



UNIVERSITAT DE  
BARCELONA

**213**

**El impacto de los Ciberriesgos  
en la Gerencia de Riesgos Tradicional**

Estudio realizado por: Sergio López Serrano  
Tutor: Francesc Xavier Monràs Vidiella

**Tesis del Máster en Dirección de Entidades  
Aseguradoras y Financieras**

Curso 2016/2017

Esta publicación ha sido posible gracias al patrocinio de ARAG SE, Sucursal en España



Cuadernos de Dirección Aseguradora es una colección de estudios que comprende las tesis realizadas por los alumnos del Máster en Dirección de Entidades Aseguradoras y Financieras de la Universidad de Barcelona desde su primera edición en el año 2003. La colección de estudios está dirigida y editada por el Dr. José Luis Pérez Torres, profesor honorífico de la Universidad de Barcelona, y la Dra. Mercedes Ayuso Gutiérrez, catedrática de la misma Universidad.

Esta tesis es propiedad del autor. No está permitida la reproducción total o parcial de este documento sin mencionar su fuente. El contenido de este documento es de exclusiva responsabilidad del autor, quien declara que no ha incurrido en plagio y que la totalidad de referencias a otros autores han sido expresadas en el texto.

## **Presentación y agradecimientos**

Primero de todo, agradecer a mi familia y mi pareja que hayan tenido tanta paciencia conmigo, no solo durante el transcurso del máster sino también durante el periodo de elaboración de la tesis.

También quiero agradecer a Seguros Catalana Occidente por darme la oportunidad de participar en este máster donde he podido adquirir nuevos conocimientos y donde he coincidido con personas maravillosas, a las cuales también quiero agradecer que me hayan hecho más llevaderos todos estos meses, viéndome muchos momentos inolvidables.

Para finalizar, también me gustaría dar las gracias a todos los profesores del máster, a Mercedes y a José Luís, por ayudar a dar este impulso al sector y, sobre todo, a los profesionales en el mundo asegurador que han contribuido a la elaboración de la tesis. Mi tutor Xavier Monràs, cuya ayuda ha sido inestimable y siempre ha sido proactivo a la hora de aconsejar; y a Carmen Segovia, cuyos conocimientos y aportes se han intentado incluir dentro del redactado.

Muchas gracias a todos.



## Resumen

La tecnología está transformando el día a día de la sociedad, tanto a nivel particular como a nivel industrial. En las organizaciones puede tener un impacto muy positivo en tanto en cuanto de mejora de productividad, pero puede traer nuevos riesgos. Es por ello que en la Gerencia de Riesgos se debería monitorizar los ciberataques, analizando en todo momento las posibilidades de transferencia de dicho riesgo (generalmente a una compañía aseguradora).

En esta tesis se hace una introducción al concepto “Gerencia de Riesgos”, un análisis de lo que son los ciberriesgos y lo que ellos representan y cómo, la aparición de estos ciberataques, debe hacer evolucionar la Gerencia de Riesgos tradicional.

**Palabras Clave:** Gerencia de riesgos, mapa de riesgos, matriz de riesgos, ciberataques, ciberriesgos, *malware*, *ransomware*, *big data*, cuarta revolución industrial.

## Resum

La tecnologia està transformant el dia a dia de la societat, tant a nivell particular com a nivell industrial. En les organitzacions pot tenir un impacte molt positiu en tant en quant pot millorar la productivitat, però pot portar nous riscos. És per això que en la Gerència de Riscos s’hauria de monitoritzar els ciberatacs, analitzant en tot moment les possibilitats de transferència del risc (generalment a una companyia asseguradora).

En aquesta tesi es fa una introducció al concepte “Gerència de Riscos”, un anàlisi del que són els ciberriscos i el que representen i com, l’aparició d’aquests atacs, ha de fer evolucionar la Gerència de Riscos tradicional.

**Paraules Clau:** Gerència de riscos, mapa de riscos, matriu de riscos, ciberatacs, ciberriscos, *malware*, *ransomware*, *big data*, quarta revolució industrial.

## Summary

Technology is transforming the day-to-day society, both at the particular and industry levels. In organizations can have a positive impact in terms of productivity improvement, but may bring new risks. That is why the Risk Management should monitor cyberattacks, analyzing at every moment the possibilities of transferring such risk (usually to an insurance company).

This thesis introduces to the concept of “Risk Management”, analyze of what cyber risks are, what they represent and how, the appearance of these cyberattacks, must evolve the traditional Risk Management.

**Keywords:** Risk Management, risk map, risk matrix, cyberattacks, ciber risks, *malware*, *ransomware*, *big data*, fourth industrial revolution.



# Índice

<b>1. Introducción .....</b>	<b>9</b>
<b>2. Qué es la gerencia de riesgos.....</b>	<b>11</b>
2.1. Introducción .....	11
2.2. Proceso continuo – importancia del plan estratégico .....	16
2.3. Fases principales de la Gestión de Riesgos.....	19
2.4. Retención y transferencia .....	28
2.5. Costes de la reducción, retención y transferencia .....	33
2.6. Plan de continuidad del negocio.....	34
2.7. ¿Por qué es importante la Gerencia de Riesgos? .....	36
<b>3. Qué es el ciberriesgo .....</b>	<b>39</b>
3.1. Introducción .....	39
3.2. Tipos de riesgos .....	41
3.3. Costes resultantes y etapas de un ciberataque.....	46
3.4. Ejemplos reales .....	51
3.5. Penetración en el tejido empresarial .....	55
<b>4. La cuarta revolución industrial y el <i>Big Data</i>.....</b>	<b>59</b>
4.1. La cuarta revolución industrial .....	59
4.2. Big Data.....	61
<b>5. Impacto de los Ciberriesgos en la Gerencia de Riesgos tradicional.....</b>	<b>63</b>
5.1. Solución aseguradora actual .....	65
5.2. Previsión de futuro.....	71
<b>6. Conclusiones.....</b>	<b>75</b>
<b>7. Bibliografía .....</b>	<b>77</b>





# El impacto de los Ciberriesgos en la Gerencia de Riesgos Tradicional

## 1. Introducción

En la actualidad, la sociedad está viviendo una era tecnológica y en constante evolución. Todo ello hace que cada vez más se utilicen los dispositivos electrónicos en la vida diaria (tanto personal como profesional), permitiendo sustituir los documentos físicos tales como hojas de papel, carpetas, agendas etc. por un simple dispositivo móvil que te permite gestionar y transportar toda la información necesaria en el bolsillo del pantalón.

Internet ha cambiado por completo la forma de comunicarse y relacionarse de ciudadanos, empresas y autoridades. Además, se ha convertido en uno de los principales pilares de gran parte de las actividades económicas, cambiando modelos de negocio y la manera de gestionar los peligros que pueden afectar directamente a cualquier organización. Se ha de tener en cuenta de que cada día se plantean nuevos peligros en el ciberespacio y que son difícilmente cuantificables en un futuro a medio y largo plazo, incluso en el corto plazo, debido a su permanente cambio y evolución.

En la actualidad, los principales miedos de la sociedad son los siguientes:

**Ilustración 1. Principales miedos de la sociedad actual**



Fuente: Chubb

Iconos fácilmente reconocibles por todos y que demuestran que realmente la sociedad ha cambiado. Los peligros de quedarse sin conexión, sin batería o de tener que esperar a que algo se cargue son los principales que van en contra de la nueva era, la de la inmediatez en las cosas, en la cual se quiere todo y al momento.

Además, con toda la era tecnológica, los modelos de negocio están cambiando. Por ejemplo, Uber es la mayor compañía de taxis y no tiene ningún taxi en propiedad; Facebook se trata del propietario más famoso de archivos multimedia, sin crear ninguno de ellos; Alibaba es el minorista más valioso, sin tener inventario; y Airbnb es el mayor proveedor de alojamiento del mundo, sin tener ninguna propiedad.

Es por ello que esta nueva sociedad está sufriendo nuevos peligros y amenazas del ciberespacio y de la digitalización, demostrando que se ha de cambiar la manera de gestionar todos estos nuevos riesgos. Se han de replantear todas las estrategias de gestión de riesgos con el fin de que las empresas puedan

aprovechar todas las ventajas de esta nueva era reduciendo al máximo los peligros asociados.

Toda esta exposición a nuevos riesgos puede afectar tanto a organizaciones empresariales, administraciones y particulares, lo cual hace que todas estas figuras deban estar interesadas y permanentemente actualizadas sobre los nuevos riesgos que aparecen, en cómo evolucionan y en la protección contra ellos, dado que hay en juego tanto el futuro de dichas organizaciones como datos sensibles de numerosas personas.

Hoy en día ya no se debe cuestionar si se sufrirá una ciberataque sino cuándo sucederá y si dispondrá de las respuestas adecuadas y necesarias para hacerles frente.

En este punto es donde las compañías aseguradoras y reaseguradoras también tienen un papel importante, y es que el hecho de estar en contacto continuo con un mercado y con unas empresas que sufren y piden soluciones a diario de nuevos riesgos, puede permitir asesorar de forma rápida a todos sus clientes así como ofrecerles productos que ayuden a mitigar el riesgo.

Otro aspecto que se deberá valorar será si las medidas de defensa que ofrecen las aseguradoras cubren en la totalidad o solo en parte los riesgos que debe afrontar una empresa. Ello puede ayudar a la hora de realizar la gerencia de riesgos y, en concreto, en la parte de retención y transferencia de riesgos ya que si una empresa no encuentra soluciones en el mercado asegurador, deberá retener y asumir los peligros derivados del riesgo asociado.

Por lo tanto, de la misma manera que evoluciona el mundo tecnológico, hace que se deba variar todo un conjunto de elementos a su alrededor. Uno de ellos es la gerencia de riesgos en una empresa. Como se verá más adelante, la gerencia de riesgos es uno de los principales pilares sobre los que el valor de la organización se consigue mantener. Es por ello que implementarlo de forma correcta podrá ayudar a su subsistencia en el tiempo.

En este estudio se pretende exponer de qué manera ha variado (o ha de ir variando) la gerencia de riesgos por la aparición de estos nuevos peligros que afectan a la tecnología (también conocidos como ciberriesgos). Para ello se basará en una introducción sobre qué es la gerencia de riesgos, posteriormente se definirá qué es un riesgo cibernético y, finalmente, la conjugación de ambos en la actualidad.

## 2. Qué es la gerencia de riesgos

### 2.1. Introducción

Antes de poder analizar el impacto que pueden tener los ciberriesgos debemos conocer qué es la gerencia de riesgos (también conocida en inglés como *Enterprise Risk Management* o por sus siglas *ERM*).

Para poder entrar en la definición de qué es la gerencia de riesgos, primero debemos definir qué es un riesgo.

#### 2.1.1 Riesgo

La definición de qué es un riesgo puede variar en función de a quién se le formule la pregunta. A continuación se darán dos definiciones. Por un lado, la que hace la Real Academia Española (RAE) y por otro, definiciones de organismos más específicos como FERMA (*Federation of European Risk Management Associations*) o, en España, AGERS (Asociación Española de Gerencia de Riesgos y Seguros).

##### Según la RAE

El término “riesgo” tiene dos acepciones:

- i. Contingencia o proximidad de un daño.
- ii. Cada una de las contingencias que pueden ser objeto de un contrato de seguro.

Y de tal forma, se define “contingencia” como:

- i. Posibilidad de que algo suceda o no suceda
- ii. Cosa que puede suceder o no suceder

Por lo tanto, como definición inicial, se podría decir que, según la RAE, el riesgo es la posibilidad o no de que ocurra un daño y que puede ser asegurable.

##### Según FERMA

Para que, a nivel europeo, se tenga el mismo concepto sobre los diferentes términos que intervienen en la Gerencia de Riesgos, se realizó la ISO/CEI 73:2010<sup>1</sup> (se abreviará como ISO 73) donde se definieron cada uno de ellos y así partir de la misma idea inicial.

---

<sup>1</sup> ISO/CEI 73:2010. Gestión de riesgos - vocabulario: Esta ISO está actualizada a 2010 pero la versión previa de esta versión data de 2002 (se inició su estudio preliminar en el año 2000). Que haga casi dos décadas que se inició lleva a comprobar que los aspectos de gerencia de riesgo tienen importancia y relevancia desde hace un tiempo y que se consideró que era necesario homogeneizar a nivel internacional todos los conceptos intervinientes.

En esta ISO 73, la definición de “riesgo” es la siguiente:

- i. Combinación de la probabilidad (1) de un suceso (2) y de su consecuencia (3).

Dentro de la ISO 73 se hacen tres apreciaciones al respecto:

- i. Destaca que el término “riesgo” suele utilizarse sólo en el caso de que exista, al menos, una posibilidad de consecuencia negativa.
- ii. Indica que en algunas situaciones, el riesgo surge de la posibilidad de desviación con respecto al resultado o suceso previsto.
- iii. Además, insta a revisar la ISO/CEI 51:2014<sup>2</sup> (que se llamará ISO 51 en adelante) para los temas relacionados con la seguridad.

Otras definiciones:

(1) Probabilidad: grado en que un suceso puede tener lugar

(1.1) Número real situado en la escala de 0 a 1 asignado a un suceso fortuito. Grado de creencia de que ocurra un suceso. Para alto grado de creencia, la probabilidad se acerca a 1.

(1.2) Al describir “riesgo”, se puede usar “frecuencia” en lugar de “probabilidad”.

(1.3) Grados de creencia acerca de la probabilidad se pueden elegir como clases o categorías, como:

- Rara / improbable / moderada / probable / casi segura, o
- Increíble / improbable / remota / ocasional / probable / frecuente

(3) Consecuencia: resultado de un suceso

(3.1) Se puede derivar más de una consecuencia de un mismo suceso.

(3.2) Las consecuencias son siempre negativas en aspectos de seguridad.

(3.3.) Las consecuencias se pueden expresar cualitativa o cuantitativamente.

(2) Suceso: ocurrencia de una serie de circunstancias particulares

(2.1) El suceso puede ser cierto o incierto

(2.2) El suceso puede tener una sola ocurrencia o una serie de ocurrencias.

(2.3) Puede calcularse la probabilidad asociada al suceso para un cierto periodo de tiempo.

Por lo tanto, FERMA utiliza directamente lo indicado en la ISO 73 para definir el riesgo como la combinación de la probabilidad de un suceso y sus consecuencias.

---

<sup>2</sup> ISO/CEI 51:2014. Aspectos de seguridad - guía para su inclusión en estándares: se trata de una ISO que data, su primera versión, de 1990; actualizada en 1999 y por última vez en 2014. Trata temas como “seguridad” y “seguro” y el proceso iterativo de reducción del riesgo.

Con todo ello, se puede observar que la definición que ofrece FERMA es muy similar a la que se desprende de la RAE pero con la diferencia de que éste último organismo lo relaciona directamente con conceptos asegurables mientras que desde FERMA se mantienen al margen.

### **2.1.2 Tipos de riesgo**

De tal manera, una vez se ha definido lo que se considera como riesgo, se ha de tener en cuenta de que estos tipos de riesgo pueden ser de una gran variedad.

Para analizar adecuadamente estos riesgos, se ha de tener una visión total de la organización, de 360º, en la cual se debe ser conscientes de que puede haber riesgos presentes que no se conozcan o que no se tengan en cuenta, cuando realmente pueden tener un impacto importante dentro de la empresa.

A grandes rasgos, los principales riesgos que suelen haber se pueden categorizar en cuatro grandes familias, que serían las siguientes:

- Riesgos Financieros
- Riesgos Estratégicos
- Riesgos Operativos
- Riesgos Fortuitos o de Azar

Además, dentro de cada uno de estos cuatro grandes grupos se puede dividir en aquellos riesgos que son por factores externos a la empresa y los que son por factores internos a la misma.

Una imagen/resumen con algún ejemplo de cada uno de los tipos de riesgo podría ser la siguiente:

## Ilustración 2. Factores de riesgo en el ERM



Fuente: FERMA

Todo estos riesgos y aspectos son los que se han de valorar a la hora de realizar la gerencia de riesgos de una empresa. Para ello, se procederá a explicar en qué consiste la gerencia de riesgos y en todo el proceso que ello comporta.

Para este último paso de identificación de riesgos y para el siguiente paso de la gerencia de riesgos, también entran en juego las normas UNE ISO 31000:2010<sup>3</sup> de “Gestión del riesgo. Principios y directrices” y la UNE ISO 31010:2011<sup>4</sup> de “Gestión del riesgo. Técnicas de apreciación del riesgo”.

<sup>3</sup> UNE ISO 31000:2010. Gestión del riesgo. Principios y directrices: la publicación de esta ISO se hizo en el año 2009 y se ha revisado en el 2013 pero llevaba desde el 2005 con propuestas ya que se consideraba necesario tener unas guías estandarizadas y comunes sobre la gestión del riesgo.

<sup>4</sup> UNE ISO 31010:2011. Gestión del riesgo. Técnicas de apreciación del riesgo: se trata de un soporte para la ISO 31000 y da una orientación sobre la aplicación de técnicas sistemáticas para la evaluación del riesgo.

### 2.1.3 Gerencia de Riesgos

Por tanto, una vez se ha definido lo que es un riesgo se puede pasar a analizar, técnicamente, qué es la gerencia de riesgos.

De igual manera que se ha hecho en el apartado anterior, se va a proceder a definir el concepto de “gerencia de riesgos” según la RAE y según FERMA, para analizar si existen diferencias importantes en los conceptos.

#### Según la RAE

Se define “Gerente” como la persona que lleva la gestión administrativa de una empresa o institución.

Por lo tanto, uniendo las definiciones del apartado anterior y de éste, según la RAE, el “Gerente de riesgos” sería el encargado de gestionar la posibilidad de que ocurra un daño y si éste es asegurable o no (tanto por no existencia de cobertura como por no interés económico).

#### Según FERMA

Es el proceso por el que las empresas tratan los riesgos relacionados con sus actividades, con el fin de obtener un beneficio sostenido en cada una de ellas y en el conjunto de todas las actividades.

Además, este organismo se hace eco de la importancia de la gerencia de riesgos indicando que reduce la probabilidad de fallo y la incertidumbre acerca de la consecución de objetivos generales de la empresa. También hace especial mención a que se ha de tratar de un proceso continuo y en constante desarrollo, aplicado a toda la empresa, y teniendo en cuenta los riesgos pasados, presentes y futuros.

En este caso la diferencia entre la RAE y FERMA ya es importante. Éste último organismo ya hace una definición mucho más completa y precisa, entrando en conceptos como “objetivos”, “estrategia” y, sobre todo, un término que no se ha de olvidar nunca que es el de “continuo análisis”.

Dado este continuo análisis y la incertidumbre actual sobre los ciberriesgos, es muy importante ser conscientes de los potenciales peligros nuevos que van apareciendo y tener, en todo momento, controlada la “transferencia y retención” (que más adelante se verá), para no sufrir unos daños no previstos y que supongan un duro revés para la salud de la empresa.

Todo este proceso continuo de gestión de riesgos comprende las fases de cuantificación y evaluación de los impactos que pueden tener los riesgos, poniendo en marcha estrategias integradas de mitigación, recuperación y restauración que permitan a la empresa gestionar sus riesgos con el fin último de proteger sus activos y, por extensión, el valor de la compañía y de sus marcas.

Se puede entender, pues, que lo importante no es buscar quién paga (normalmente una compañía de seguros), sino que el negocio no se pare, que no se pierda a los clientes ni a los proveedores e, incluso, que los competidores no aprovechen la circunstancia para acabar con el negocio.

## **2.2. Proceso continuo – importancia del plan estratégico**

El proceso de gerencia de riesgos es un proceso que requiere una implicación continua desde todas las áreas y niveles jerárquicos de una organización.

La ISO 31000 (ya comentada anteriormente), hace hincapié en estos dos conceptos de continuidad y aplicación en 360° de la organización. Además, determina tres elementos clave para una gestión de riesgos efectiva, transparente, sistemática y creíble. Dichos elementos son:

- Principios de la gestión de riesgos
- Marco de trabajo para la gestión de riesgos
- Proceso de gestión de riesgos

### **2.2.1 Principios de la Gerencia de Riesgos**

Según esta ISO, una efectiva gestión de riesgos debería cumplir una serie de principios, que se definen como:

- 1) Crear y proteger el valor
- 2) Estar integrada en todos los procesos de la organización
- 3) Ser parte de la toma de decisiones
- 4) Tratar explícitamente la incertidumbre
- 5) Ser sistemática, estructurada y oportuna
- 6) Basarse en la mejor información disponible
- 7) Alinearse al contexto y al perfil de riesgos de la organización
- 8) Tener en cuenta los factores humanos y culturales
- 9) Ser transparente e inclusiva
- 10) Ser dinámica, iterativa y sensible al cambio
- 11) Facilitar la mejora continua

Muchos de estos principios son básicos y lógicos pero que se hayan decidido remarcar dentro de una norma ISO indica de su importancia y de que es necesario tenerlos en cuenta en todo momento.

