penetración por parte de las entidades especializadas (*"ethical Hacking*").

Hoy en día existe una brecha en los ciberseguros que es el daño físico ante un ciberataque. Este no es cubierto por los seguros por la gran dificultad que supone localizar el origen del equipo afectado.

La volatilidad en el precio de los seguros y la segmentación del mercado continuarán creciendo como consecuencia de que hoy en día no hay suficientes datos para medir de forma completa el riesgo, a pesar de que el mercado tiene mucha capacidad.

Para finalizar es importante mencionar que el seguro no es un reemplazo para una buena seguridad, sino que es un complemento. No consiste en contratar el seguro y olvidarse de la ciberseguridad, sino que tienen que ir de la mano.

5.3. Ciberinteligencia.

Cada vez más empresas integran servicios y herramientas de inteligencia en la ciberseguridad, con ello consiguen no solo reforzar la protección de sus infraestructuras y sistemas, sino también mejorar la detección. Es imposible establecer técnicas de defensa sin tener inteligencia, es decir, es necesario conocer quién puede atacar y en qué momento, qué procedimiento y qué técnicas utiliza, desde dónde ataca y cuál es su motivo.

La demanda de inteligencia está creciendo de forma exponencial, tanto en las empresas grandes que cuentan con numerosos equipos internos pero que contratan a diferentes proveedores piezas concretas para elaborar su propia capacidad de inteligencia, como las empresas más pequeñas que prefieren la solución en mano, actualmente centrada en inteligencia asociada a su exposición digital.

El papel de la ciberinteligencia es mejorar la capacidad de detección y respuesta, a través la investigación la vigilancia, utilizando las herramientas y las personas adecuadas. Es por ello por lo que es fundamental para la ciberseguridad.

El ciclo de inteligencia adaptado a la ciberseguridad se basa en 4 etapas:

- Identificación de la víctima: proceso mediante el cual se determina las fortalezas frente al ataque y las debilidades que le han permitido.
- Capacidades técnicas del atacante: consiste en determinar las herramientas utilizadas por el atacante, su capacidad de ocultación y persistencia, los vectores de infección utilizados y la capacidad de despliegue por la red.
- Infraestructuras utilizadas: se trata de identificar si los medios utilizados son propios o alquilados, cuál es su avatar y su fin.
- Identificación final del atacante: se cataloga el tipo de agente que lo realiza, su objetivo, su elección del objetivo, su técnica y sus operativas.

Actualmente existen 3 técnicas que ayudan al avance de la inteligencia:

- Bases de datos NoSQL: son bases de datos que no requieren estructuras fijas.
- *Machine Learning:* sistemas que configuran algoritmos automáticamente, “aprenden” automáticamente.
- Big Data: conjunto de datos cuyo tamaño, velocidad de crecimiento y complejidad imposibilita el procesamiento mediante herramientas convencionales.

Las principales ventajas de utilización de la inteligencia en la ciberseguridad son:

- Poder mejorar la capacidad predictiva de una organización al compartir y trabajar información interna con datos externos relevantes.
- Mejora la visibilidad de la información, muy necesario debido a que existe una gran cantidad de datos.

- Detectar y entender una amenaza de forma rápida generando datos significativos a través de actividades vinculadas a personas, aplicaciones, datos e infraestructuras.
- Conectar distintos eventos entre sí, mediante la colocación de todos los datos dentro de un mismo repositorio, permitiendo identificar las actividades que se encuentran fuera de lo normal y elaborar planes para poner solución a esas amenazas.

Los principales inconvenientes son las dificultades de categorizar correctamente los términos y de poder priorizar y gestionar los enormes volúmenes de información, para poder obtener conclusiones que aporten valor.

5.4. Intercambio de información.

Existen diferentes métodos como el "*information sharing"* cuyo objetivo principal es la creación de un procedimiento que permita el almacenamiento, la recopilación y la distribución de la información necesaria para reaccionar de forma rápida, homogénea y eficaz contra las ciberamenazas.