### **2.2.2 Marco de trabajo**

En cuanto al marco de trabajo se intenta establecer cómo debe ser la estructura de soporte, con el objetivo principal de integrar el proceso de gestión de riesgos al gobierno corporativo.

Se recomienda establecer un marco de trabajo utilizando como base el círculo de Deming o también conocido con el nombre de diagrama PDCA (*Plan-Do-Check-Act*), que básicamente consiste en:



- Planificar: fase en la que se debe diseñar todo el proceso necesario para la gerencia de riesgos. Incluye la comprensión por parte de toda la organización, el definir la política de gestión de riesgos que se llevará a cabo, la integración en los procesos, etc.
- Hacer: fase en la que se ha de implementar el proceso de gestión de riesgos, así como todo el marco necesario de trabajo.
- Controlar o verificar: la efectividad del marco de trabajo, revisión del avance, monitoreo de desviaciones; en resumen, revisar la efectividad del proceso.
- Actuar: corresponde a la mejora continua del marco de trabajo y del proceso, tomando las decisiones correspondientes.

Todo ello es de vital importancia que vaya acompañado de un compromiso total por parte de la dirección de la organización.

### **2.2.3 Proceso**

Hasta ahora se han analizado los principios que debe cumplir la gestión de riesgos y el marco de trabajo sobre el que se ha de realizar. A continuación se explicará cómo se ha de desarrollar este proceso de *ERM*, siempre dentro del contexto de los dos puntos anteriormente comentados.

Todo empieza teniendo bien definidos los objetivos estratégicos de la organización, conociendo el apetito al riesgo que se puede llegar a tener. A partir de ahí, empieza todo un proceso de valoración y tratamiento de los riesgos. Este proceso deberá ser un proceso iterativo y estar en constante funcionamiento y actualización para así cumplir los principios marcados por la ISO 31000 para el proceso de gerencia de riesgos.

Este proceso del *ERM* ha de ser un proceso continuo y orientado siempre al plan estratégico de la organización. Por lo tanto, acudiendo al diagrama elaborado por FERMA basándose en la información facilitada en la ya comentada ISO 31000, se debería actuar de la siguiente manera:

Gráfico 1. Proceso ERM completo



Fuente: FERMA

Una vez los objetivos están definidos claramente, se debe proceder a la valoración de los riesgos (etapa que incluye tanto el análisis como la evaluación de dichos riesgos). Una vez valorados, se debe realizar el informe de riesgos para así poder tomar la decisión de cómo tratar el riesgo y ver si residualmente queda algún aspecto.

Por último, siempre se ha de tener una supervisión de todo el proceso que puede hacer modificar cualquiera de los puntos anteriores del diagrama, incluso los objetivos estratégicos de la organización.

Paralelamente, también se ha de ir haciendo una auditoría para comprobar que todos los pasos del proceso se han realizado de forma correcta y que la empresa no esté asumiendo riesgos para los cuales no esté preparado. Esta auditoría también puede ser de gran utilidad para obtener información de modificaciones que se han de realizar en alguno de los apartados del diagrama.

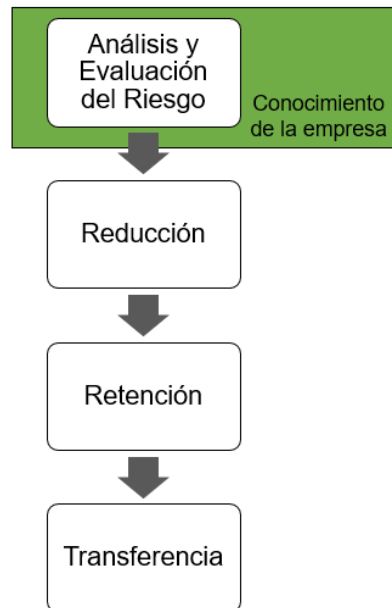
En el siguiente punto se desarrollará más en profundidad las fases principales de todo este proceso, tanto a nivel teórico-académico como a nivel práctico-real.

### 2.3. Fases principales de la Gestión de Riesgos

Con todo lo que se está comentando queda claro que es básico conocer todos los riesgos que pueden afectar a una empresa y, posteriormente, tomar las decisiones adecuadas para proteger el valor de la compañía.

El procedimiento teórico y simplificado del *ERM* se podría esquematizar de la siguiente manera:

**Gráfico 2. Procedimiento teórico ERM**



Fuente: elaboración propia

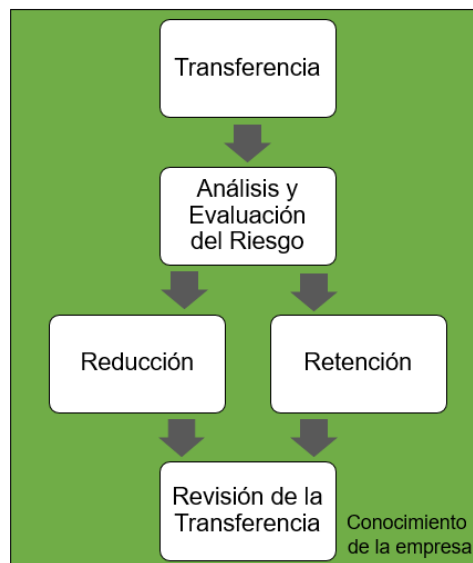
De forma ideal se debería analizar y evaluar el riesgo al que se está sometido o se podría estar sometido, que formaría parte del conocimiento de la empresa para así, posteriormente, reducir aquel riesgo que se pudiera, retener el que se considerara según la política de la empresa u otros intereses (económicos sobretodo) y transferir el resto de riesgos.

Las fases de retención y transferencia son dos puntos que forman parte directa de la estrategia que quiera seguir la empresa. Aumentar la retención y disminuir la transferencia puede suponer un ahorro en costes pero hace aumentar la incertidumbre sobre el impacto de un posible riesgo. Sin embargo, reducir la retención y aumentar la transferencia puede ser más costoso pero aporta a la empresa la tranquilidad de que es un riesgo que tiene derivado a un tercero (generalmente compañía de seguros).

El proceso que se acaba de comentar es un proceso académico-teórico que abarca lo que sería ideal dentro de un contexto de conocimiento de la empresa previo a la toma de decisiones. El problema es que la fase de conocimiento de la empresa no es algo que se pueda hacer -bien- de forma rápida y directa, sino que es un proceso que requiere de un largo periodo de tiempo y por lo tanto retrasaría la aplicación del ERM y aumentaría el tiempo de exposición de la compañía a los riesgos que la afecten.

Por tanto, pasando de la parte académica a la práctica y que realmente se aplica en las organizaciones, debería ser algo como:

**Gráfico 3. Procedimiento práctico ERM**



Fuente: elaboración propia

Lo primero de todo debería ser la transferencia de los riesgos (o por lo menos de los riesgos que inicialmente se tienen identificados que pueden no ser todos y que no se quieren retener de ninguna de las maneras) para así reducir la exposición. Generalmente, cuando se inicia la gerencia de una empresa que ya está en funcionamiento, ya tiene la tradición aseguradora ya que, probablemente, cuente con un seguro que cubre los principales daños materiales que puede sufrir (incendio, robo, etc.).

En este primer punto las decisiones a tomar son generalmente muy obvias y por lo tanto se pueden resolver de una forma inmediata pero, paralelamente, es necesario realizar la fase de análisis y evaluación del riesgo, que sería la misma fase que, académicamente, se debía hacer al inicio. En esta fase se debería analizar y evaluar el riesgo y observar cuáles se podrían reducir y cuáles retener según la estrategia que decida seguir la empresa.

Una vez se han identificado todos los riesgos y se han reducido y retenido, así como se ha ido incrementando el conocimiento de la empresa, se debe revisar la transferencia inicial que se hizo para iterar todo el proceso de nuevo, modificando dicha transferencia según los cambios que ha habido y según la retención que se haya decidido asumir dentro de los objetivos estratégicos de la organización.

Todo ello se debe realizar mientras se está en el proceso de conocimiento de la empresa.

Además, indicar que dentro del punto “análisis y evaluación del riesgo”, la parte de “análisis” está dividida en tres partes que consistirían en la “identificación, descripción y estimación de riesgos” para así posteriormente poder evaluarlos.

Estos tres últimos pasos son esenciales en la gerencia de riesgos y requieren de un gran conocimiento tanto interno de la empresa como externo, del mercado en el que opera así como del entorno político, social, cultural y legal que rodea.

Por tanto, a continuación se procederá a hacer una explicación de en qué consisten estas tres fases que componen el “análisis y evaluación del riesgo”, así como en qué consiste la fase de “reducción” del riesgo, que viene definido según la norma ISO 51 ya comentada anteriormente.

### **2.3.1 Identificación**

El apartado de identificación debe realizarse de forma metódica para asegurarse de que se han tenido en cuenta todas las actividades de la empresa así como que se han definido todos los riesgos de dichas actividades. Los cuatro grandes bloques en los que se podrían dividir estos riesgos son los ya comentados con anterioridad (Estratégicos, Financieros, Operacionales y Del Azar).

Tener en cuenta todas las actividades que realiza la empresa incluye el tener en cuenta aspectos como los riesgos de crédito, que generalmente no son concebidos por las organizaciones como un peligro real para la cuenta de resultados pero que pueden tener un gran impacto. Por lo tanto, se deberá prestar especial atención a aquellos riesgos que pueden estar presentes y que no se conocen o que pueden estar presentes y no se consideran.

### **2.3.2 Descripción**

Una vez identificados todos los riesgos hay que describirlos de forma estructurada y bajo un mismo patrón. FERMA propone una tabla de descripción de riesgos en la cual, para cada riesgo, se deberían describir nueve parámetros:

1. Nombre del riesgo
2. Alcance del riesgo (descripción cualitativa de tamaño, tipo, etc.)
3. Naturaleza del riesgo (Estratégico, Operacional, Financiero o Del Azar)
4. Interesados (personas afectadas y sus expectativas)
5. Cuantificación del riesgo (importancia y probabilidad)
6. Tolerancia/apetito del riesgo (impacto financiero del riesgo)
7. Tratamiento del riesgo y mecanismos de control (medios por los que se gestiona el riesgo actualmente)
8. Acción potencial de mejora (recomendaciones para su reducción)

## 9. Política y estrategia a desarrollar (identificación del responsable de la función)

De esta forma, cumplimentando esta tabla para cada uno de los riesgos se pueden tener mucho más controlados y accesibles para las personas a las que deban hacerse partícipes.

### 2.3.3 Estimación / Evaluación

El último punto del análisis de los riesgos se trata de la estimación. Esta estimación puede ser, en cuanto a su probabilidad de ocurrencia y posibles consecuencias, cuantitativa (o semi-cuantitativa) o cualitativa, en función de la posibilidad de representar de forma numérica la probabilidad y costes de ocurrencia.

Se ha comentado en puntos anteriores que el riesgo puede ser visto tanto como una amenaza como una oportunidad. Es por ello que, a la hora de analizar la estimación de los riesgos, se deben analizar tanto desde el punto positivo como desde el punto negativo.

Para estimar un riesgo se debe considerar el impacto que puede tener dentro de la cuenta de resultados y los aspectos a controlar son tanto sus consecuencias (impacto económico que supondría la ocurrencia) como su probabilidad (frecuencia con la que se puede dar el riesgo).

En función del tamaño de la empresa y de su apetito al riesgo, las estimaciones tanto de consecuencias como de probabilidad pueden ser más o menos detalladas. De tal forma, en algunas empresas se puede/interesa hacer una medición de los dos parámetros con tres términos en cada uno de ellos y en otras empresas puede ser necesario un mayor detalle y se debe hacer con más términos.

Poniendo un ejemplo de una empresa que considera que con cuatro términos<sup>5</sup> por cada uno de los parámetros, se procede a describir los que corresponden a las "Consecuencias":

---

<sup>5</sup> Cabe destacar que la selección de términos depende de muchos factores, como tamaño de la empresa, aversión al riesgo, etc. pero que cuatro términos suele ser insuficiente, pero se ha elegido este número a nivel académico y para tratarlo como un ejemplo que no sea demasiado extenso.

**Tabla 1. Descripción y valoración de consecuencias de un riesgo**

Consecuencias	Valores	Descripción
Altas / Catastróficas	4	Fuerte impacto en la operatividad de la empresa, hasta el punto de dejarla sin funcionamiento. El impacto es susceptible de superar x€ (determinados por la empresa).
Moderadas	3	Impacto moderado en la operatividad de la empresa y se requiere un tiempo para volver a poder operar. Impacto financiero susceptible de situarse entre y€ y x€.
Bajas	2	Bajo impacto en la estrategia u operatividad de la empresa, con un impacto financiero bajo.
Insignificantes	1	Su eventual ocurrencia no supondría prácticamente pérdida operativa ni financiera, así como tampoco afectaría a la consecución de los objetivos de la empresa.

Fuente: elaboración propia

Una vez se han evaluado las consecuencias de los posibles riesgos, se debe analizar la probabilidad de ocurrencia que tienen. Para ello, se determinan igualmente cuatro términos:

**Tabla 2. Descripción y valoración de probabilidad de ocurrencia**

Ocurrencia	Valores	Descripción
Muy probable / Casi certeza	4	Riesgo con probabilidad muy alta, que se podría definir con un porcentaje entre el 75% y el 100% de seguridad de ocurrencia.
Probable	3	Siguen siendo riesgos con probabilidad alta de ocurrencia, que se pueden definir entre el 51% y el 74% de seguridad de que se presente.
Posible	2	Riesgos con una seguridad de ocurrencia de entre el 26% y el 50%, empiezan a perder frecuencia.
Improbable	1	Riesgo con una posibilidad de ocurrencia baja, que se sitúa entre el 1% y el 25% de seguridad de ocurrencia.

Fuente: elaboración propia

El cálculo del valor que se asigna tanto de las consecuencias como de la probabilidad de ocurrencia es un valor subjetivo que se debe basar en la experiencia tanto del Gerente de Riesgos como en las experiencias vividas en la propia empresa, utilizando registros y datos del pasado. Hay que recordar que resultados pasados no garantizan ocurrencias futuras pero pueden servir a modo orientativo. Por tanto, se vuelve a poner de manifiesto la necesidad de que todo este ciclo del *ERM* sea continuo y que no se realice una única vez.

Una vez realizada la estimación de los riesgos se puede calcular lo que recibe el nombre de "Índice de riesgo" que es simplemente el producto de la probabilidad de ocurrencia con las consecuencias del riesgo. A mayor índice, más aten-

ción se deberá prestar al riesgo dado que es más probable que ocurra y con mayores consecuencias.

A estas alturas ya se es capaz de cumplimentar una tabla como la que se muestra a continuación como idea para tener los riesgos completamente identificados, descritos y estimados:

**Tabla 3. Análisis y evaluación de los riesgos**

<b>Análisis y evaluación del riesgo</b>						
<b>Identificación y descripción</b>				<b>Estimación</b>		
Número/ Código	Nombre	Alcance	Naturaleza	Consecuencia	Ocurrencia	Índice riesgo

Fuente: elaboración propia

Esta tabla es de vital importancia para tener todos los riesgos detectados adecuadamente relacionados y así poder ver, de forma rápida y sencilla el “índice de riesgo” que tienen dentro de la empresa.

El siguiente paso consistirá en representar la matriz de riesgos y el mapa de riesgos, dos conceptos que se comentarán a continuación pero que se nutrirán de toda la información desarrollada en la tabla anterior.

### 2.3.4 Reducción del riesgo - Matriz y mapa de riesgos

Una vez se dispone de todos los riesgos adecuadamente identificados, descritos y estimados, junto con su “índice de riesgo”, se puede hacer una tabla de tolerancias a este índice. Siguiendo el ejemplo de las tablas anteriores, la tolerancia podría ser la siguiente:

**Tabla 4. Tolerancias a los riesgos**

Índice de riesgo		Índice de riesgo
16	<b>Intolerable</b>	16
15		15
14		14
13		13
12		12
11		11
10		10
9		9
8	<b>Significativo</b>	8
7		7
6		6
5		5
4		4
3	<b>Tolerable</b>	3
2		2
1		1

Fuente: elaboración propia



Dicha matriz divide los riesgos según su probabilidad de ocurrencia y su consecuencia y por lo tanto muestra, de manera muy visual e intuitiva, los riesgos separados en función de la repercusión que pueden tener en el negocio.

**Tabla 5. Matriz de riesgos**

		Ocurrencia			
		Improbable	Posible	Probable	Muy probable
Consecuencias	Altas	4	8	12	16
	Moderadas	3	6	9	12
	Bajas	2	4	6	8
	Insignificantes	1	2	3	4

Fuente: elaboración propia

Una vez se dispone de la matriz de riesgos, se puede confeccionar el mapa de riesgos que, de manera rápida, indica el trato que se debe dar a cada uno de los riesgos. Para poner un tipo de ejemplo sencillo, se muestra el mapa de riesgos por grupo de riesgos:

**Tabla 6. Mapa de riesgos**

		Ocurrencia			
		Improbable	Posible	Probable	Muy probable
Consecuencias	Altas	Grupo III. Riesgos de atención periódica		Grupo I. Riesgos de atención inmediata	
	Moderadas				
	Bajas	Grupo IV. Riesgos controlados		Grupo II. Riesgos de segui- miento	
	Insignificantes				

Fuente: elaboración propia

Llegado a este punto, nuevamente se debe tener en cuenta la estrategia de la empresa del estudio. Como se ha comentado anteriormente, los riesgos pueden ser considerados como amenazas o como oportunidades y, como es lógico, el trato que se les debe dar así como la manera de afrontarlos, ha de ser diferente en función de la consideración que reciban dentro de la organización.

**Riesgo = amenaza:**

Aquellas estrategias que consideren que el riesgo es una amenaza, deberán intentar reducir al máximo todos aquellos riesgos con un índice de riesgo alto y llevarlos a zonas más de “confort”, es decir, se deberá tratar de reducir los riesgos intolerables a significativos y los significativos a tolerables.

Por lo tanto, la idea tanto de la matriz de riesgos como del mapa de riesgos sería la siguiente:

**Tabla 7. Matriz de riesgos (riesgo = amenaza)**

		Ocurrencia			
		Improbable	Posible	Probable	Muy probable
Consecuencias	Altas				
	Moderadas				
	Bajas				
	Insignificantes				

Fuente: elaboración propia

**Tabla 8. Matriz de riesgos (riesgo = amenaza)**

		Ocurrencia			
		Improbable	Posible	Probable	Muy probable
Consecuencias	Altas	Grupo III.		Grupo I.	
	Moderadas				
	Bajas				
	Insignificantes	Grupo IV.		Grupo II.	

Fuente: elaboración propia

Como se puede observar en las tablas anteriores, si el riesgo es considerado como amenaza, siempre se debe intentar reducir en la medida de lo posible. Y reducir significa intentar disminuir sus probabilidades de ocurrencia y/o (siempre que sea posible y dependiendo del riesgo) reducir las magnitud de las consecuencias que pueden acarrear.

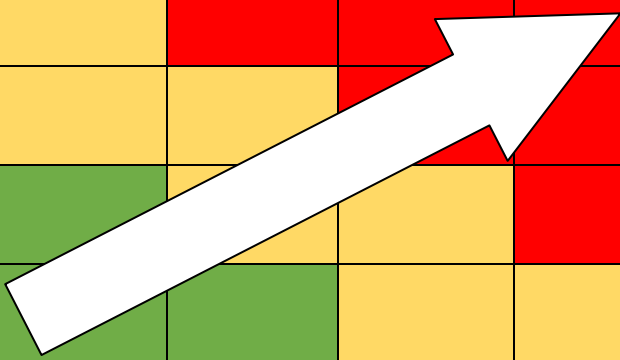
Alguna de las posibilidades que se tienen para conseguir este cometido es la instalación de algunos controles o procedimientos orientados a mitigar el impacto que un riesgo puede tener en la cuenta de resultados. Estas medidas dependerán, casi siempre, de la naturaleza del riesgo y por lo tanto es difícil encontrar soluciones “estándar” para todas las organizaciones.

**Riesgo = oportunidad:**

Por el contrario, aquellas empresas cuyo apetito al riesgo es mayor y pueden considerar el riesgo como una oportunidad, los intereses serán que los riesgos tengan mayor probabilidad de ocurrencia y mayor impacto de sus consecuencias en la cuenta de resultados. Por ello, la matriz y mapa de riesgos en estos casos serán de la siguiente manera:

**Tabla 9. Mapa de riesgos (riesgo = oportunidad)**

		Ocurrencia			
		Improbable	Posible	Probable	Muy probable
Consecuencias	Altas				
	Moderadas				
	Bajas				
	Insignificantes				



Fuente: elaboración propia

Tabla 10. Matriz de riesgos (riesgo = oportunidad)

		Ocurrencia			
		Improbable	Posible	Probable	Muy probable
Consecuencias	Altas	Grupo III.		Grupo I.	
	Moderadas	↑		→	↑
	Bajas	↓		→	↓
	Insignificantes	Grupo IV.		Grupo II.	

Fuente: elaboración propia

En estos casos cuyo apetito de riesgo de la empresa es mayor y, por lo tanto, es más tolerable al riesgo, lo que se busca es que, de un riesgo con índice de riesgo elevado, intentar sacar un beneficio.

Un claro ejemplo de estos casos son los riesgos financieros. Es posible aumentar el índice de riesgo (es decir, aumentar las probabilidades de ocurrencia y/o el impacto en la cuenta de resultados) invirtiendo en carteras consideradas más “peligrosas”. Por ejemplo, no es lo mismo invertir en renta fija que renta variable enfocada a países emergentes o *startups*<sup>6</sup>. Si se invierte todo el capital financiero en renta variable, se está aumentando mucho el índice de riesgo ya que las probabilidades de pérdida están aumentando. Sin embargo, si al cabo de unos meses dichas acciones han tenido un aumento importante de valor, el beneficio que obtiene la empresa es muy importante.

Con este claro ejemplo, se puede entender que haya empresas cuya tolerancia al riesgo sea mayor para, posteriormente, intentar sacar más beneficio. Eso sí, no cabe decir que al estar más expuesto al riesgo, las opciones de pérdida también son mayores.

## 2.4. Retención y transferencia

Llegados a este punto en el cual la empresa ya conoce y tiene bien descritos todos los riesgos, así como su probabilidad de ocurrencia y su impacto directo en la organización, se debe analizar la conveniencia de la retención y la transferencia.

<sup>6</sup> *Startups*: Sociedades de nueva creación, que buscan sacar ventajas competitivas mediante las nuevas tecnologías y que están enfocadas a los clientes.

La retención (que puede ser voluntaria o involuntaria) es cuando la propia organización asume las pérdidas que supondría la aparición del riesgo.

La transferencia consiste en derivar la eventual ocurrencia del riesgo a un tercero, como puede ser una compañía aseguradora, una cautiva, etc.

Volviendo a la estrategia de la empresa, se debe valorar qué se desea retener y qué se desea transferir. Algunas organizaciones de pequeño tamaño prefieren transferir prácticamente la totalidad del riesgo ya que el ratio coste/tranquilidad les es beneficioso.

Sin embargo, otras organizaciones de mayor tamaño no pueden transferir todo el riesgo por el coste que supondría o, simplemente, porque no encuentran a quién transferírselo.

Por lo tanto, a la hora de decidir qué riesgos se retienen y qué riesgos se transfieren hay que tener en cuenta el índice de riesgo (probabilidad ocurrencia e impacto) y el coste que tendría una eventual transferencia o un eventual acontecimiento negativo para la empresa y que no se ha transferido.

Utilizando de nuevo el mapa de riesgos explicado anteriormente, hay que distinguir entre cuatro grandes grupos de riesgos para valorar la conveniencia sobre la retención o la transferencia.

#### **2.4.1 Grupo I. Riesgos de atención inmediata**

Se trata de riesgos con una alta probabilidad de ocurrencia y un con unas consecuencias muy negativas. Por lo tanto, aquellos riesgos que no se hayan podido reducir y que aún se encuentren en este grupo, habrá que prestarles gran atención y transferirlos directamente ya que si ocurriesen (alta probabilidad), las consecuencias para la cuenta de resultados serían importantes.

#### **2.4.2 Grupo II. Riesgos de seguimiento**

Se tratan de aquellos riesgos con una probabilidad de ocurrencia elevada pero con unas consecuencias prácticamente insignificantes.

En este caso, la decisión dependerá del tamaño y de la estrategia de cada organización. Para algunas organizaciones grandes, que pueden crear un fondo propio para tener liquidez, es mejor asumir las pocas consecuencias que ocasionan estos riesgos y así no tener el coste de un seguro. Para organizaciones más pequeñas y que pueden no tener tanta liquidez, asumir estos siniestros frecuentemente puede suponer un problema así que pueden transferir el riesgo a una aseguradora, por ejemplo, para así no tener que estar constantemente preocupados.

### 2.4.3 Grupo III. Riesgos de atención periódica

Como se ha especificado en el mapa de riesgos, estos son aquellos con una baja probabilidad de ocurrencia pero que pueden tener unas consecuencias más o menos importantes, es decir, pueden llegar a tener repercusión en la cuenta de resultados.

Generalmente, en este grupo también es muy conveniente transferir el riesgo atendiendo a las consecuencias que podría tener el retener el riesgo.

### 2.4.4 Grupo IV. Riesgos controlados

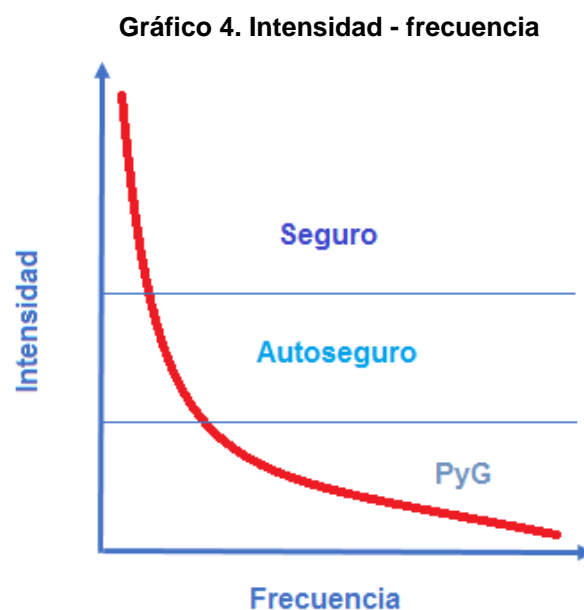
Riesgos cuya probabilidad de ocurrencia es baja o nula, al igual que sus consecuencias, que son bajas o insignificantes.

Igual que en los riesgos del grupo II, en estos casos se debería valorar la opción de retenerlos o transferirlos, en función de la estrategia de la organización.

Una organización grande puede retener estos riesgos sin ningún tipo de problema y sin necesidad de crear ningún fondo propio (este método se conoce como "Autoseguro"). Sin embargo, una pequeña empresa puede no sentirse cómoda con esta situación y preferir transferirlo todo mediante, por ejemplo, una póliza de Comercios o Pyme.

Como se comentaba anteriormente, cabe la posibilidad de que haya una parte de retención desconocida, de forma involuntaria. Por lo tanto, es muy importante intentar minimizar el desconocimiento de los riesgos y evitar una incorrecta evaluación de los mismos, para así no tener una exposición mayor a la deseada.

Gráficamente, se podría representar las diferentes decisiones de la siguiente manera:



Fuente: elaboración propia

El gráfico intensidad-frecuencia indica que los siniestros de alta intensidad tienen una frecuencia muy baja y que los de baja intensidad suelen tener una frecuencia más alta. Por lo tanto, se pueden definir diferentes tramos de intensidad para decidir si se debe transferir el riesgo o si se debe asumir.

Para los siniestros de alta intensidad, se deben transferir mediante un seguro. Las intensidades intermedias se podrían retener a través de un autoseguro o a través de empresas cautivas<sup>7</sup>. Para las bajas intensidades se deberían asumir directamente en la cuenta de Pérdidas y Ganancias a través de franquicias o exclusiones de los seguros contratados para la transferencia.

Todos estos niveles dependen de los tamaños de las empresas e incluso alguna de las etapas puede no existir. Puede ser que empresas pequeñas no puedan optar a un autoseguro mediante cautiva y por lo tanto únicamente disponer de las fases de transferencia a través de seguro y de retención mediante franquicias.

Además, los niveles de intensidad dependen de diferentes variables como pueden ser la capacidad financiera de la organización, la aversión (o apetito) al riesgo que se haya definido y la situación del mercado, que le indicarán a la empresa qué capacidades deberá asumir y cuáles transferir.

#### **2.4.5 Nuevos riesgos y riesgos en evolución**

Además de los grupos que, gráficamente, se han mostrado dentro de la matriz de riesgos, hay un grupo que es sobre el cual hay que poner un especial foco y tener constantemente monitorizados y controlados ya que pueden suponer la aparición de un nuevo riesgo en uno de los grupos de peligro (como el grupo I, de atención inmediata) o evolucionar y hacer pasar un riesgo del grupo IV (riesgos controlados) al grupo I (en el peor de los casos).

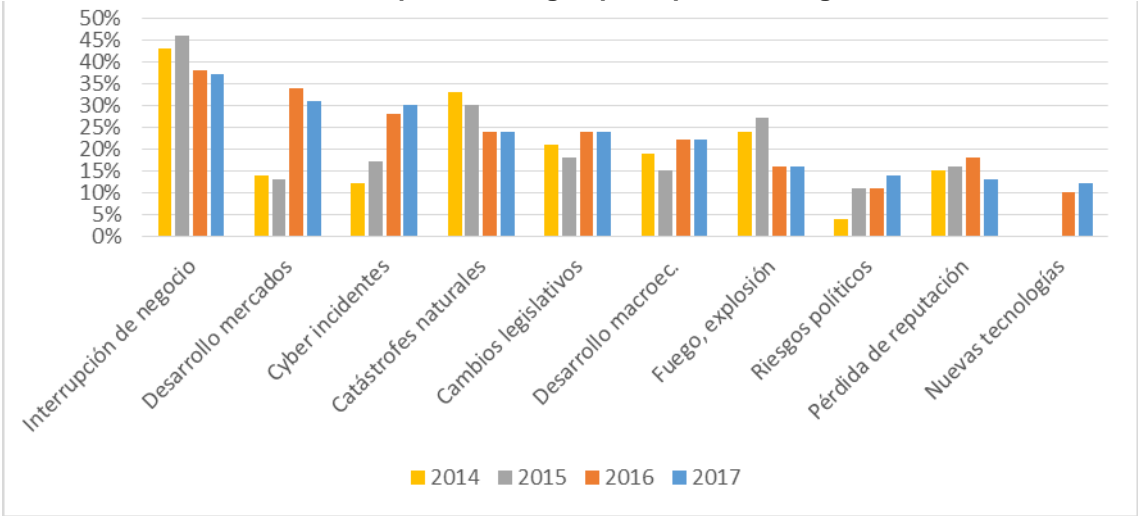
Estos riesgos pueden ser de cualquiera de los tipos anteriormente comentados (financieros, estratégicos, operacionales o fortuitos/azar) y se caracterizan por ser riesgos que o no existían o se transforman de manera muy rápida, pasando a ser una amenaza muy importante para la organización.

---

<sup>7</sup> Empresas cautivas: se trata de empresas filiales que aseguran (o reaseguran) parte o todos los riesgos de una empresa o grupo matriz. Es una modalidad mediante la que grandes empresas reducen primas de seguro asumiendo ellas mismas parte del riesgo.

Según un estudio que realiza Allianz<sup>8</sup>, estos son los diez riesgos que más han preocupado a las organizaciones en los últimos años:

**Gráfico 5. Top 10 de riesgos principales de negocios**



Fuente: elaboración propia con datos de Allianz

Se puede observar como las nuevas tecnologías son consideradas un nuevo riesgo desde hace pocos años y, ver la evolución que tendrán dentro de los modelos de negocio y los procesos productivos, es una de las preocupaciones principales de los directivos de las empresas.

Los ciberincidentes llevan más años dentro de los riesgos principales y se puede ver cómo, año tras año, incrementa su preocupación. Por lo tanto, podríamos considerar que se trata de un riesgo en constante evolución y que por ello siempre ha de estar correspondientemente monitorizado y actualizado.

Otros riesgos que preocupan a los directivos por la evolución que pueden tener con los desarrollos de los mercados, los cambios legislativos y el desarrollo macroeconómico; riesgos que crean una incerteza tanto a corto como a medio y largo plazo, lo cual hace necesario tenerlos también constantemente analizados dentro de la gestión del *ERM*.

Por lo tanto, una vez se ha llegado a este punto en el proceso del *ERM*, se deben valorar todas las opciones de retención y transferencia y tomar decisiones en función del tipo de riesgo y del coste que se está dispuesto a asumir (y cuando se habla de costes no significa únicamente monetarios sino también de exposición a dicho riesgo).

<sup>8</sup> Allianz - Allianz Risk Barometer (2017)



## 2.5. Costes de la reducción, retención y transferencia

Una vez comentados cada uno de los apartados, hay que tener en cuenta diferentes consideraciones para poder hacer una correcta reducción de los riesgos y para que se retenga y transfiera el riesgo de forma adecuada y siempre dentro de los márgenes presupuestarios de los que disponga la compañía.

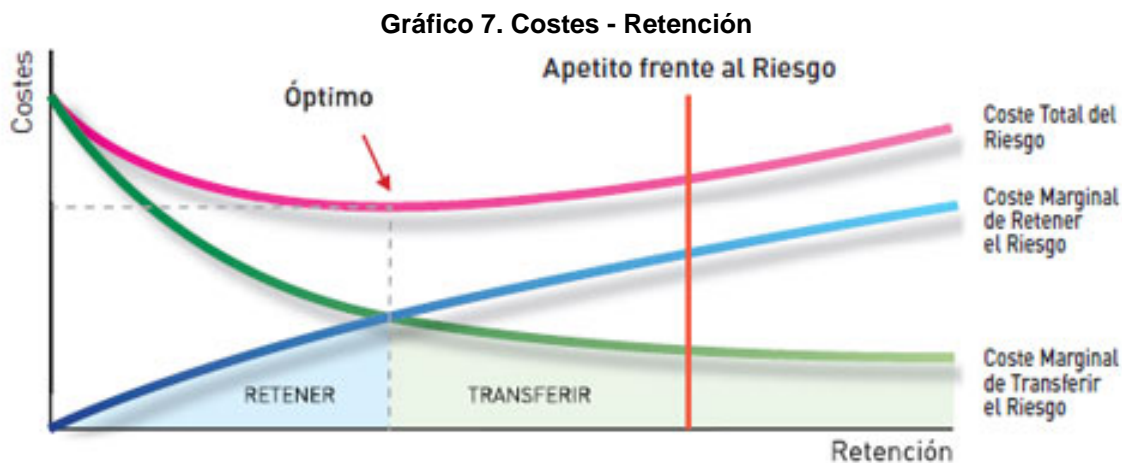
A la hora de la reducción del riesgo, siempre se ha de ser conscientes de que el riesgo 0 no existe por mucha inversión que se haga. Esto se puede apreciar en el siguiente gráfico:



Como se observa en el gráfico, al principio, con una “pequeña” inversión, se puede reducir de forma importante el riesgo pero llega un punto en el que se requieren grandes inversiones para reducir ligeramente el riesgo.

Para ello, a la hora de hacer la reducción de los riesgos, siempre hay que tener en mente el coste que puede suponer y establecer el punto hasta el que se esté dispuesto a llegar.

De igual manera, en la transferencia y reducción del riesgo también se debe trazar la estrategia que se debe seguir teniendo en cuenta el coste que supone cada una de las etapas y según el apetito al riesgo de la organización. Todo ello, se puede observar en el siguiente gráfico:



Tal y como se observa en dicho gráfico, y la lógica así lo indica, el coste marginal de retener el riesgo aumenta a mayor retención se practica. Esto es lógico dado que, a más riesgo se decide retener, más posibilidad de impacto en la cuenta de resultados hay y por lo tanto aumenta el coste.

De igual manera, la curva de coste marginal de la transferencia de riesgos disminuye a más retención se tiene. También es lógico ya que si hay mucha retención, hay menos transferencia y por lo tanto se reduce el coste. Por el contrario, si la retención es mínima, el coste de transferir el riesgo aumenta de forma exponencial.

Con lo cual, el punto óptimo entre la retención y la transferencia sería el punto donde se cruzan estas dos gráficas. De manera teórica es muy sencillo pero a la hora de llevarlo a la práctica, es mucho más complejo ya que encontrar este equilibrio no es tan trivial.

Además de todo ello, el punto de equilibrio óptimo es el cruce de las gráficas pero, como se ha comentado anteriormente, también depende del apetito al riesgo que se tenga. Si dicho apetito al riesgo es inferior al punto óptimo, se deberá asumir más coste del necesario pero en consecuencia, la exposición al riesgo será menor ya que se transfiere más riesgo.

Si el apetito al riesgo es mayor, habrá una menor transferencia y una mayor retención, lo que hará incrementar el coste total del riesgo pero, tal y como se ha expuesto en puntos anteriores, también hay más posibilidades de convertir dicho riesgo en una oportunidad e incrementar así los beneficios que obtiene la organización.

## 2.6. Plan de continuidad del negocio

Acompañando a todo el proceso de conocimiento y actuación ante los riesgos que pueden afectar a un negocio, es muy importante establecer un plan de continuidad del negocio para que, el día de la eventualidad, se pueda reestablecer el negocio cuanto antes y minimizar de esta manera las pérdidas que se puedan sufrir. Además, estas pérdidas pueden no ser únicamente monetarias

sino que también pueden haber pérdidas del nombre de marca, etc. que, con una buena y rápida actuación, puede acabar siendo una oportunidad para ganar reputación.

Dentro del proceso del ERM se ha de hacer la identificación del peor escenario posible ante una eventualidad negativa que pueda afectar al negocio. Una vez identificado, se ha de tener en cuenta las consecuencias e impacto que puede tener. Como consecuencias, se han de valorar tanto consecuencias estratégicas, el impacto financiero que puede ocasionar, la afectación a la producción y el impacto en los procesos operativos.

Una vez se ha realizado este estudio, se debe desarrollar e implantar la solución, integrándola en toda la organización. Este desarrollo debe dar respuesta a la emergencia, dar las pautas para gestionar la crisis e indicar cómo se debe recuperar la actividad.

Todos estos pasos es muy importante que se entrenen ya que si únicamente se aplican el día de la crisis, en un momento de tensión y pánico, las cosas tienden a no salir como deberían y, por lo tanto, no sería de la utilidad buscada. Siempre es importante tener el plan de continuidad bien entrenado para que, el día que sea realmente necesario, gente tenga automatizadas sus responsabilidades.

El diagrama, gráficamente, se podría representar de la siguiente manera:



Fuente: Munich RE

Una vez sucede el “estallido” de la crisis, debe entrar la respuesta a la emergencia a través del manual de autoprotección. Este manual contiene:

- Las evaluaciones de los riesgos operativos
- Medios de combate en cada instalación
- Modo de respuesta ante cada emergencia
- Implantación del Plan

Por lo tanto, en dicho manual se encontrará la respuesta que se debe dar ante cada una de las emergencias (si se ha realizado de forma correcta).

Posteriormente, se debe hacer la gestión de la crisis. En dicha gestión de la crisis se ha de crear el comité de crisis y definir las funciones y responsabilidades de todos los actores. Además se ha de establecer un plan de comunicación a clientes, proveedores, empleados, seguros, etc. así como los procedimientos de actuación (retirada de producto, etc.).

Una vez gestionada la crisis, se debe proceder a la recuperación del negocio. Para ello, se deben activar los planes específicos y recuperar la información vital de la empresa. También es importante diseñar los programas de financiación interna y externa para la recuperación total.

Igual que todo el proceso de ERM, el plan de continuidad del negocio es un plan en constante actualización y evolución para garantizar su operatividad en cada momento. Para ello, es muy importante disponer de información veraz y actualizada, de todo el personal bien formado y realizar ejercicios parciales, simulacros y revisiones periódicas.

## **2.7. ¿Por qué es importante la Gerencia de Riesgos?**

Según lo que se ha desarrollado en estos párrafos, se puede observar que tanto el punto de “conocimiento de la empresa” como el de “análisis y evaluación del riesgo” son procesos continuos y que nunca se han de dejar de hacer. Por tanto, si estos dos puntos son continuos, quiere decir que todo el proceso es dinámico y que está en constante movimiento dado que siempre irán apareciendo nuevos riesgos que se deberá decidir si transferir o retener; o irán apareciendo nuevos métodos para reducir posibles riesgos “antiguos” pero que aún amenazan a la compañía.