Los beneficios que genera la compartición de la información son:

- Generar una conciencia de estado global de seguridad.
- Maduración del conocimiento a través del intercambio de las lecciones aprendidas.
- Prevención a través de la información generada por otras entidades, evitando situaciones de riesgo y actuando sobre las mismas.
- Respuesta ágil al conocer ya como han resultado los procedimientos aplicados anteriormente.

Compartir información y trabajar en conjunto entre equipos de respuesta facilita la creación de una inteligencia global que hace mejorar la actuación preventiva, clave para afrontar las nuevas amenazas cibernéticas que son cada vez más complejas.

Pero la puesta en marcha de un proceso de compartición de información no es fácil, hay que superar una serie de barreras como el establecimiento de una red

de confianza, llegar un consenso para establecer el formato en el que facilitar la información, y superar el recelo de compartir la información.

A continuación, se muestran las principales barreras para la compartición de la información:

Aspectos técnicos: es la barrera más común. Suelen estar relacionados con si el método utilizado en un caso sirve para los demás o si la información que se genera de un caso es relevante para los demás o no.

Aspectos legales: es otra de las barreras más frecuente y consiste en la incertidumbre respecto a si la información intercambiada presenta problemas en materia de protección de la privacidad y de datos, debido a que dentro de la UE la compartición de datos está muy restringida por la legislación.

Confianza: en un elemento clave en ciberseguridad para que la cooperación sea exitosa. Es frecuente que la cooperación entre centros privados sea escasa debido a que si se comparte la información puede hacer que una entidad no invierta en investigación y se aproveche de la información que comparten las demás. La confianza se debilita si sólo una de las partes está activa en la cooperación. Otro de los factores por los que no se comparte la información es por el daño reputacional que puede acarrear conocer que la entidad ha sido víctima de un ataque.

Interés: no es frecuente que exista desinterés por las partes. En cambio, como consecuencia de una excesiva carga de trabajo es probable que el proceso de compartir la información se demore en el tiempo. La carga de trabajo es un inhibidor importante.

Otra forma de compartir la información podría ser mediante consorcios, que son la unión de varias entidades con el fin de conseguir un objetivo conjunto, en este caso sería el de mejorar la gestión del riesgo mediante el intercambio de información relevante del mismo.

Un ejemplo de consorcio es ORX, asociación sin ánimo de lucro creada por entidades financieras en el año 2002 gestionada por sus miembros. Fue creada con el objetivo de intercambiar información de alta calidad acerca de eventos relacionados con el riesgo operacional de forma segura y anónima para

mejorar la gestión y cuantificación de este riesgo. Actualmente también es un foro de debate sobre la modelización y gestión del riesgo operacional para entidades financieras.

En sus orígenes estaba compuesta[39] por 12 bancos y actualmente son casi 100, posee una base de datos que es la más grande del mundo, cuenta con casi 600.000 eventos.

Su funcionamiento se basa en tres pasos:

- Cada entidad prepara sus datos para su transmisión.
- El custodio realiza el análisis de los datos y el control de su calidad.
- Los informes elaborados son distribuidos a los bancos asociados.

Otro ejemplo de consorcio es CERO: organización formada por los responsables de los departamentos de riesgo operacional de las entidades del sector financiero español desde el año 2003. Se creó con los objetivos de:

- Unificar los criterios de interpretación de las normas.
- Formar grupos de intercambio de experiencias y buenas prácticas entre sus miembros.
- Crear grupos de trabajo para la evolución de la gestión del riesgo operacional.

[39] 25. O.R.X (2018). Operational risk loss data for insurers submitted between 2012 and 2017. Annual Insurance Loss Report. Recuperado el 14 de julio de 2018 en https://managingrisktogether.orx.org/sites/default/files/downloads/2018/07/annual_insurance_loss_report_2018.pdf.