Por lo tanto, es muy importante tener un buen proceso de Gerencia de Riesgos para conocer la empresa. Cuando se habla de conocer no se está diciendo que se sepa qué producto fabrican, por ejemplo, o cuantos empleados tiene. Estos datos son importantes pero no es lo único. También se debe conocer a qué riesgos está expuesta la organización y, para ello, es muy importante que la estructura que se forme de Gerencia de Riesgos permita el continuo desarrollo

y que no esté focalizado a hacer un proceso puntual y que, posteriormente, no se pueda sacar provecho.

De igual forma, también es un proceso, el de Gerencia, que ayuda a tener en cada momento identificados y definidos todos los riesgos de manera que si, puntualmente se tiene conocimiento de una nueva técnica de reducción de riesgos o conocimiento de que un riesgo ha cambiado, es posible conocer de forma rápida y casi intuitiva la manera en la que afectará a toda la organización.

Todo este proceso de gerencia de riesgos lleva años establecido en las grandes organizaciones e instituciones, pero es más difícil de observar en pequeñas empresas. Sin embargo, el proceso debería estar igualmente independientemente del tamaño y tipo de organización.

Volviendo a la ISO 31000 ya comentada en los puntos previos, el primer principio de la implementación del *ERM* es el "Crear y proteger el valor" de la empresa. Este principio, además, es la principal preocupación de cualquier empresario, así como su primer objetivo, ya que el valor de la empresa es lo que hace que ésta funcione. Por lo tanto, crear valor y protegerlo es un principio básico para el mantenimiento de una organización y, a través del *ERM*, se puede conseguir.

Sin embargo, es necesario que todo el proceso de gerencia de riesgos esté completamente y adecuadamente implementado y es por ello que se debe modificar la mentalidad de muchas organizaciones y no considerar la seguridad como un gasto, sino como una inversión para proteger la empresa y asegurarse su supervivencia a lo largo del tiempo.



## 3. Qué es el ciberriesgo

### 3.1. Introducción

*Phishing, Botnet, RansomWare...* diferentes términos anglosajones con compleja o ninguna traducción a nuestro idioma en la actualidad y que cada vez más se pueden leer en la prensa, ver por la televisión o, si se es desafortunado, sufrir en las propias carnes.

De un tiempo a esta parte se ha incrementado el fenómeno conocido como *Bring Your Own Device* (BYOD). Cada vez más difícil de controlar, se trata del aumento de dispositivos (Androids, iPhones, tablets, etc.) que se pueden conectar a internet en el lugar de trabajo. Todos estos dispositivos pueden actuar como puertas de acceso, aumentando la exposición del usuario y de la organización a los *hackers* más experimentados.

Por tanto, los ciberriesgos son todos aquellos peligros que se pueden dar debido al incremento de la importancia de las tecnologías en todo el proceso de negocio de las empresas.

Este incremento en las tecnologías es un arma clara de doble filo. Por un lado son claramente necesarias para la evolución de las organizaciones ya que aportan una mejora en la mayoría de los aspectos del negocio pero a la vez incrementan la vulnerabilidad del sistema, abriendo muchas más brechas por las que pueden acceder los *hackers* y, en el peor de los casos, a los ciberatacantes (cabe recordar que la diferencia entre *hacker* y ciberatacante es que los primeros se consideran que son aquellos que tienen habilidades especiales con la programación y los segundos son aquellos que usan estas habilidades con intenciones fraudulentas o dañinas).

De hecho, el cibercrimen está moviendo grandes cantidades de dinero en los últimos años. Según un estudio de McAfee <sup>9</sup> en 2014, este tipo de delitos movieron un volumen de 400.000 millones de dólares, lo que equivale a un 0,8% del PIB mundial. Para hacer una idea, el tráfico de drogas tiene un volumen del 0,9% del PIB mundial y, por lo tanto, el volumen que se mueve en ambos negocios ya es muy similar.

Además, estos ataques son, generalmente, realizados por bandas de crimen organizado, siendo únicamente un 25% de los ataques realizados por personas que actúan de forma individual. Pero, realmente, ¿quién y qué hay detrás de cada ataque?

---

<sup>9</sup> McAfee - Net Losses: Estimating the Global Cost of Cybercrime. 2014

A continuación se muestra una tabla resumen:

**Tabla 11. Origen y motivaciones de los ciberataques**

<b>Origen</b>	<b>Motivación</b>
Estados	Mejorar su posición geopolítica o estratégica
Organizaciones criminales	Beneficio económico (directo e indirecto)
Organizaciones privadas	Ciberespionaje: obtención de información de valor
Ciberterroristas	Alterar el normal desenvolvimiento social, atemorizar a la población o incluir en las decisiones políticas
Ciberyihadistas	Propaganda, reclutamiento
Ciberactivismo	Ideología
Cibervándalos y <i>Script Kiddies</i> <sup>10</sup>	Evidenciar vulnerabilidades, piratería, diversión, retos
Actores internos	Venganza, beneficio económico, motivos ideológicos
Ciberinvestigadores	Evidenciar debilidades, autoafirmación

Fuente: CCN-CERT (Centro Criptológico Nacional)

Como se puede observar, detrás de un ciberataque hay numerosos orígenes posibles, con diferentes motivaciones, y es por ello que, a día de hoy, parece que este tipo de ataques no van a tener fin.

Uno de los grandes problemas es que, por miedo a una posible pérdida reputacional que afecte directamente a la cuenta de resultados, hay muchas compañías que tratan estos ataques como un tema tabú y no aceptan reconocer haber sufrido un ataque de este estilo. Según un estudio de Ponemon<sup>11</sup>, solo un 46% de los encuestados afirman haber sufrido un cibercrimen cuando, de otro estudio de esta misma entidad (Ponemon<sup>12</sup>) indica que es mucho más frecuente de lo que se declara ya que hay un 25% de probabilidades anuales de sufrir uno de estos ataques con pérdidas de datos.

Para poder analizar cómo puede afectar al *ERM* de una empresa, primero de todo hay que conocer cuáles son los riesgos cibernéticos más comunes a día de hoy. Para ello, se procederá a explicar los principales y que más daño causan. También es importante analizar el impacto de estos nuevos riesgos en el tejido empresarial y hacia dónde están más enfocados.

<sup>10</sup> *Script Kiddies* - Son aquellos que, con conocimientos limitados y haciendo uso de herramientas construidas por terceros, perpetran sus acciones a modo de desafío, sin ser, en muchas ocasiones, plenamente consciente de sus consecuencias.

<sup>11</sup> Ponemon Institute - Study on Mobile and Internet of Things Application Security. 2017

<sup>12</sup> Ponemon Institute - Cost of Data Breach Study: Global Analysis. 2016



## 3.2. Tipos de riesgos

En el punto anterior se han citado algunos de los ciberataques que se conocen hoy en día. A continuación se procederá a explicar los más comunes y que pueden tener más impacto tanto en una Pyme como en una gran empresa.

### 3.2.1 *Phishing* (suplantación de identidad)

El término *phising* tiene su origen en la palabra inglesa *fish* y que significa “pescar”. El motivo es porque este tipo de ciberataques se basa en el robo de información confidencial “tirando el anzuelo y esperando a que alguien pique”.

Este tipo de robo de información está considerado que puede darse de dos maneras.

La primera de ellas es una manera muy común pero que puede llegar a ser muy peligrosa y basta, únicamente, en que te revisen el móvil o el ordenador cuando se están escribiendo usuarios, contraseñas, identificaciones, etc., que se pueden estar usando para acceder al banco o al correo.

La segunda manera es la manera más común y la que sí que tiene carga cibernética y consiste en adquirir información confidencial de forma fraudulenta, suplantando la identidad de alguna persona, banco, etc.

Alguno de los ejemplos más comunes son el recibir un correo electrónico de tu supuesto banco pidiéndote el código pin; o acceder a una página web creyendo que es la de tu banco pero realmente es otra URL diferente, dando todos tus datos y pudiendo ser posteriormente robado.

### 3.2.2 *Pharming*

Ataque muy similar y relacionado con el anterior, consiste en atacar los servidores de, por ejemplo, un banco y hacer que cada vez que alguien accede a la URL de dicho banco sea redirigido a otra página, de igual aspecto que la esperada, pero donde por detrás hay unos ciberatacantes almacenando toda la información que se facilita.

El término viene de la palabra inglesa *farm* (que significa granja) ya que, cuando vas accediendo a diferentes servidores de diferentes empresas, vas teniendo una “granja” donde posteriormente puedes obtener los datos personales de forma fraudulenta.

### 3.2.3 *Botnet*

Es un término para hablar de robos informáticos (también conocidos como *bots*), que se encargan de ejecutar de manera autónoma y automática las indicaciones del artífice de la *botnet*.

Por lo tanto, este ciberatacante puede controlar todos los servidores y dispositivos infectados de forma remota, pudiéndolos ejecutar desde cualquier lugar y cualquier acción.

El ejemplo de este tipo de ataque es cuando un ordenador, de manera descontrolada, empieza a abrir páginas web sin que el usuario que está utilizando el dispositivo ejecute dicha acción. Seguramente sea el artífice de la *botnet* el que esté ejecutando estos comandos.

### **3.2.4 Ransomware**

Se trata de uno de los *malwares* que más se está extendiendo en la actualidad y es conocido como “secuestro de información”.

Este tipo de ataques es un programan informático malicioso que bloquea el acceso a los archivos del sistema infectado, pidiendo un rescate a cambio de desbloquear dichos archivos. Alguno de estos ataques bloquean directamente los archivos del sistema operativo, inutilizando así por completo el dispositivo.

Generalmente, estos archivos maliciosos van ocultos dentro de otros archivos más confiables para el usuario, para que así sea más fácil quedar infectado. Por ejemplo, pueden ir dentro de archivos adjuntos de correos electrónicos, vídeos de páginas de dudoso origen o incluso en actualizaciones de sistemas y programas que podrían parecer fiables.

El principal problema que presenta este tipo de ataques es que no tienen por qué producirse en el acto. El virus se puede quedar en el dispositivo y, hasta que el ciberatacante no decida ejecutarlo, se queda dentro del sistema como si estuviese dormido.

### **3.2.4 Robo de información**

De manera similar al apartado anterior, los atacantes también pueden, en vez de bloquear todos los documentos, acceder al lugar donde se almacenan y robarlos.

En función de los datos robados, se puede derivar en dos grandes problemas. El primero de todos, si los archivos robados son datos de los clientes de la empresa, puede suponer un grave problema a nivel legal debido a las sanciones que se imponen con la Ley Orgánica de Protección de Datos (LOPD) actual.

El segundo de los problemas es si el robo de información es de la propiedad intelectual de la compañía. Estos datos son el mayor tesoro de las compañías ya que, generalmente, es el *core* de la organización y lo que les hace diferenciarse de la competencia. Sufrir un robo de esta información puede suponer un importante impacto en la cuenta de resultados ya que puede permitir a los competidores a realizar el producto diferencial que tenía la organización que sufre el robo.

Además de todo esto, uno de los principales problemas es la dificultad en el rastreo, como se puede ver en el dibujo siguiente:

**Ilustración 3. Diagrama del robo de información**



Fuente: Munich RE

Como se puede ver en el mapa, un usuario desde Nueva York puede tener, sin él conocer, sus datos de usuario almacenados en un servidor en, por ejemplo, India. Un ciberatacante desde, por ejemplo, Brasil, puede estar accediendo a este servidor situado en la India y robando todos los datos de este usuario entre lo que se puede encontrar su nombre, dirección, tarjetas de crédito, claves de acceso, etc.

Este robo de información, se puede hacer combinando con el primer ciberriesgo que se ha comentado, el *phishing*. Además, toda esta información, posteriormente puede ser revendida en la *deepweb* de forma ágil y sin dejar apenas rastro.

Según un estudio de *TrendMicro*, los precios que se suelen pagar son los siguientes:

**Tabla 12. Coste de compra en la DeepWeb**

Cuenta de acceso a	Precio (\$)
Origin (Juegos)	<1
Spotify (Música)	2
Beats Music (Música)	2
Hulu Plus (TV online)	4
Netflix (TV online)	5
Dish Network Anywhere (TV online)	7
Lumosity (Juegos)	7
Paypal (Plataforma de pagos)	9
Sirius Radio Satélite (Radio)	15

Fuente: TrendMicro - North America Underground

Por lo tanto, dado que es un método relativamente sencillo de obtener información ilícita y de venderla, además de poco rastreable, es uno de los ciberataques más utilizados.

Además, otros datos mucho más sensibles también están muy cotizados en la *deepweb*. Hay estudios que confirman que los datos de todo el censo estadounidense se encuentra en el *darkside* de internet o que, por unos pocos de dólares, se pueden obtener los datos de la seguridad social de un habitante americano, para darle el uso que posteriormente el comprador desee.

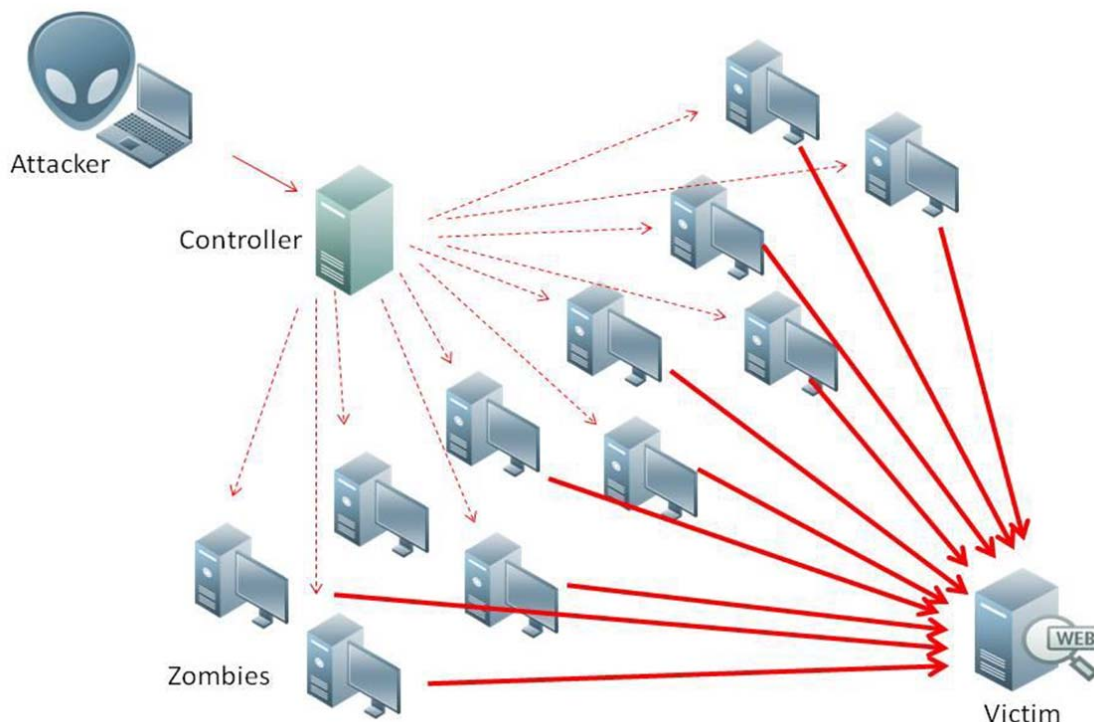
### 3.2.5 Denegación del servicio (DoS, Denial of Service)

Este tipo de ataques son muy comunes dada la sencillez de realización y que los perjuicios que se pueden causar pueden llegar a ser importantes.

La denegación del servicio consiste en sobrecargar el servidor de una empresa mediante un gran flujo de datos, consiguiendo que dicho servidor quede sobrecargado e inutilizado y que sus legítimos usuarios no puedan acceder.

Un claro ejemplo consiste en tener un conjunto de *bots*<sup>13</sup> que empiecen a acceder a la misma página web (10 accesos por segundo) durante un tiempo prolongado, consiguiendo que dicha página web se bloquee por no estar preparada para recibir tantos usuarios.

Ilustración 4. Diagrama de denegación del servicio



Fuente: [www.howtogeek.com](http://www.howtogeek.com)

<sup>13</sup> Bots (robots informáticos): ordenadores/servidores infectados que se ejecutan de manera autónoma y automática, pudiéndose controlar de forma remota.

En la imagen anterior se puede observar lo comentado y cómo un atacante puede, mediante la red de *bots* (zombies) atacar a su víctima denegando el acceso a todos los usuarios de dicha página web.

Según una encuesta realizada por la empresa Neustar, de las empresas participantes, un 73% sufrió un ataque DoS, un 49% perdió, al menos, 100.000 dólares por hora durante los periodos punta y el 53% tuvo un robo de datos como resultado del ataque DoS ya que resultó infectada la página web y se consiguió acceder a los sistemas de estas empresas.

Si se mira el impacto de estos ataques por zona geográfica, el resumen es el siguiente:

**Ilustración 5. DoS por zona geográfica**



Fuente: CCN-CERT (Centro Criptológico Nacional)

Se puede ver que el impacto de estos daños es a nivel mundial; recurrente, ya que se repite varias veces en las organizaciones; y, sobretodo, se suele utilizar como “puente” para iniciar otro tipos de ataque con *malware*.



### **3.2.6 Otros riesgos asociados a los ciberataques**

Una vez comentados los principales ciberriesgos que hay en la actualidad, se debe ser consciente de que cada uno de ellos puede derivar en otras variantes. Por ejemplo, una vez se ha producido un robo de información o un secuestro digital, posteriormente se puede sufrir una ciberextorsión reclamando dinero como compensación de no divulgar o para desbloquear la información.

Además de todo esto, siempre que ocurre un ciberataque, hay otros daños asociados que se pueden derivar. Claros ejemplos de estas consecuencias puede ser la pérdida de reputación, y como ya se ha comentado anteriormente que, por este motivo, aún hay muchas organizaciones que son reacias a reconocer que han sufrido un ataque cibernético; paralización de la actividad, ya que un ataque puede dejar inutilizados los equipos y por lo tanto bloquear la producción de una empresa; o incluso se podría llegar a la destrucción de los sistemas operativos y productivos, como se verá más adelante en los ejemplos.

Además de la pérdida de reputación, pueden haber otras pérdidas, como puede ser la de competitividad, si se sufre el robo de información confidencial y secreta, una pérdida de beneficios por el tiempo que han estado parados los sistemas o incluso una responsabilidad civil derivada de haber sufrido un robo de información de terceros.

## **3.3. Costes resultantes y etapas de un ciberataque**

Una vez se ha hecho una introducción de lo que es un ciberataque y a cuáles son los conocidos más comunes a día de hoy, se puede indagar en los factores que se ven afectados en un ataque cibernético y en las etapas en las cuales se desarrollan este tipo de ataques. Esta información será de mucha utilidad en puntos posteriores para analizar dónde se debe poner el foco y así poder reducir al máximo el riesgo de los ciberataques. También será muy útil para conocer qué costes se pueden transferir a un seguro y cuáles se deberán asumir de forma propia.

### **3.3.1 Factores de impacto**

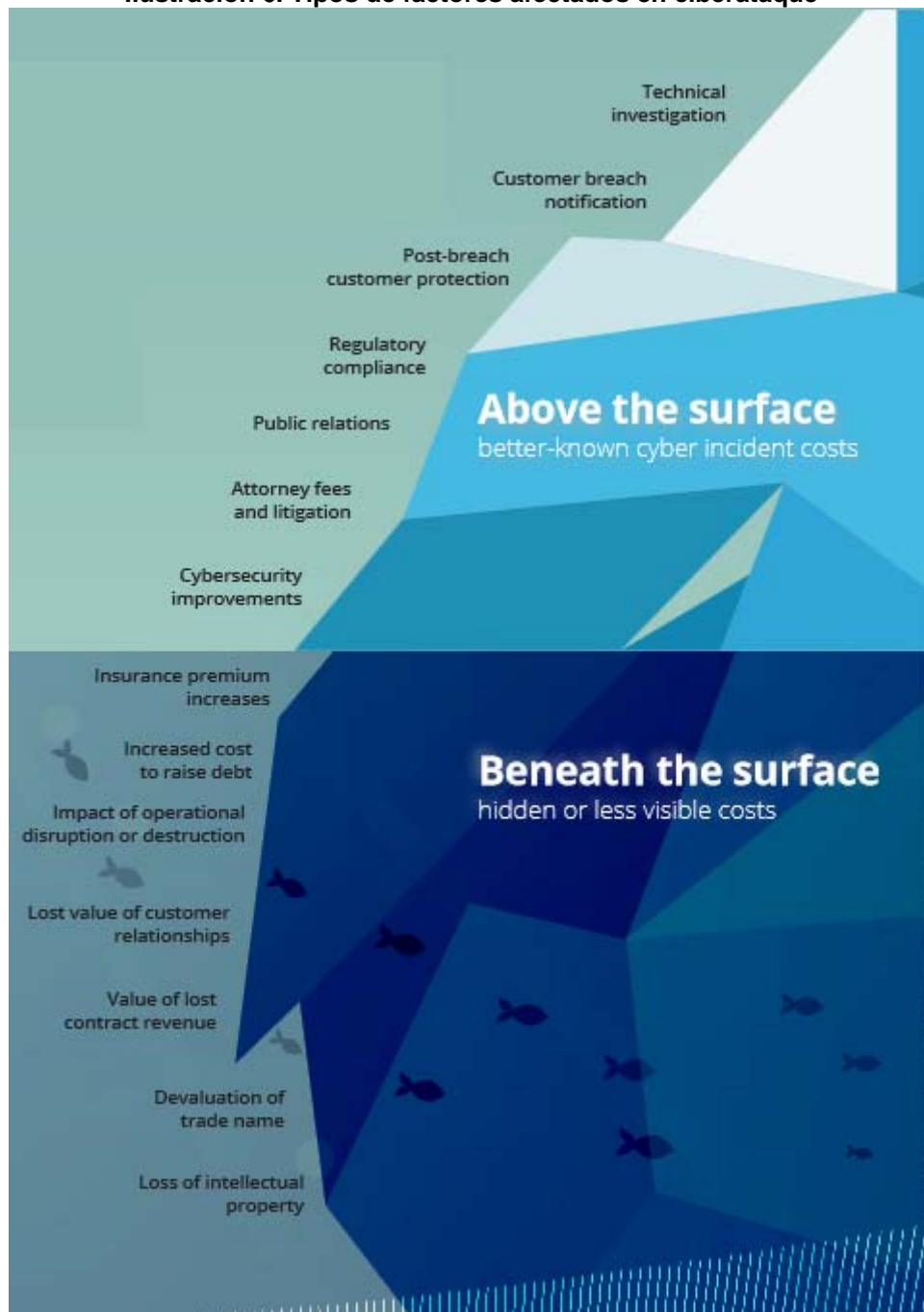
Tal y como se ha visto en los puntos anteriores, hay muchas maneras en las que un ciberataque puede afectar a una organización. El impacto dependerá directamente de la naturaleza y severidad de dicho ataque, así como de la preparación que tenga esta empresa ante estas posibles eventualidades.

Es por ello que hay 14 factores de impacto que se deben conocer y familiarizarse con ellos. Algunos son más comunes y conocidos y otros son incluso intangibles, siendo más difícil de cuantificar.

Por tanto, se podrían clasificar los 14 tipos de costes diferentes entre aquellos que se pueden cuantificar de forma objetiva y que por lo tanto son bien conocidos (los que están en la superficie, visibles) y aquellos costes que, por su natu-

raleza, es más complicado de cuantificar (los que están debajo de la superficie, ocultos):

**Ilustración 6. Tipos de factores afectados en ciberataque**



Fuente: Deloitte

Aquellos que se encuentran en la superficie son los siguientes:

- Investigación técnica

Básicamente son los costes asociados al análisis sobre lo que ha sucedido durante un incidente cibernético. Como objetivo inmediato tiene el detectar la propagación de un posible ataque y tomar medidas para limitar su impacto en los sistemas. Por tanto, es uno de los factores clave en

la gestión del *ERM* ya que, como se ha comentado anteriormente, es importantísimo reducir al máximo los riesgos y sus posibles impactos.

- Notificación de la brecha a los clientes

Una vez se ha sufrido un ataque, se debe comunicar a todos los clientes de los cuales se almacena información. Esta comunicación debe ser de forma fehaciente y, generalmente, se basa en enviar burofax o carta certificada. Según un estudio de Deloitte<sup>14</sup>, el coste medio es de \$2,75 por cliente.

- Protección post-brecha a los clientes

Costes directos asociados a la protección con servicios para detectar y proteger potenciales usos ilícitos de la información personal robada en el ataque cibernético. El coste medio, siempre según el estudio de Deloitte, suele estar en \$10 y \$30 por cliente.

- Cumplimiento normativo

Impuestos y multas que se puedan derivar del no cumplimiento normativo en cuanto a la protección de datos, establecido en cada país de forma diferente.

- Relaciones públicas

Son todos aquellos costes directos derivados del daño de imagen creado después de un ciberataque. Por lo tanto, incluye todas las campañas de publicidad que se lleven a cabo.

- Honorarios de abogados

Honorarios de abogados y costes de litigios que pueden abarcar una amplia gama de honorarios de asesoría legal, costes de liquidación de impuestos y costes asociados con acciones legales que la compañía puede tomar para defender sus intereses.

- Mejoras en ciberseguridad

Costes asociados con mejoras en ciberseguridad, que pueden incluir mejoras técnicas en infraestructuras, controles de seguridad, etc. en resumen, dotar a toda la organización de todos los medios necesarios para prevenir futuros ataques. Por lo tanto, igual que el primero, este es un factor muy importante a tener en cuenta ya que está directamente relacionado con la mejora continua de los procesos de la gerencia de riesgos.

Una vez se han revisado los factores que son fácilmente observables, se puede empezar a analizar los factores que están “debajo de la superficie” pero que, como ya se ha comentado, estos son más complicados de ver y analizar.

---

<sup>14</sup> Deloitte - Beneath the surface of a cyberattack (2016)



- Incrementos de la prima de los seguros

Debido a la falta de información y de experiencia siniestral en tanto en cuanto a ciberataques; una vez es conocido un nuevo ataque, las primas pueden incrementar de manera importante a todos los tomadores de este tipo de pólizas, aunque no hayan tenido siniestro alguno. Según el estudio de Deloitte, los incrementos pueden ir hasta el 200 por cien por la misma cobertura que el año anterior, e incluso denegar la cobertura del año siguiente una vez un ciberataque es conocido.

- Aumento del coste de la deuda

Otro de los costes “ocultos” debajo de la superficie. Es el incremento que ha de soportar una organización que sufre un ciberataque por su decremento de *rating* crediticio. Lleva a tener que soportar intereses más altos a la hora de solicitar o de renegociar una deuda.

- Impacto de la interrupción o destrucción operacional

Sufrir un ataque cibernético puede conllevar a una destrucción operacional, como puede ser la destrucción de maquinaria o la disminución de la capacidad productora. Por ello, hay unos costes de “puesta a punto” de toda esta maquinaria y de buscar alternativas temporales para poder recuperar la capacidad productiva cuando antes.

- Pérdida de valor en las relaciones con los clientes

Después de un ciberataque es difícil cuantificar cuántos usuarios se pierden. Para ello es posible hacer una aproximación asignando un “valor” a cada cliente para cuantificar cuánto debe invertir la organización para adquirir a uno igual. Este coste puede variar mucho en función del tipo de industria y de organización y por ello, evaluarlo con este método puede ser muy útil.

- Valor de los ingresos perdidos del contrato

Incluye la pérdida final de ingresos así como el coste futuro de oportunidad asociado con contratos que se cancelan debido a un incidente cibernético.

- Devaluación del nombre de la marca

Coste intangible pero a su vez muy importante. Se refiere a la pérdida en el valor de nombres, marcas o símbolos que una organización utiliza para distinguir sus productos y servicios.

- Pérdida de la propiedad intelectual

Otro coste intangible pero importantísimo ya que es el coste asociado a la pérdida del control de secretos del negocio, *copyrights*, planes de inversión y de información secreta y confidencial de otros propietarios; que puede llevar a la pérdida de capacidad competitiva, pérdida de ingresos y quizás a un daño económico irreparable para la organización.

Una vez analizados todos los factores que se han de tener en cuenta a la hora de analizar el impacto de un ciberataque, se puede proceder a analizar las fases en las que estos factores son mostrados.

### 3.3.2 Etapas tras un ciberataque

Una vez una organización ha sufrido un ataque cibernético, hay tres etapas diferenciadas en las cuales se aprecian los factores anteriormente comentados. Estas fases pueden variar en duración en función del tipo de organización y de medidas preventivas de las que disponga. Además, pueden subsistir a la misma vez durante un periodo de tiempo, por lo tanto, puede ser que se observen dos en el mismo momento.

La primera de las fases tras un ataque es la fase de triaje. Es una fase altamente reactiva, que se da en los primeros días o semanas después de descubrir el ataque. Durante esta fase se deben tomar decisiones y acciones a corto plazo, incluyendo la comunicación externa. También, si se ha producido una interrupción del negocio, se deben formular estrategias para la continuidad de las operaciones más importantes.

En esta fase se incluye el análisis de la brecha, cómo detenerlo si aún está en curso y la revisión de los controles de seguridad para evitar situaciones futuras similares. Este último punto, directamente relacionado con lo comentado en puntos anteriores, cuando se indicó que el *ERM* debe ser un proceso en constante actualización.

La segunda fase es la fase de gestión del impacto. Se suele dar en las semanas o meses posteriores al ataque y son los esfuerzos reactivos necesarios para reducir y abordar las consecuencias directas del incidente. Las decisiones a tomar pueden ser muy variadas en función del tipo de ataque y de la intensidad, pero pueden incluir los esfuerzos para mantener una infraestructura provisional y ajustar procesos operativos, reducir los daños en las relaciones con los clientes y socios e iniciar o responder a asuntos legales o de aplicación de la ley.

La última de las fases es la de la recuperación del negocio. Probablemente en todos los casos será la fase más larga, puede durar meses o años hasta que no se consigue la reparación de daños al negocio y la prevención de la ocurrencia de un evento similar en el futuro. Igual que en la fase anterior, también es muy variable en función de los negocios pero puede incluir la reconstrucción o rediseño de procesos, sistemas, aplicaciones u otros activos empresariales; desarrollo de estrategias para mejorar (o recuperar) la reputación; inversión en mejoras de seguridad, etc. En resumen, todas las medidas necesarias con el objetivo de salir de la crisis más fuertes que antes.

Tras hacer una revisión de todo lo que una organización se encuentra después de un ciberataque, se puede proceder a poner unos cuantos ejemplos ilustrativos de empresas que lo han sufrido y han tenido que lidiar con ello. Posteriormente, se procederá a comprobar si las organizaciones de hoy en día están tomando este tipo de riesgos con la importancia que realmente tienen.

### 3.4. Ejemplos reales

Definidos los principales riesgos cibernéticos que se conocen en la actualidad, se procederá a describir algunos de los ataques más conocidos que han sucedido y que han tenido gran impacto a nivel tanto de paralización y pérdida de beneficios como a nivel de pérdida de reputación.

#### 3.4.1 Robo de información en Sony Computer Entertainment

“Hemos descubierto que entre el 17 de Abril y el 19 de Abril de 2011, determinada información de usuarios de PlayStation Network y Qriocity fue puesta en compromiso en conexión con una intrusión ilegal no autorizada en nuestro sistema.

[...]

A pesar de estar todavía investigando los detalles de este incidente, creemos que personas no autorizadas han podido obtener vuestra información personal: nombre, dirección (ciudad, provincia y código postal), país, dirección de correo electrónico, fecha de nacimiento, nombre de acceso y contraseña de *PlayStation Network / Qriocity* y PSN ID. [...] A pesar de no haber evidencia de que los datos de tarjeta de crédito hayan sido obtenidos no podemos negar esta posibilidad.”

Esta información la facilitaba la compañía Sony a todos los usuarios de sus sistemas en el año 2011 después de que se perpetrara un acceso ilegal a sus servidores, robando numerosa cantidad de datos de, aproximadamente, 1.000.000 de usuarios.

#### 3.4.2 Robo de información y soporte digital en Sony Computer Entertainment

Nuevamente Sony, esta vez en 2015, sufrió un nuevo ataque en sus sistemas. En este caso, el ataque dirigido a la rama de entretenimiento de Sony Corp. habría sido el más destructivo hasta el momento contra una compañía privada en suelo estadounidense.

En este caso, se habrían borrado cantidades de datos, accedido al correo de los trabajadores así como a datos privados de los mismos (incluyendo resultados médicos, etc.) y también pirateado nuevas películas aún sin estrenar en la cartelera.

En palabras del presidente ejecutivo de Sony, Michael Lynton, se describía el ataque como “si alguien entrara a tu casa, te robara y luego la quemara”. “Como uno de los investigadores me dijo, quien fuese que escribió este software estaba muy, muy molesto”.

Todas las sospechas se dirigieron hacia el gobierno de Corea del Norte ya que Sony había anunciado el lanzamiento de su nueva película “The Interview” en la cual se ridiculizaba la imagen del líder norcoreano.

### **3.4.3 Papeles de Panamá (fuga de información)**

3 de abril de 2016, salta la noticia en 109 medios de comunicación de 76 países diferentes.

Una fuente no identificada se consiguió hacer con 2,6 terabytes de información de empresas, activos, ganancias y evasiones tributarias de jefes de Estado y de gobierno, líderes de la política mundial, y otras personalidades de negocios, arte y deporte.

Toda esta información pasa a ser de dominio público, creando uno de los mayores revuelos y escándalos de los últimos años. Todos los implicados contrataban al bufete de abogados consultores de empresas Mossack Fonseca para poder fundar y establecer compañías en paraísos fiscales de modo que se ocultara la identidad de los propietarios.

### **3.4.4 Stuxnet**

Según lo define el portal especializado Symantec “Esta amenaza no es parecida a nada de lo visto anteriormente, no sólo en lo que hace, sino en cómo se descubrió. Es el primer virus informático que permite hacer daño en el mundo físico. [...] Es también el primer ataque cibernético que hemos visto que ataca específicamente a sistemas de control industrial.”.

Tal y como indican, este virus se trata de un gusano informático que penetra en los sistemas de control de la maquinaria industrial y es capaz de reprogramarla para que se autodestruya.

Este caso se descubrió en 2010 cuando Stuxnet destruyó 1.000 máquinas en la central nuclear de Natanz, Iran. Esta maquinaria afectada participaba en la producción de materiales nucleares y se les dio instrucciones para autodestruirse. ¿La manera?

El primer paso fue acceder a la red de la central. Sysmantec afirma que la posibilidad más viable fue que entrara a través de una memoria USB infectada.

Una vez en el interior de la red, Stuxnet buscó el software que controla las centrifugadoras (maquinaria que gira a altas velocidades para, en este caso, obtener el uranio enriquecido).

En el momento en el que el gusano encontró este software, se encargó de reprogramarlo para que se aceleraran y empezaran a girar peligrosamente rápido para, posteriormente, hacerlas girar demasiado lento. Estas fluctuaciones en las velocidades se produjeron distintas veces durante varios meses.

Esta variación en las velocidades, con el tiempo, provocó en las centrifugadoras una tensión para la que no estaban preparadas, logrando dejarlas fuera de servicio.

Analizando el virus, se considera que detrás están los servicios secretos de Estados Unidos y de Israel, con lo cual sería un claro ejemplo de ataque bélico y de cómo pueden evolucionar las guerras en los próximos años.

### **3.4.5 US Target Corporation**

Se trata de la tercera cadena de venta al por menor de Estados Unidos y sufrió una violación de datos masiva consistente en el robo de hasta 70 millones de tarjetas de crédito y de débito de sus clientes.

El malware se activó a través de un correo electrónico que había llegado a la empresa contratada para gestionar el sistema de aire acondicionado, que estaba conectado al sistema informático de Target.

Se estimó que el daño económico superó probablemente los 1.000 millones de dólares americanos de los cuales 264 millones de dólares serían de costes directos ocasionados por dicha violación de datos.

### **3.4.6 Anthem, aseguradora de Salud estadounidense**

Las aseguradoras tampoco se han librado de sufrir este tipo de ataques y fue Anthem, la segunda aseguradora de Salud más importante de EE.UU., sufrió una violación de datos a gran escala.

Fueron sustraídos 78 millones de números de afiliación a la seguridad social y otros datos de todos sus ramos de negocio, con la comprensible duda de para qué serán usados (en hospitales, urgencias, farmacias...).

En este caso, la aseguradora disponía de una póliza Cyber pero que agotó el límite solo con los costes de las notificaciones a las víctimas y los servicios para controlar posibles robos y créditos.

### **3.4.7 WannaCry**

12 de mayo de 2017. Esta fecha tardará en olvidarse dentro de muchas empresas de todo el mundo, incluida Telefónica.

Este día se produjo el mayor ataque cibernético en España, afectando a diferentes empresas del Ibex-35 y a grandes empresas de otros países.

Las estimaciones indican que se han visto afectados 74 países, entre los que se encuentran España, Taiwán, Ucrania, Turquía, Rusia o el Reino Unido, donde el *heckeo* ha afectado a más de una docena de hospitales y centros médicos.

En este caso, se trató de un ataque de *Ransomware* (ya comentado en puntos anteriores) en el cual se pedía un rescate con Bitcoins<sup>15</sup> (en concreto se exigían 300 dólares en esta moneda digital) y que aprovechaba una vulnerabilidad detectada de Microsoft. Esta vulnerabilidad, denominada *EternalBlue*, fue conocida por Microsoft en el mes de marzo, y un día después se empezó a distribuir parches de seguridad. Sin embargo, aquellos equipos que no habían actualizado su sistema operativo y que, por lo tanto, no tenían instalado el mencionado parche, aún tenían la vulnerabilidad accesible.

Y así sucedió, en el mes de mayo, cuando a numerosos ordenadores de grandes compañías les empezó a aparecer el siguiente mensaje:

Ilustración 7. Mensaje Wanna Cry



Fuente: <http://www.asuamaytinh.com/>

La aparición de este ataque hizo que muchas empresas importantes del país, decidiesen dejar de trabajar y apagar todos sus ordenadores ante el miedo de verse infectados.

A medida que han ido pasado los días y que se ha podido ir investigando, se sospecha que el ataque no tenía una intención recaudatoria de dinero sino que más bien tenía intenciones de probatura (lo que aún no se conoce para qué). El motivo de esta sospecha es que, en el mensaje mostrado anteriormente, la dirección de correo electrónico a la que se debía remitir el pago del rescate, no estaba registrada (no pertenecía a nadie) y por lo tanto, nadie podía recaudar el dinero si se pagaba.

<sup>15</sup> Bitcoin: Moneda virtual. Descentralizada, no está respaldada por ningún gobierno ni depende de ninguna entidad bancaria y con transacciones directas sin intermediarios.

Además, a día de efectuar esta tesis, no se ha encontrado todavía el “paciente cero” es decir, no se ha encontrado cuál fue el origen y quién fue la primera persona que se infectó con este *ransomware* y que se fue transmitiendo de equipo en equipo.

### 3.4.8 *Petya*

Durante la realización de esta tesis sucedió un nuevo ataque *ransomware*, que recibió el nombre de *Petya*.

Según comentan los expertos, este nuevo ataque, que también accedía a los sistemas a través de una brecha en Microsoft, es mucho más profesional y complejo que *WannaCry* ya que el diseño y la estrategia del ataque estuvo cuidadosamente planeado para que se extendiera de forma rápida y eficaz. Además, se encargaron de corregir muchos de los errores de su predecesor, eliminando, por ejemplo, cualquier interruptor de seguridad que permitiese anular el *malware*.

Sin embargo, de nuevo, una de las preguntas es quién hay detrás de este ataque y cuál es su principal objetivo ya que, de nuevo, parece que no es tanto un motivo económico sino un motivo de causar daños a objetivos concretos.

Se han visto afectados más de 64 países, entre ellos Rusia, Polonia, Italia, Alemania y, sobre todo, Ucrania, que ha sido el que más ha sufrido. Es por ello que se sospecha que puede ser un ataque planificado por algún gobierno, pero aún se desconoce el origen y el “paciente cero” (primer dispositivo en infectarse).

## 3.5. Penetración en el tejido empresarial

Una vez se ha hecho una pequeña introducción al concepto de ciberataques, los factores que intervienen, costes “visibles” y “ocultos” y vistos algunos de los principales ejemplos que existen en la actualidad, es el momento de analizar si a día de hoy la gente está concienciada con estos riesgos o si, por el contrario, aún parece un concepto etéreo del cual no hay que preocuparse ni afrontar.