6. CONCLUSIONES.

La investigación y realización de este trabajo me ha permitido alcanzar las siguientes conclusiones:

- El ciberespacio ha introducido una nueva dimensión en la sociedad y su uso se ha incorporado a la vida cotidiana y se ha generalizado.
- No hay independencia en los ataques, ni en cuanto a los objetivos, ni en cuanto a los atacantes. Un ataque dirigido a un sector no afecta sólo a ese sector, sino que puede afectar a otro y un ataque puede ser realizado tanto por un atacante como por varios a la vez.
- Todos los estados y entidades deben asumir un papel primordial a la hora de hacer frente a los ataques contra las TIC y las comunicaciones de las administraciones públicas, gobiernos y empresas estratégicas.
- Si tan sólo una de cada 10.000 personas fuera un ciberdelincuente, existirían 745.000 ciberdelincuentes en el mundo. Por lo tanto no basta solo con la instalación de sistemas de seguridad, sino que hay que mejorar la cultura del ciberriesgo de los usuarios de la tecnología.
- Garantizar la ciberseguridad de nuestros dispositivos, nuestra información y nuestra vida digital es un proceso que requiere un esfuerzo continuo, constante y permanente. Nunca existirá un ciberataque perfecto ni un sistema de seguridad perfecto, sino que tanto el ataque como la defensa irán evolucionando de forma continua.
- Existe la certeza de que se va a ser víctima de un ciberataque, pero no de cuándo.
- El coste real de los ciberataques es muy elevado, en la mitad de las ocasiones supone más de 500.000$.

7. BIBLIOGRAFÍA

1. Adamek, A. P. (1977). *Seguridad y confiabilidad de los sistemas de computación bancaria*. Reunión de Bancos Centrales Americanos. Banco Central de Bolivia, Bolivia.
2. Agencia EFE (2016). *El ciberdelito mueve el 0,8 por ciento del PIB mundial al año, según Intel Security*. Recuperado el 17 de julio de 2018 en https://www.efe.com/efe/america/tecnologia/el-ciberdelito-mueve-0-8-por-ciento-del-pib-mundial-al-ano-segun-intel-security/20000036-2877620.
3. Allianz Global Corporate & Specialty (2015). *A Guide to Cyber Risk.* Recuperado el 14 de junio de 2018 en https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.
4. Allianz Risk Barometer (2017). *Top Business Risks 2017.* Recuperado el 30 de julio de 2018 en https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf.
5. Buczak, A., Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Comunications Surveys & Tutorials*. 18, 1153-1174.
6. Camilo, M. (2017). Cybersecurity: Risks and management of risks for global Banks and financial institutions. *Journal of Risk Management in Financial Institutions, 10* (2), 196-200.
7. CIA, The World FactBook (2012). Recuperado el 14 de agosto de 2018 en https://www.cia.gov/library/publications/the-world-factbook/rankorder/2184rank.html.
8. Corchado Rodríguez, J. M., Villalba Fernández, A. (2017). Análisis de las ciberamenazas. *Dialnet. 185,* 97-138.
9. Centro Criptológico Nacional (2015). *Informe de Actividades.* Recuperado el 07 de julio de 2018 en https://www.ccn-cert.cni.es/documentos-publicos/2160-memoria-de-actividad-2015-2016-version-paginas-enfrentadas/file.html.