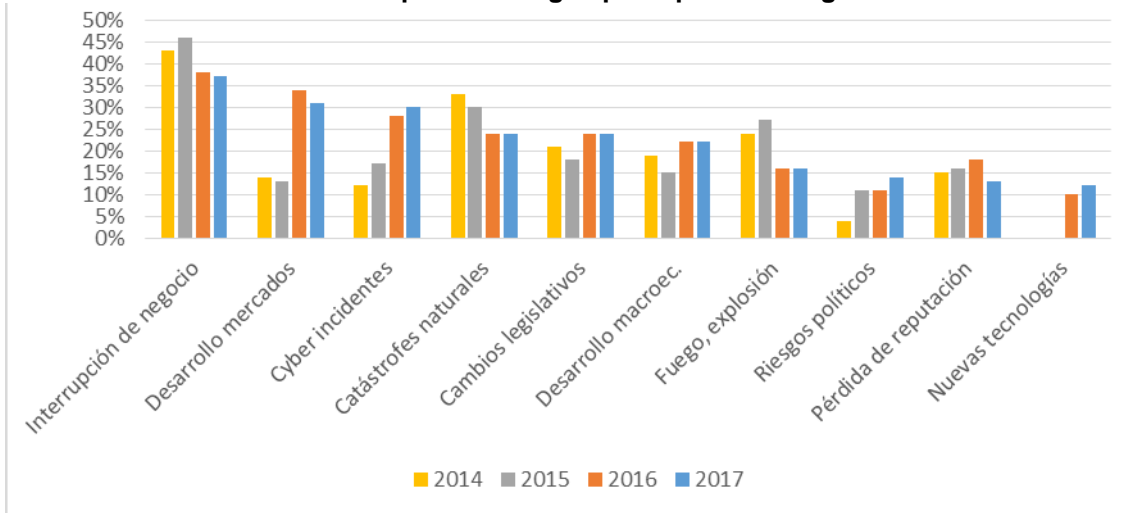
Recordando el gráfico ya visto anteriormente basado en los datos de Allianz<sup>16</sup>, se puede analizar si la ciberseguridad es una preocupación a día de hoy:

---

<sup>16</sup> Allianz - Allianz Risk Barometer (2017)



**Gráfico 9. Top 10 de riesgos principales de negocios**

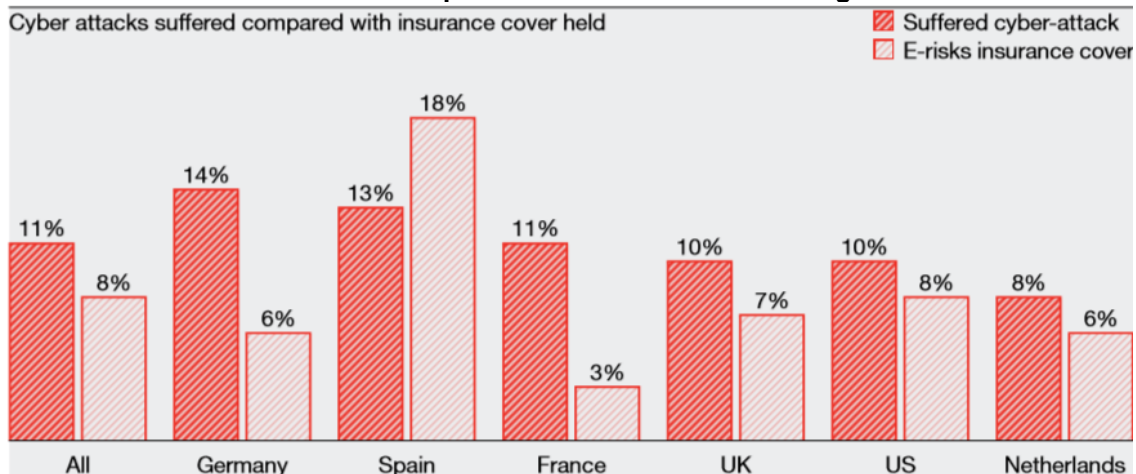


Fuente: elaboración propia con datos de Allianz

Se puede observar la clara evolución de todos los peligros relacionados con la digitalización y la nueva era tecnológica ya que los únicos riesgos que incrementan en preocupación son los de “ciberincidentes” y los relacionados con la aparición de “nuevas tecnologías”.

Sin embargo, existe una gran diferencia entre la preocupación que muestran los empresarios con la realidad de protección ante estos ataques. Acudiendo al estudio Hiscox<sup>17</sup>, se puede observar las pocas empresas que reconocen tener asegurados los ciberriesgos:

**Gráfico 10. Ciberataques sufridos vs. cobertura aseguradora**



Fuente: Hiscox

Se puede observar que, del general de las organizaciones, solo un 8% reconocen tener asegurados los riesgos cibernéticos (de todos los países, destaca positivamente España, donde este porcentaje aumenta hasta el 18%).

Centrando el foco en España, un 74% afirma no haber sufrido nunca un ataque cibernético. Un 13% dice no saberlo y el otro 13% confirma haber sufrido uno.

<sup>17</sup> Hiscox - DNA of an Entrepreneur report 2016 (2017)



De los que lo han sufrido, un 37% indica que las pérdidas que se ocasionaron fueron graves para la empresa. Además, de estos que han sufrido un ataque, el 78% no disponía de seguro para cubrir los daños probocados por el ataque.

Por lo tanto, se puede concluir que a pesar de que existe un miedo generalizado en las organizaciones a sufrir un ataque de este tipo, de momento parece ser un concepto más “etéreo” ya que no se corresponde con la realidad asegurada.



## 4. La cuarta revolución industrial y el *Big Data*

Otra de las variables que se ha de tener en cuenta a la hora de analizar el posible impacto de los ciberriesgos en la Gerencia de Riesgos es la cuarta revolución industrial, impulsada sobre todo por una automatización de procesos y apoyada por el *Big Data*.

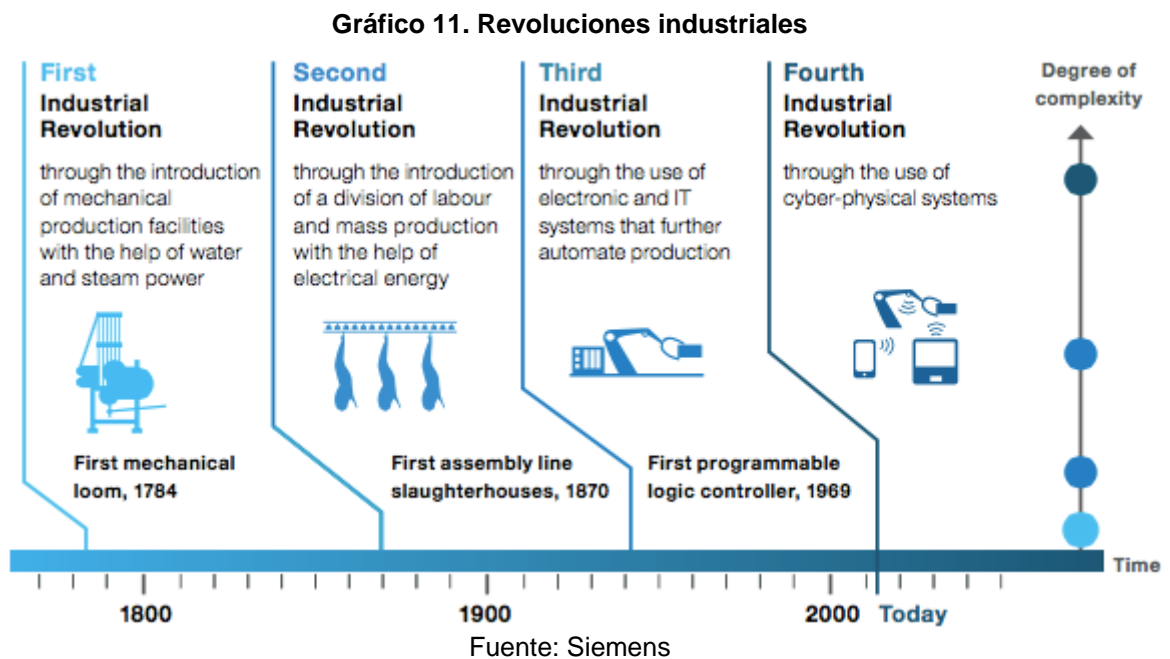
### 4.1. La cuarta revolución industrial

La cuarta revolución industrial ha sido el tema principal de 2016 del *World Economic Forum (WEF)*, más conocido como *Foro de Davos*, por la ubicación de sus reuniones, que se realizan en el Monte de Davos, en Suiza.

Tal y como ellos se definen son una organización internacional, independiente y sin ánimo de lucro que reúne a los principales líderes políticos, empresariales y otros de la sociedad para dar tratar temas con afectación mundial.

Por lo tanto, que haya sido el tema estrella de este foro es un indicador de la importancia y magnitud que está adquiriendo este concepto.

A modo resumen, las revoluciones industriales que ha sufrido la humanidad son las siguientes:



Como se puede ver en la imagen anterior, la primera revolución industrial, que data aproximadamente de entre los años 1760 y 1830, marcó el paso de la producción manual a la mecanizada.

La segunda revolución industrial, aproximadamente sobre el año 1850-1870 trajo la electricidad y permitió la manufactura en masa.

La tercera hubo que esperar a mediados del siglo XX, con la llegada de la electrónica y la tecnología de la información y las telecomunicaciones. Un ejemplo representativo es la aparición del primer *Programmable Logic Controller* (PLC), en 1969.

“La cuarta revolución industrial, no se define por un conjunto de tecnologías emergentes en sí mismas, sino por una transición hacia nuevos sistemas que están contruidos sobre la infraestructura de la revolución digital (anterior)”. Palabras de Schwab, director ejecutivo del *WEF*, y uno de los principales entusiastas de la nueva revolución.

Por lo tanto, el concepto de Industria 4.0, corresponde a una nueva manera de aprovechar los sistemas que ya se consiguieron en la tercera revolución industrial. El objetivo es alcanzar fábricas “inteligentes” (*Smart factories*), basadas en la automatización completa de todo el proceso industrial y así mejorar la eficiencia del proceso de producción.

Las bases tecnológicas en las que se apoya esta nueva orientación son el Internet de las cosas (*Internet Of Things – IoT*), tecnologías y sistemas ciberfísicos, cultura “hágalo usted mismo” (*Build Your Own – BYO*), *Big Data*, etc.

“Hay tres razones por las que las transformaciones actuales no representan una prolongación de la tercera revolución industrial, sino la llegada de una distinta: la velocidad, el alcance y el impacto de los sistemas. La velocidad de los avances actuales no tiene precedentes en la historia...y está interfiriendo en casi todas las industrias de todos los países”, apunta el *WEF*.

Toda esta nueva revolución industrial hará que se deban cambiar los modelos de negocios de las empresas y creará muchas oportunidades y amenazas a las que se deberán enfrentar las organizaciones y de las que únicamente saldrán victoriosos las que sepan adaptarse al cambio.

El hecho de tener lo que se ha denominado como “fábrica inteligente” hará que se deban tener todos los sistemas interconectados mediante una red a través de la cual se gestionará todo (ritmo de producción, funcionamiento de las máquinas, carga de las mismas, etc.). Todas estas interconexiones que serán necesarias, y que poco a poco se van dando en las industrias actuales, abren un número desconocido de ventanas por las cuales todos los ciberataques pueden entrar.

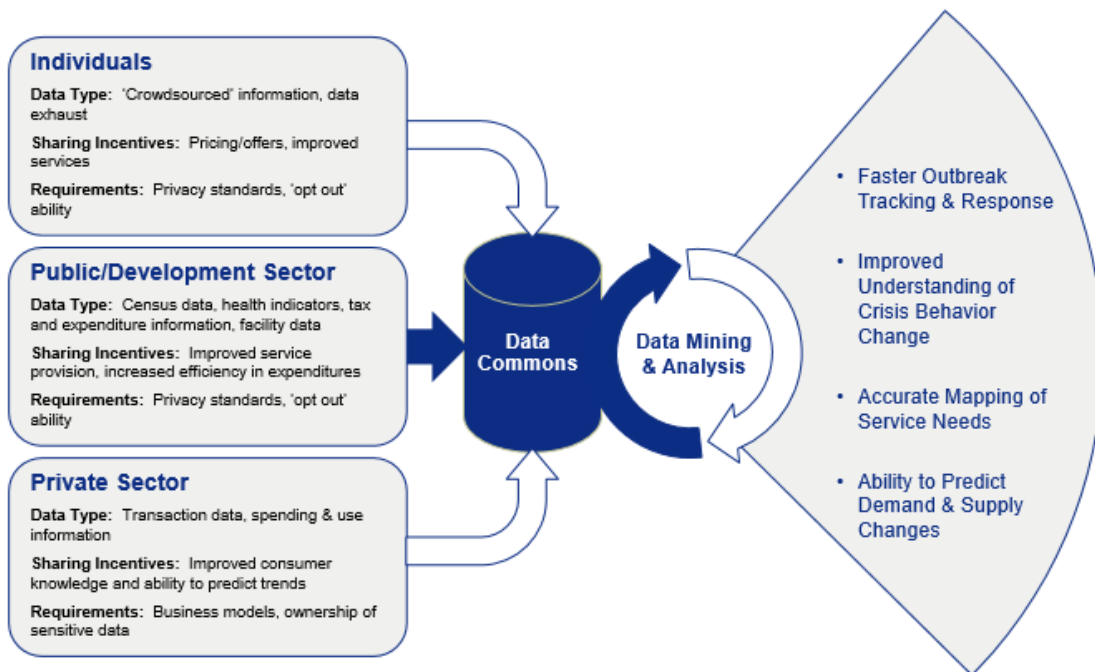
Parece claro pensar que, a mayor conectividad y mayor dependencia de los sistemas tecnológicos, mayor es la posibilidad de tener una pérdida económica (y de mayor cuantía) si se sufre un ataque cibernético.

## 4.2. Big Data

Uno de los aspectos que impulsa a la cuarta revolución industrial comentada en el punto anterior es la aparición del *Big Data*. O quizás, más que la aparición es el aprovechamiento de la información que se va almacenando y de la que hasta ahora no se ha sacado provecho.

Pero, ¿qué es el *Big Data*? El *Big Data* es un término que hace referencia al almacenaje y proceso de una gran cantidad de datos. De forma esquemática, sería:

Gráfico 12. Big data



Fuente: weforum

En la imagen anterior se puede observar que tenemos una base de datos enorme y que se va nutriendo cada día con infinidad de bytes y que, posteriormente, hay que procesar y analizar para obtener la información que se desea.

Y todo este tipo de datos...¿qué son y de dónde provienen?

Los datos que se almacenan pueden provenir de infinidad de lugares. Puede ser desde información transaccional que las organizaciones guardan de sus clientes, proveedores, etc. así como también se pueden obtener del sector público ya que la administración gestiona datos como el censo de población, registros médicos, impuestos, etc. Además de todo ello, también hay datos que provienen directamente de los usuarios, como por ejemplo de las redes sociales (se manejan datos de que en un día se generan alrededor de 2,5 quintillones<sup>18</sup> de bytes mundialmente).

<sup>18</sup> 1 quintillón =  $10^{30}$  = 1.000.000.000.000.000.000.000.000.000

Todos estos datos que se han comentado son datos generados por los seres humanos pero, cada vez más, también hay los datos utilizados para la comunicación entre máquinas, denominados *machine-to-machine (M2M)*, como pueden ser, por ejemplo, los sensores digitales de contenedores para determinar la ruta de entrega de algún paquete. Se estima que el número de datos creados *M2M* crezca del orden de un 30% anual.

Quien más quien menos siempre ha hecho un almacenaje de toda la información que iba recogiendo. El principal problema del *Big Data* es la gestión de toda esta información y, sobre todo, la explotación de dicha base de datos.

Si este análisis de los datos almacenados se hace de forma ágil y adecuada, los beneficios que puede obtener la organización son incalculables ya que será capaz de, entre otras cosas, analizar correctamente las necesidades y comportamientos de sus clientes, teniendo la habilidad de predecir cambios en la demanda y la oferta.

Igual que en el punto anterior de la revolución industrial, el tema del *Big Data* abre una infinidad de oportunidades a las empresas para evolucionar y automatizarse, aumentando la efectividad, pero tiene amenazas muy importantes y peligrosas, sobre todo pensando en ataques cibernéticos. Almacenar tantos datos, muchos de ellos personales, sensibles y confidenciales, de personas, puede suponer grandes problemas sobre protección de datos con lo cual todos estos datos que se almacenen deben de estar adecuadamente protegidos y siempre deberán tener una importancia elevada dentro del mapa de riesgos del *ERM* ya que el impacto que puede llegar a tener en la cuenta de resultados (por sanciones y por pérdida de negocio por pérdida de reputación y marca), pueden ser muy negativos.

## 5. Impacto de los Ciberriesgos en la Gerencia de Riesgos tradicional

Una vez que se han analizado las variables que pueden afectar a la evolución del *ERM* de una organización empresarial en lo referente a la nueva era de las tecnologías, es conveniente hacer un breve resumen para poner en situación y así posteriormente poder analizar el impacto real que se puede esperar.

Por tanto, de lo visto en los puntos anteriores, se debería recordar que:

- El *ERM* es un proceso sobre el cual la empresa analiza todos los riesgos a los que está expuesto y que, con mayor o menor frecuencia, puede sufrir; y que significaría un impacto en la cuenta de resultados de la organización.
- Que dicho *ERM* debe ser un proceso continuo.
- Este proceso deriva en un resumen esquemático que recibe el nombre de matriz de riesgos y de mapa de riesgos y que debe ser sobre lo que pivote todo análisis y actualización.
- Otro punto importante de la Gerencia de Riesgos es la decisión de retención y transferencia. Para ello, se debe conocer, entre otros aspectos, las soluciones aseguradoras disponibles en cada momento para poder hacer el correcto análisis de costes.
- Los ciberriesgos están en constante evolución. Los que se conocen hoy en día seguramente no tienen nada que ver con los que se verán en un futuro. Serán más sofisticados y más peligrosos, pudiendo causar un impacto mucho mayor.
- Las fases tras un ataque de este tipo pueden prolongarse en el tiempo durante años, por lo tanto no es un riesgo que se soluciona de manera inmediata
- Los costes que se derivan de un ataque pueden ser costes “visibles” o pueden ser costes “debajo de la superficie”, los cuales son más complicados de analizar y valorar, así como de protegerse ante ellos.
- Cada vez más y más rápido, se está interconectando todo el mundo, aumentando el peligro de expansión de los ciberataques.
- Con la cuarta revolución industrial, cada vez más todos los procesos e información de las empresas dependen de las tecnologías, por lo tanto, sufrir un ciberataque puede tener un mayor impacto en la cuenta de resultados.

- Como nota positiva, cada vez la gente parece estar más concienciada sobre estos peligros, pero siempre dentro de un marco de incertidumbre, por la evolución de estos riesgos.
- Como nota negativa, este incremento en la concienciación de las organizaciones sobre los ciberriesgos no se traduce en una mayor transferencia de estos peligros a través de pólizas aseguradoras.

Con todo lo visto hasta ahora durante todo el desarrollo del proyecto y en el resumen inmediatamente anterior, se desprende que el futuro de los ciberataques es incierto. Es por ello que se deben tener en constante vigilancia.

Pero, ¿cómo han afectado realmente los ciberriesgos a la gerencia de riesgos tradicional?

Hace unos años, las empresas, realizando un correcto proceso de *ERM* podían tener controlados todos los riesgos a los que se enfrentaban y, en mayor o menor medida, saber a qué se podían enfrentar (severidad del riesgo) y cada cuánto (frecuencia del mismo). Con lo cual, lógicamente era necesario ir actualizando todo el proceso de Gerencia de Riesgos pero siempre moviéndose sobre unos parámetros muy similares. Además, era relativamente sencillo saber qué se podía transferir a entidades aseguradoras a través de pólizas de seguros ya que la mayoría de daños que se podían causar eran a nivel material (incendios, averías, etc.) o a nivel financiero (pérdida de beneficios, pérdidas de inversiones, etc.). Estos daños son comunes en los cuales las entidades aseguradoras se sienten cómodas realizando su actividad ya que conocen desde hace mucho tiempo y, a través de los cálculos actuariales correspondientes, saben qué prima han de cobrar para que el negocio sea rentable.

Sin embargo, la aparición de estos nuevos tipos de riesgos, los cibernéticos, ha creado todo un entorno de incerteza, tanto a las organizaciones como a las compañías aseguradoras. Esta incerteza viene derivada por el desconocimiento de la evolución que tendrán estos nuevos riesgos. Es por ello que, tal y como ya se ha ido comentando anteriormente, las organizaciones han de estar constantemente actualizando el mapa de riesgos del *ERM* para tener monitorizado tanto la frecuencia como el impacto que pueden tener en la cuenta de resultados estos riesgos. Es por ello que será importante que el gestor de riesgos sea una persona competente en estos nuevos aspectos tecnológicos y que esté permanentemente actualizado para conocer la evolución que sufren los ciberriesgos y los nuevos impactos que pueden provocar.

Por lo tanto, a nivel de la organización, todo debería pivotar entorno al mapa de riesgos, para saber cuáles se pueden reducir, cuáles transferir y cuáles asumir, siendo conocedores del impacto que puede causar en todo momento.

En lo que hace referencia a la transferencia de los riesgos, es decir, en cómo afecta a las compañías aseguradoras estos ataques cibernéticos, hay que comentar que la incerteza creada alrededor de la nueva era tecnológica también supone un gran cambio respecto a la manera de asegurar tradicional. Las pólizas de ciberriesgos, como veremos más adelante, aseguran todo lo que, ac-



tualmente, se conoce (infección de equipos, robo de información, etc.). Pero, ¿será esto suficiente y se podrá considerar una póliza estándar para todas las organizaciones? ¿qué prima técnica deben tener estas pólizas si no se dispone de datos siniestros?

Todas estas preguntas será el entorno que deberán afrontar todas las aseguradoras que quieran aprovechar la aparición de nuevos ataques cibernéticos como una oportunidad de vender más pólizas a todas aquellas empresas que realmente se preocupen por el impacto que les puede suponer.

Una vez introducida la problemática que se encuentran a día de hoy las compañías aseguradoras, es posible analizar la situación de estas pólizas en la actualidad para ver qué pueden contratar las organizaciones para transferir estos riesgos.

## **5.1. Solución aseguradora actual**

La principal manera que tienen las empresas hoy en día de protegerse contra los ciberriesgos es acudiendo a las compañías aseguradoras y transferir el riesgo.

La transferencia que se puede hacer, como se verá a continuación, no es de la totalidad del riesgo y, por lo tanto, siempre tendrá que haber una parte de retención. Por tanto, adquiere todavía más importancia el hecho de tener completamente actualizado el *ERM* y el mapa de riesgos, para así tener la información al día y saber qué parte se está reteniendo por parte de la organización y el impacto que ello puede suponer en la cuenta de resultados.

A continuación se procederá a analizar las partes que componen tanto la contratación de la póliza (cuestionarios, reuniones, etc.) como la composición estándar de estos productos (qué cubren, qué no cubren, etc.).

### **5.1.1 Cuestionario de solicitud de póliza**

Antes de la contratación de una póliza de ciberriesgos, la empresa que está buscando su protección frente a estos ataques se debe someter a un cuestionario previo. Dependiendo del producto a comprar y de la compañía aseguradora, el cuestionario es más o menos amplio.

Los cuestionarios de las aseguradoras no son estándar ni comunes y por lo tanto la información que se solicita es diferente, aunque la esencia de lo que se pide sí que se puede considerar similar.

Si el producto que se desea contratar es un producto con garantías básicas, el cuestionario al que se somete la organización es un cuestionario más corto y básico. Generalmente, los datos que más preocupan es si se trabaja en el mercado de Estados Unidos (ya que los ataques en este país son mucho más frecuentes y cuantiosos); si almacena datos de terceros (ya que se puede incurrir en más daños por Responsabilidad Civil); e información general de la empresa

como actividad, facturación e información que puede ayudar a conocer en profundidad a la organización a asegurar. También se suele preguntar sobre protección ante posibles intrusiones.

Si la póliza que se está buscando es más completa, con mayores coberturas (se verá más adelante), el cuestionario puede ser un poco más extenso y se solicitará, además de lo comentado en el párrafo anterior, actividad que se tiene no solo en Estados Unidos sino también en el resto de países. También, además de preguntar sobre protección ante posibles intrusiones, también se suele preguntar sobre el tiempo aproximado que se calcula para volver a restaurar los sistemas y el impacto que se estima que podría tener un ciberataque en la cuenta de resultados.

### **5.1.2 Reunión**

Una vez cumplimentado el cuestionario, en función del tipo de póliza y del tamaño de la empresa, el siguiente paso es reunirse con los responsables de la organización, utilizando el cuestionario como guion, pero siempre intentando obtener más información de la empresa, para hacerse una idea sobre la protección ante los ciberriesgos y el impacto que pueden suponer en la cuenta de resultados, para ofrecer la mejor póliza posible, siempre teniendo en cuenta de que no se podrá transferir todo y que habrá que retener algo del riesgo.

### **5.1.3 Análisis de la información**

Cuando la compañía aseguradora dispone ya de toda la información porque tiene el cuestionario de solicitud de póliza cumplimentado y han tenido una reunión con los altos cargos de la organización, es el momento de analizarlo todo y comprobar si se le puede dar la cobertura que solicita o no.

Para ello, además de ayudarse de toda la información recogida, es muy común utilizar compañías como *BitSight*, que ofrecen un *rating* de protección al ciberataque.

De igual manera que hay compañías que se dedican a hacer *ratings* financieros de las organizaciones (*Standard and Poor's*, por ejemplo), también están empezando a aparecer compañías que se dedican a hacer análisis sobre las protecciones y las facilidades de acceso al sistema de una empresa.

Para ello, siempre intentándose mantener dentro de la legalidad, intentan encontrar brechas en los sistemas de las organizaciones, sin llegar a penetrar a ellas.

Con esta información pueden ofrecer una valoración que, a la postre, puede ser de mucha utilidad a las compañías aseguradoras para conocer si realmente una compañía está bien protegida o si presenta brechas de seguridad muy claras en sus sistemas.

#### 5.1.4 Cobertura aseguradora

Una vez se ha recabado toda la información necesaria para dar cobertura a la organización, si todo está dentro de unos estándares de seguridad, se puede ofrecer la póliza. Como se ha mencionado anteriormente, hay diferentes tipos de póliza, en función de la cobertura que ofrecen.

Generalmente, la división de las pólizas de ciberriesgos es común y, en lo que se diferencian, es en el alcance de dichas coberturas.

Para ello, siempre se ofrece cobertura para la responsabilidad frente a terceros, los daños ocasionados a la propia organización, los costes de la gestión de incidentes después de un ciberataque y servicios online de prevención y análisis.

##### Responsabilidad frente a terceros

En función del tipo de póliza, se da cobertura a la responsabilidad frente a terceros por:

- La violación de la privacidad y confidencialidad por una brecha, para pérdidas de datos personales y/o corporales.
- La seguridad de la red, por reclamaciones por fallar en la protección de la red.
- La actividad en medios digitales. Reclamaciones por difusión de contenidos en portales de la sociedad (como web, blogs, etc.).
- Costes legales. Costes por la defensa y multas o penalizaciones.
- Costes de investigación interna y externa.
- Costes *PCI DSS* (*Payment Card Industry Data Security Standard* – Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago), por penalizaciones contractuales impuestas por la *PCI* por una brecha de datos, incumpliendo los *DSS*.

##### Daños a la propia organización

Además de asumir los costes y reclamaciones de terceros por un hecho causado dentro de los sistemas del asegurado, las pólizas Cyber también asumen una parte de daños causados a la propia organización a causa de una brecha:

- Pérdida de Beneficios por interrupción del negocio a causa de un ciberataque, así como otros costes asociados. Esta interrupción del negocio se refiere a la pérdida por la interrupción de redes.

- Pérdida de Beneficios por la interrupción del negocio a causa de un error interno o a causa de un fallo técnico inesperado.
- Pérdida de Beneficios por la interrupción del negocio debido a una orden del Regulador.
- Pérdida económica sufrida por un robo de ciberatacantes.
- Costes asociados con la Ciberextorsión.

### Costes de la gestión de incidentes

Además de los daños a terceros y de la interrupción de negocio que pueda sufrir la organización, también se incluyen otro tipo de gastos, derivados de la gestión de los incidentes:

- Costes de la gestión de incidentes, para los costes asociados con un ciberincidente.
- Primera respuesta, que incluye los honorarios y gastos de asesores de respuesta, especialistas tecnológicos y consultores en relaciones públicas, debido a algún fallo (de seguridad, sistemas...)
- Servicios legales, compuesto por los honorarios de un asesor para coordinar las labores de coordinación y notificación a los afectados, así como realizar el seguimiento de las quejas.
- Informática forense. Gastos y honorarios de un especialista tecnológico para determinar lo ocurrido e identificar si ha supuesto un uso ilegítimo de datos personales o de información corporativa. También será el encargado de contener el ataque, resolverlo (eliminar software malicioso, virus, etc.) y examinar el sistema para proponer acciones correctivas necesarias.
- Recuperación de datos, incluyendo los costes y gastos de determinar si los datos son recuperables, recrearlos en el caso que sea posible y reconfigurar el software.
- Restitución de imagen. Consultor de relaciones públicas y cualquier otro consultor independiente para prevenir o mitigar el potencial daño reputacional. Incluye el diseño y gestión de una estrategia de comunicación.
- Gastos de notificación. Gastos, costes y honorarios necesarios para la creación de un centro de atención al cliente (o *Call Center*) para recopilar toda la información de afectados y preparar las notificaciones necesarias por una violación de datos.

- Servicios de control de identidad y crédito, que incluye los honorarios, costes y gastos necesarios para servicios de control de crédito y robo de identidad de personas físicas por un posible empleo ilegítimo de datos personales.

### Servicios Online

Además de todos los costes referidos anteriormente, algunas pólizas Cyber, sobre todo las que están enfocadas a empresas de un tamaño menor, suelen incorporar unos servicios de prevención en sus pólizas y que, en su gran mayoría, se gestionan de forma online.

Este servicio incluye:

- Análisis de vulnerabilidades internas, tomando en cuenta toda la red de la organización y buscando posibles brechas y puntos de acceso a los sistemas. Se emite un informe con las vulnerabilidades detectadas y los métodos correctivos que se puedan/deban tomar.
- Análisis de vulnerabilidades de páginas Web. Igual que el punto anterior, se analizan los posibles puntos de acceso a través de la URL de la compañía.
- Corrección de vulnerabilidades en remoto. De aquellas detectadas en los puntos anteriores y que se puedan hacer en remoto y sin coste para la organización, el proveedor del servicio se compromete a corregirlas.
- Aplicación *AntiRansomWare*. Se trata de un software que actúa de forma preventiva e intenta evitar la instalación de las extensiones de archivo típicas de los *Ransomware*, dentro de las rutas típicas en las que se suelen almacenar.
- Evaluación del cumplimiento de la LOPD. Como servicio adicional, ofrecen un software que ayuda a la organización a tener toda la documentación almacenada y protegida tal y como indica la normativa actual.
- Vigilancia digital y reputación online. También, como servicio adicional, ponen a disposición del asegurado la posibilidad de monitorizar todos los comentarios que salen de la empresa por internet y gestionarlos de la manera que se crea oportuna.

Todo lo comentado suele encontrarse en pólizas estándar para empresas de diferentes tamaños. Hay algunos de los servicios que únicamente se ofrecen en pólizas de empresas pequeñas dado que, por sus características, pueden no disponer de un servicio informático tan completo como en una gran organización.

Sin embargo, las pólizas con las garantías más completas tienen una prima mucho más elevada, lo que impide a las pequeñas empresas acceder a este tipo de seguros completos y únicamente quedan al alcance de las grandes organizaciones.

Estas pólizas más completas, además de lo comentado anteriormente, se pueden acabar ampliando según las necesidades de la organización a asegurar. Por ejemplo, se ha visto pólizas que incluían ampliación de cobertura para todas las filiales, repartidas por diferentes países (es decir, que no se limitaba únicamente a España); ampliación de los fallos no únicamente de los sistemas y redes sino también a fallos en servicios *Cloud*<sup>19</sup>, incluyendo también las pérdidas de beneficio por interrupción de negocio que pueda generar este fallo; *hacking* telefónico, es decir, que se utilicen los sistemas telefónicos de la sociedad mediante un acceso no autorizado; cupón *Goodwill*<sup>20</sup>, donde se asegura la pérdida del cupón que se produzca como resultado de una interrupción material; e incluso se asegura el fallo de un proveedor externo de servicios.

Esta última garantía que se ofrece es una cobertura que asegura cualquier pérdida de cupón *Goodwill* durante el tiempo de interrupción material (de los sistemas, redes, etc.).

Se puede observar que las pólizas que hay hoy en día en el mercado son pólizas con un alcance amplio de cobertura, en su gran mayoría de coste de análisis y puesta en marcha tras una brecha.

Hay varias compañías que, a día de hoy, ofrecen este producto dentro de su portfolio y se espera que, conforme se vaya avanzando y se vayan produciendo más siniestros de este tipo, haya más compañías que se sumen.

El punto que está pendiente, como se puede desprender del análisis de cobertura que se ha realizado, es la parte de daños materiales por un ataque cibernético. Como se ha podido ver al inicio de la tesis, ya hay ejemplos reales de daños materiales derivados de una brecha en el sistema y, por lo tanto, es un tema que a día de hoy preocupa a las organizaciones y que no está bien resuelto. De momento, estos daños materiales deben ser retenidos por la organización ya que no dispone de medios para transferirlo al mercado asegurador.

### 5.1.5 Prima

Uno de los principales problemas con los que se encuentran estas compañías que comercializan el Ciberseguro es la prima actuarial que deberían tener. Dado que no hay masa de datos siniestros, los cálculos de frecuencia y coste medio se deben hacer a nivel muy teórico y por lo tanto, la prima resultante no siempre es la adecuada.

---

<sup>19</sup> *Cloud*: Hace referencia a la nueva tecnología de computación en la nube.

<sup>20</sup> Cupón *Goodwill*: Se trata de un cupón que ofrece un descuento o reembolso por una futura compra de productos o servicios.

Es por ello que en la contratación y en las renovaciones de la póliza, la prima puede ir variando mucho. De hecho, una póliza que sufre siniestralidad, seguramente verá su prima incrementada de manera importante pero, además, a pesar de no sufrir ningún siniestro durante el año de vigencia, puede ver la prima incrementada si en el mercado han surgido nuevos riesgos cibernéticos o si ha habido un número importante de ataques a empresas, ya que las compañías aseguradoras actualizarán todos sus cálculos al alza para hacer frente una posible eventualidad en alguna compañía asegurada.

Además, otro de los problemas con los que se encuentran las compañías comercializadoras actualmente es el control de los cúmulos. Es muy difícil controlar los cúmulos que se pueden llegar a tener ya que en un mismo ataque se pueden ver afectadas todas las pólizas de la cartera, lo que haría que el siniestro, considerado como cúmulo al ser un único evento, tuviese un coste inesperado y nada proporcionado a las primas que se habían estado cobrando hasta ese momento.

## 5.2. Previsión de futuro

Una vez se ha analizado la situación actual, tanto de los ciberataques como de la solución aseguradora, hay que intentar mirar hacia el futuro e intentar observar hacia dónde evoluciona.

### 5.2.1 De los ciberriesgos

La evolución de los ciberriesgos está siendo, en los últimos tiempos, una evolución vertiginosa. Expertos en el tema, indican que en los años venideros, seguirá siendo de la misma manera.

Cada vez que aparece un nuevo *ransomware*, lo hace con una mayor virulencia y mucho más “profesional” que el anterior. Además, a pesar de que en las organizaciones de protección ante ciberataques siempre se intenta actuar de forma proactiva, la realidad es que siempre se va un paso por detrás de los cibercriminales, debiendo actuar de forma reactiva.

Además, se benefician de la facilidad de efectuar estos ataques ya que, los pagos siempre se suelen exigir en *Bitcoins* y por lo tanto son casi imposibles de rastrear.

Ya se ha comentado en puntos anteriores pero la aparición del *IoT*, también va a hacer incrementar el número de ciberataques y las brechas de seguridad.

Por otro lado, en los próximos años también van a incrementar el número de ataques contra sistemas de control industrial y contra toda la nueva tecnología que va apareciendo. Unos ejemplos claros son tanto el *DronJacking* y el *Car-Hacking*, es decir, atacar directamente a vehículos o maquinaria autopropulsada, haciéndoles fallar alguno de sus sistemas vitales.

También tendrá impacto la evolución de la normativa legal. Por ejemplo, el año pasado se aprobó el Reglamento 2016/679 del Parlamento europeo y del Consejo de 27 de abril relativo a la protección de las personas físicas, derogando la Directiva 95/46/CE. Este reglamento no comenzará a aplicarse hasta el 25 de mayo de 2018 pero, una vez entre en vigor, tendrá un impacto muy elevado.

De esta directiva hay que destacar una de las principales novedades que introduce y es que, a partir de dicha fecha, será de obligación notificar las violaciones de seguridad de datos.

Esta modificación en el reglamento tendrá muchísimo impacto dada la reticencia actual de las empresas a reconocer públicamente sus brechas de seguridad, intentando evitar pérdidas de reputación.

Eso sí, a nivel de las compañías aseguradoras, será un punto a favor muy importante ya que permitirá obtener mucha información que actualmente no dispone y ayudará a saber a qué se enfrentan día a día las organizaciones, permitiendo protegerlas mejor.

## **5.2.2 De la solución aseguradora**

Tal y como se ha visto anteriormente, los daños propios es un asunto pendiente de este tipo de pólizas de seguro. Pero las preguntas sobre el futuro van dirigidas sobre cómo evolucionará esta póliza de seguro.

Una de las claves de la evolución será el comportamiento de las primas de las pólizas de ciberriesgos. Actualmente, las pólizas tienen un comportamiento inestable, pudiendo variar mucho de un año para otro. Además, a día de hoy, se puede considerar que tienen un precio elevado en comparación con el resto de seguros de daños materiales, donde ya se dispone de mucha más tradición aseguradora, teniendo más información siniestral y pudiendo afinar más en la prima correspondiente a la exposición real del riesgo.

Habrá que ver cómo, cuando se vaya teniendo más información técnica, evolucionan las primas; ver si se estabilizan a la baja.

Otra de las claves del aprendizaje será el cuantificar de una manera más fácil y rápida todas las pérdidas que, a día de hoy, requieren de un estudio muy completo y complejo, cuando se habla de pérdidas de reputación, pérdidas de beneficios o pérdidas de competitividad por robo de información confidencial.

También, viendo la evolución de la normativa, habrá que ver si se amplían las opciones de cobertura. Por ejemplo, con la nueva Directiva comentada anteriormente, las pólizas de ciberriesgos tienen la opción de hacerse cargo de dichos gastos, facilitando a las organizaciones la transferencia de este nuevo riesgo.

Por otro lado, también habrá que ver si, con el tiempo, se acaba incorporando la póliza de ciberriesgos dentro de las pólizas generalistas de Daños o de las de Responsabilidad Civil o incluso si la póliza contra los ciberataques acaba



siendo una póliza generalista en sí misma, en la cual se pueda incluir, además de todas las respuestas técnicas ante un ciberataque y los costes asociados, las averías a la propia maquinaria o equipos y las responsabilidades que puedan llegar a ser exigibles tanto a la organización como a los altos cargos por mala gestión.



## 6. Conclusiones

Una vez analizados todos los factores intervinientes y necesarios para la realización de este trabajo, se pueden extraer varias conclusiones claramente diferenciadas.

La primera es que realizar el proceso del *ERM* es básico, ya no solo a nivel de detección de riesgos cibernéticos sino a nivel global de la compañía, saber a qué riesgos se enfrenta una organización es clave para su supervivencia ya que les permite crear y mantener el valor.

El desarrollo de este proceso, que no es rápido, automático ni sencillo, ha de ir acompañado siempre de varios aspectos que ayuden a su correcta implantación, gestión y, sobretodo, actualización.

A la hora de su análisis e incorporación a la organización, se debe realizar con una visión de 360º, teniendo en cuenta a toda la empresa y haciéndola participe, para así poder cumplir con los principales principios de la ISO 31000 e implementar de forma adecuada toda la gestión de riesgos.

Una vez incorporado a la organización, es necesario tenerlo correctamente actualizado en todo momento. Esta permanente iteración del esquema del *ERM* ha de realizarse desde todos los puntos de la organización y, por lo tanto, unos directivos comprometidos y concienciados de la necesidad e importancia del *ERM* ayudará a que se alcance el objetivo buscado y a que se mantenga en el tiempo.

También será importante que, de manera interna, se asuma que el dinero utilizado para la seguridad no es un gasto, sino una inversión que ayudará a proteger y asegurar la continuidad de la organización.

Por otro lado, los ciberataques son unos riesgos en constante evolución y que se han de tener correctamente monitorizados para estar siempre alerta. A día de hoy, la frecuencia y severidad que pueden llegar a alcanzar estos riesgos, así como la evolución que tendrán, es completamente desconocido. En cualquier caso, lo que sí que parece claro es que no se va a mantener tal y como son actualmente sino que tenderá a incrementar tanto la frecuencia como el impacto económico que significará.