10. CISCO (2018). *Informe anual de ciberseguridad de Cisco 2018*. Recuperado el 20 de junio de 2018 en https://www.cisco.com/c/es_es/products/security/security-reports.html.
11. Davis, G., García, A., Zhang, W. (2009). Empirical Analysis of the Effects of Cyber Security Incidents*. Risk Analysis, Vol. 29, No. 9,* 1304-1315.
12. DELTA INSURANCE (2018). *The evolution of cyber threats*. Recuperado el 15 de agosto de 2018 en https://deltainsurance.co.nz/wp-content/uploads/2018/02/Delta-Insurance-Cyber-White-Paper.pdf.
13. Denning, D. E (1987). An Intrusion Detection Model. *IEEE Transactions on Software Engineering*, Vol SE- 13, No. 2, 222-232.
14. ElEconomista (2018). *Más test a la banca: el BCE examinará la resistencia ante los ciberataques*. Recuperado el 23 de julio de 2018 en http://www.eleconomista.es/empresas-finanzas/noticias/9289415/07/18/Mas-test-a-la-banca-el-BCE-examinara-la-resistencia-ante-los-ciberataques.html.
15. ENISA (2017). *ENISA Threat Landscape Report 201715 Top Cyber-Threats and Trends*. Recuperado el 2 de julio de 2018 en https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.
16. Fernández, J. G. (2018). Del 'phishing' al 'ransomware', los desafíos de la ciberseguridad. *Expansión*. Recuperado el 7 de agosto de 2018 de http://www.expansion.com/economia-digital/2018/08/07/5b68bb2c468aeb38088b457b.html.
17. Johnson, Kristin N. (2016). *Managing cyber risks.* Gergia Law Review, vol 50, pg 547-592. Recuperado el 7 de junio de 2018 de http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=10&sid=22eeadff-be7c-4fac-95cf-1f27bb1a8e57%40sessionmgr4010.
18. Lamastra, G., Luca, Viale, I. (2005). Tecnologie innovative per il rilevamento e il contrasto degli attacchi informatici. *Notiziario Tecnico Telecom Italia, 14,* 6-18.
19. Laube, S., & Böhme, R. (2017). Strategic Aspects of Cyber Risk Information Sharing. *ACM Computing Surveys*, 50 (5), 1-36.
20. Marchal, D. (2017). Inteligencia, la mejor estrategia para combatir las ciberamenazas. *Red Seguridad, 75*, 46-50.

21. MARSH (2017). *Tres formas de cuantificar el riesgo de interrupción de negocio por ataque cibernético.* Recuperado el 28 de julio de 2018 de https://www.marsh.com/co/insights/risk-in-context/tres-formas-de-cuantificar-el-riesgo-de-interrupcion-de-negocio-.html.
22. Marsh & McLennan Companies (2018). *Informe de riesgos mundiales*. Recuperado el 31 de julio de 2018 de http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=10&sid=22eeadff-be7c-4fac-95cf-1f27bb1a8e57%40sessionmgr4010.
23. Marsh & McLennan Companies (2018). *MMC Cyber Risk Handbook 2018.* Recuperado el 10 de agosto de https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/mmc-cyber-handbook-2018.pdf.
24. Menon, N., Ogut, H., Raghunathan, S. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, *Vol. 31, No. 3,* 497-511.
25. Narváez Bonet, J E (2015). El contrato del seguro y los contratos de la actividad financiera: Coberturas y tendencias del seguro global bancario, 43 RIS, 49-102. Recuperado el 26 de mayo de 2018 de http://dx.doi.org/10.11144/Javerina.ris43.csaf.
26. OBS Business School (2015). Estudio Big Data 2015. Recuperado el 31 de julio de 2018 en https://www.obs-edu.com/es/noticias/estudio-obs/en-2020-mas-de-30-mil-millones-de-dispositivos-estaran-conectados-internet.
27. O.R.X (2018). *Operational risk loss data for insurers submitted between 2012 and 2017*. Annual Insurance Loss Report. Recuperado el 14 de julio de 2018 en https://managingrisktogether.orx.org/sites/default/files/downloads/2018/07/annual_insurance_loss_report_2018.pdf.
28. Pérez García, P., Rego Fernández, M.A. (2017). El intercambio de información de ciberamenazas. *Dialnet*. *185,* 139-170.
29. K, S, Kwak. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*. 3, 678-703.

30. Willis Update (2018). *Tendencias en Ciber Riesgo 2018*. Recuperado el 06 de junio de 2018 de https://willisupdate.com/tendencias-en-ciber-riesgo-2018/.