Además, ya no solo irán a peor los ataques que sufrirán las organizaciones sino que, con toda la nueva era tecnológica y todas las nuevas ventanas que se abren con el *IoT*, puede llegar a ser relativamente más fácil este acceso, siempre que la empresa no sea consciente de todos los peligros y no se proteja de forma adecuada. Cabe recordar que esta falta de protección puede ser de forma voluntaria, es decir, conociendo que hay un riesgo y sin protegerse de él o de forma involuntaria, es decir, que la organización puede ser desconocedora de la exposición que se está teniendo.

Se ha comentado que los accesos pueden llegar a ser más fáciles, pero también pueden llegar a ser de más importancia en tanto en cuanto las organizaciones cada vez almacenan más información de todos sus proveedores y clientes. Este incremento en el aumento de datos, sumado al incremento de la severidad de la Ley, que cada vez se está enfocando a la necesidad de proteger de forma correcta todos los datos, sobre todo si son sensibles, hará que los costes asociados a un ciberataque vayan incrementando de forma sustancial.

Por todo ello, los ciberriesgos han afectado (o deberían haber ya afectado) a todas las organizaciones. Quizás no en el sentido de haber sufrido un ciberataque pero sí en el sentido de haber hecho modificaciones en el esquema del *ERM*. Hace unos años, los riesgos asociados a la tecnología básicamente estaban relacionados con la rotura de un equipo tecnológico clave o de la pérdida de datos o licencias de *software*, que hiciesen que se tuviese que interrumpir el negocio por un tiempo, hasta conseguir reponer el equipo o *software* dañado. Estos peligros han evolucionado hasta la actualidad, pudiendo suponer el cierre de una organización que no lo tuviese contemplado, debido a los costes que podría llegar a tener que soportar tras un ataque.

Hoy en día, como se ha visto, las pólizas de ciberriesgos permiten transferir los costes relacionados con las paralizaciones y gestión de la crisis (servicios legales, informática forense, etc.). Por lo tanto, otro de los puntos sensibles y que se deberá ver cómo evoluciona es el relacionado con los daños a los propios equipo tras un ciberataque ya que a día de hoy se han visto ejemplos reales donde se han sufrido este tipo de daños y que, probablemente, en el futuro se puedan ver con más facilidad y asiduidad.

Esta evolución la marcarán, principalmente, las compañías aseguradoras, que deberán analizar si es sostenible, dentro de unas primas más o menos lógicas y asumibles para las organizaciones, dar esta cobertura. Mientras tanto, las empresas deben ser conscientes de que pueden sufrir este tipo de daños propios en su maquinaria y que es un daño que deberán retener a no ser que dispongan de otro método de transferencia del riesgo que no sea la propia compañía aseguradora.

Con todo lo comentado, se puede concluir que efectivamente los ciberriesgos han provocado una evolución en la gestión de la Gerencia de Riesgos. Si hay alguna organización que aún no ha procedido, debería hacerlo con la mayor celeridad posible dado que puede llegar a tener un impacto muy severo en la cuenta de resultados si no se trata correctamente o incluso si no se es conocedor del coste que puede llegar a tener un ataque de este tipo.

## 7. Bibliografía

### Artículos:

MONRÀS VIDIELLA, Xavier. La Gerencia de Riesgos y la gestión técnica de Grandes Riesgos Industriales. Barcelona. 2017.

FRETTLOEHR, Oliver. Riesgos cibernéticos. Múnich. 2016

PÉREZ VILA, Fernando. Gerencia de riesgos (definiciones, objetivos y procesos). Múnich. 2016

### Informes:

FERMA. A Risk Management Standard. Bruselas. 2003.

CCN-CERT. Ciberamenazas y Tendencias. Madrid. 2017.

Swiss Re Institute. Cibernética: cómo enfrentarse a un riesgo complejo. Zúrich. 2017.

Hiscox. DNA of an Entrepreneur - Small businesses in numbers. Londres. 2016.

Fundación Mapfre. Gerencia de Riesgos y Seguros. Madrid. 2012.

Fundación Mapfre. Guía para la protección de la pequeña empresa. Madrid. 2015.

World Economic Forum (WEF). The Global Risks Report. Ginebra. 2016.

World Economic Forum (WEF). The Global Risks Report. Ginebra. 2017.

McAfee. Net Losses: Estimating the Global Cost of Cybercrime. California. 2014.

Ponemon Institute. Study on Mobile and Internet of Things Application Security. Michigan. 2017.

Ponemon Institute. Cost of Data Breach Study: Global Analysis. Michigan. 2016.

Deloitte. Beneath the surface of a cyberattack. Nueva York. 2016.

Allianz. Allianz Risk Barometer. Múnich. 2017.

Allianz. Allianz Risk Barometer. Múnich. 2016.

Allianz. Allianz Risk Barometer. Múnich. 2015.

## Fuentes de internet:

FERMA.

<<http://www.ferma.eu/>>

(Fecha de consulta: abril 2017).

Instituto Nacional de Ciberseguridad (INCIBE).

<<https://www.incibe.es/>>

(Fecha de consulta: mayo 2017).

Centro Criptológico Nacional (CCN-CERTA).

<<https://www.ccn-cert.cni.es/>>

(Fecha de consulta: mayo 2017).

Real Academia Española de la lengua (RAE).

<<http://www.rae.es/>>

(Fecha de consulta: mayo 2017).

DELOITTE. Los riesgos ocultos de un ciberataque. 2016.

<<https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/los-riesgos-ocultos-de-un-ciberataque.html>>

(Fecha de consulta: mayo 2017).

PERASSO, Valeria. Qué es la cuarta revolución industrial (y por qué debería preocuparnos). 2016. <<http://www.bbc.com/mundo/noticias-37631834>>

(Fecha de consulta: junio 2017).

CONSTANTINI, Luca. Los robots, la cuarta revolución industrial. 2016.

<[http://economia.elpais.com/economia/2016/02/05/actualidad/1454685123\\_400320.html](http://economia.elpais.com/economia/2016/02/05/actualidad/1454685123_400320.html)>

(Fecha de consulta: junio 2017).

WORLD ECONOMIC FORUM.

<<https://www.weforum.org/>>

(Fecha de consulta: mayo 2017).

SIEMENS.

<<https://www.siemens.com/innovation/en/home/pictures-of-the-future/archive.html>>

(Fecha de consulta: junio 2017).

BARRANCO, Ricardo. IBM. ¿Qué es Big Data)

<<https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/>>

(fecha de consulta: junio 2017).

### **Fuentes Oficiales:**

REGLAMENTO 2016/679 del Parlamento europeo y del Consejo de 27 de abril relativo a la protección de las personas físicas.

UNE-ISO 73:2010. Gestión del riesgo. Vocabulario.

UNE-ISO 51:2014. Aspectos de seguridad. Guías para su inclusión en estándares.

UNE-ISO 31000:2010. Gestión del riesgo. Principios y directrices.

UNE ISO 31010:2011. Gestión del riesgo. Técnicas de apreciación del riesgo.

ISO-IEC 27001:2013. Gestión de la Seguridad de la Información (SGSI).

### **Webinar:**

FUNDACIÓN MAPFRE (Abel Linares -CEO Nunkyworld-, María Díaz-Lladó -Directora General de JLT March Re- e Iratxe San Pedro -Subdirectora Área Responsabilidad Civil MAPFRE-). Los ciberriesgos y su transferencia al mercado asegurador. Madrid. 2017.

### **Entrevista:**

Realizada entrevista con Carmen Segovia, Directora de Líneas Financieras Cataluña y Baleares de Aon Risk Solutions y una de las personas con mayor conocimiento de los ciberataques y del mundo asegurador alrededor de dichos ataques.





## **Sergio López Serrano**

Nacido en Barcelona, el 28 de mayo de 1989.

A nivel académico, licenciado en Ingeniería Industrial Superior, especializado en Organización Industrial, por la Universidad Politécnica de Catalunya; realizando parte de los estudios en la Politécnico di Torino.

A nivel profesional, desarrollando su carrera dentro de la compañía Seguros Catalana Occidente desde 2013, estando bajo su responsabilidad el producto Multirriesgos Pyme, después de haber pasado por varios departamentos como Suscripción de Particulares o Siniestros Especiales de Particulares.



**COLECCIÓN “CUADERNOS DE DIRECCIÓN ASEGURADORA”**  
Máster en Dirección de Entidades Aseguradoras y Financieras  
Facultad de Economía y Empresa. Universidad de Barcelona

**PUBLICACIONES**

- 1.- Francisco Abián Rodríguez: “Modelo Global de un Servicio de Prestaciones Vida y su interrelación con Suscripción” 2005/2006
- 2.- Erika Johanna Aguilar Olaya: “Gobierno Corporativo en las Mutualidades de Seguros” 2005/2006
- 3.- Alex Aguyé Casademunt: “La Entidad Multicanal. Elementos clave para la implantación de la Estrategia Multicanal en una entidad aseguradora” 2009/2010
- 4.- José María Alonso-Rodríguez Piedra: “Creación de una plataforma de servicios de siniestros orientada al cliente” 2007/2008
- 5.- Jorge Alvez Jiménez: “innovación y excelencia en retención de clientes” 2009/2010
- 6.- Anna Aragonés Palom: “El Cuadro de Mando Integral en el Entorno de los seguros Multirriesgo” 2008/2009
- 7.- Maribel Avila Ostos: “La tele-suscripción de Riesgos en los Seguros de Vida” 2009/2010
- 8.- Mercé Bascompte Riquelme: “El Seguro de Hogar en España. Análisis y tendencias” 2005/2006
- 9.- Aurelio Beltrán Cortés: “Bancaseguros. Canal Estratégico de crecimiento del sector asegurador” 2010/2011
- 10.- Manuel Blanco Alpuente: “Delimitación temporal de cobertura en el seguro de responsabilidad civil. Las cláusulas claims made” 2008/2009
- 11.- Eduard Blanxart Raventós: “El Gobierno Corporativo y el Seguro D & O” 2004/2005
- 12.- Rubén Bouso López: “El Sector Industrial en España y su respuesta aseguradora: el Multirriesgo Industrial. Protección de la empresa frente a las grandes pérdidas patrimoniales” 2006/2007
- 13.- Kevin van den Boom: “El Mercado Reasegurador (Cedentes, Brokers y Reaseguradores). Nuevas Tendencias y Retos Futuros” 2008/2009
- 14.- Laia Bruno Sazatornil: “L'ètica i la rentabilitat en les companyies asseguradores. Proposta de codi deontològic” 2004/2005
- 15.- María Dolores Caldes Llopis: “Centro Integral de Operaciones Vida” 2007/2008
- 16.- Adolfo Calvo Llorca: “Instrumentos legales para el recobro en el marco del seguro de crédito” 2010/2011
- 17.- Ferran Camprubí Baiges: “La gestión de las inversiones en las entidades aseguradoras. Selección de inversiones” 2010/2011
- 18.- Joan Antoni Carbonell Aregall: “La Gestió Internacional de Sinistres d'Automòbil amb Resultat de Danys Materials” 2003-2004
- 19.- Susana Carmona Llevadot: “Viabilidad de la creación de un sistema de Obra Social en una entidad aseguradora” 2007/2008
- 20.- Sergi Casas del Alcazar: “El PLAN de Contingencias en la Empresa de Seguros” 2010/2011
- 21.- Francisco Javier Cortés Martínez: “Análisis Global del Seguro de Decesos” 2003-2004
- 22.- María Carmen Ceña Nogué: “El Seguro de Comunidades y su Gestión” 2009/2010
- 23.- Jordi Cots Paltor: “Control Interno. El auto-control en los Centros de Siniestros de Automóviles” 2007/2008
- 24.- Montserrat Cunillé Salgado: “Los riesgos operacionales en las Entidades Aseguradoras” 2003-2004
- 25.- Ricard Doménech Pagés: “La realidad 2.0. La percepción del cliente, más importante que nunca” 2010/2011
- 26.- Luis Domínguez Martínez: “Formas alternativas para la Cobertura de Riesgos” 2003-2004
- 27.- Marta Escudero Cutal: “Solvencia II. Aplicación práctica en una entidad de Vida” 2007/2008
- 28.- Salvador Esteve Casablancas: “La Dirección de Reaseguro. Manual de Reaseguro” 2005/2006

- 29.- Alvaro de Falguera Gaminde: "Plan Estratégico de una Correduría de Seguros Náuticos" 2004/2005
- 30.- Isabel M<sup>a</sup> Fernández García: "Nuevos aires para las Rentas Vitalicias" 2006/2007
- 31.- Eduard Fillet Catarina: "Contratación y Gestión de un Programa Internacional de Seguros" 2009/2010
- 32.- Pablo Follana Murcia: "Métodos de Valoración de una Compañía de Seguros. Modelos Financieros de Proyección y Valoración consistentes" 2004/2005
- 33.- Juan Fuentes Jassé: "El fraude en el seguro del Automóvil" 2007/2008
- 34.- Xavier Gabarró Navarro: ""El Seguro de Protección Jurídica. Una oportunidad de Negocio"" 2009/2010
- 35.- Josep María Galcerá Gombau: "La Responsabilidad Civil del Automóvil y el Daño Corporal. La gestión de siniestros. Adaptación a los cambios legislativos y propuestas de futuro" 2003-2004
- 36.- Luisa García Martínez: "El Carácter tuitivo de la LCS y los sistemas de Defensa del Asegurado. Perspectiva de un Operador de Banca Seguros" 2006/2007
- 37.- Fernando García Giralt: "Control de Gestión en las Entidades Aseguradoras" 2006/2007
- 38.- Jordi García-Muret Ubis: "Dirección de la Sucursal. D. A. F. O." 2006/2007
- 39.- David Giménez Rodríguez: "El seguro de Crédito: Evolución y sus Canales de Distribución" 2008/2009
- 40.- Juan Antonio González Arriete: "Línea de Descuento Asegurada" 2007/2008
- 41.- Miquel Gotés Grau: "Assegurances Agràries a BancaSeguros. Potencial i Sistema de Comercialització" 2010/2011
- 42.- Jesús Gracia León: "Los Centros de Siniestros de Seguros Generales. De Centros Operativos a Centros Resolutivos. De la optimización de recursos a la calidad de servicio" 2006/2007
- 43.- José Antonio Guerra Díez: "Creación de unas Tablas de Mortalidad Dinámicas" 2007/2008
- 44.- Santiago Guerrero Caballero: "La politización de las pensiones en España" 2010/2011
- 45.- Francisco J. Herencia Conde: "El Seguro de Dependencia. Estudio comparativo a nivel internacional y posibilidades de desarrollo en España" 2006/2007
- 46.- Francisco Javier Herrera Ruiz: "Selección de riesgos en el seguro de Salud" 2009/2010
- 47.- Alicia Hoya Hernández: "Impacto del cambio climático en el reaseguro" 2008/2009
- 48.- Jordi Jiménez Baena: "Creación de una Red de Agentes Exclusivos" 2007/2008
- 49.- Oriol Jorba Cartoixà: "La oportunidad aseguradora en el sector de las energías renovables" 2008/2009
- 50.- Anna Juncá Puig: "Una nueva metodología de fidelización en el sector asegurador" 2003/2004
- 51.- Ignacio Lacalle Goría: "El artículo 38 Ley Contrato de Seguro en la Gestión de Siniestros. El procedimiento de peritos" 2004/2005
- 52.- M<sup>a</sup> Carmen Lara Ortíz: "Solvencia II. Riesgo de ALM en Vida" 2003/2004
- 53.- Haydée Noemí Lara Téllez: "El nuevo sistema de Pensiones en México" 2004/2005
- 54.- Marta Leiva Costa: "La reforma de pensiones públicas y el impacto que esta modificación supone en la previsión social" 2010/2011
- 55.- Victoria León Rodríguez: "Problemàtica del aseguramiento de los Jóvenes en la política comercial de las aseguradoras" 2010/2011
- 56.- Pilar Lindín Soriano: "Gestión eficiente de pólizas colectivas de vida" 2003/2004
- 57.- Victor Lombardero Guarnier: "La Dirección Económico Financiera en el Sector Asegurador" 2010/2011
- 58.- Maite López Aladros: "Análisis de los Comercios en España. Composición, Evolución y Oportunidades de negocio para el mercado asegurador" 2008/2009
- 59.- Josep March Arranz: "Los Riesgos Personales de Autónomos y Trabajadores por cuenta propia. Una visión de la oferta aseguradora" 2005/2006
- 60.- Miquel Maresch Camprubí: "Necesidades de organización en las estructuras de distribución por mediadores" 2010/2011
- 61.- José Luis Marín de Alcaraz: "El seguro de impago de alquiler de viviendas" 2007/2008

- 62.- Miguel Ángel Martínez Boix: "Creatividad, innovación y tecnología en la empresa de seguros" 2005/2006
- 63.- Susana Martínez Corveira: "Propuesta de Reforma del Baremo de Autos" 2009/2010
- 64.- Inmaculada Martínez Lozano: "La Tributación en el mundo del seguro" 2008/2009
- 65.- Dolors Melero Montero: "Distribución en bancaseguros: Actuación en productos de empresas y gerencia de riesgos" 2008/2009
- 66.- Josep Mena Font: "La Internalización de la Empresa Española" 2009/2010
- 67.- Angela Milla Molina: "La Gestión de la Previsión Social Complementaria en las Compañías de Seguros. Hacia un nuevo modelo de Gestión" 2004/2005
- 68.- Montserrat Montull Rossón: "Control de entidades aseguradoras" 2004/2005
- 69.- Eugenio Morales González: "Oferta de licuación de patrimonio inmobiliario en España" 2007/2008
- 70.- Lluís Morales Navarro: "Plan de Marketing. División de Bancaseguros" 2003/2004
- 71.- Sonia Moya Fernández: "Creación de un seguro de vida. El éxito de su diseño" 2006/2007
- 72.- Rocio Moya Morón: "Creación y desarrollo de nuevos Modelos de Facturación Electrónica en el Seguro de Salud y ampliación de los modelos existentes" 2008/2009
- 73.- María Eugenia Mugerza Goya: "Bancaseguros. La comercialización de Productos de Seguros No Vida a través de redes bancarias" 2005/2006
- 74.- Ana Isabel Mullor Cabo: "Impacto del Envejecimiento en el Seguro" 2003/2004
- 75.- Estefanía Nicolás Ramos: "Programas Multinacionales de Seguros" 2003/2004
- 76.- Santiago de la Nogal Mesa: "Control interno en las Entidades Aseguradoras" 2005/2006
- 77.- Antonio Nolasco Gutiérrez: "Venta Cruzada. Mediación de Seguros de Riesgo en la Entidad Financiera" 2006/2007
- 78.- Francesc Ocaña Herrera: "Bonus-Malus en seguros de asistencia sanitaria" 2006/2007
- 79.- Antonio Olmos Francino: "El Cuadro de Mando Integral: Perspectiva Presente y Futura" 2004/2005
- 80.- Luis Palacios García: "El Contrato de Prestación de Servicios Logísticos y la Gerencia de Riesgos en Operadores Logísticos" 2004/2005
- 81.- Jaume Paris Martínez: "Segmento Discapacitados. Una oportunidad de Negocio" 2009/2010
- 82.- Martín Pascual San Martín: "El incremento de la Longevidad y sus efectos colaterales" 2004/2005
- 83.- Montserrat Pascual Villacampa: "Proceso de Tarificación en el Seguro del Automóvil. Una perspectiva técnica" 2005/2006
- 84.- Marco Antonio Payo Aguirre: "La Gerencia de Riesgos. Las Compañías Cautivas como alternativa y tendencia en el Risk Management" 2006/2007
- 85.- Patricia Pérez Julián: "Impacto de las nuevas tecnologías en el sector asegurador" 2008/2009
- 86.- María Felicidad Pérez Soro: "La atención telefónica como transmisora de imagen" 2009/2010
- 87.- Marco José Piccirillo: "Ley de Ordenación de la Edificación y Seguro. Garantía Decenal de Daños" 2006/2007
- 88.- Irene Plana Güell: "Sistemas d'Informació Geogràfica en el Sector Assegurador" 2010/2011
- 89.- Sonia Plaza López: "La Ley 15/1999 de Protección de Datos de carácter personal" 2003/2004
- 90.- Pere Pons Pena: "Identificación de Oportunidades comerciales en la Provincia de Tarragona" 2007/2008
- 91.- María Luisa Postigo Díaz: "La Responsabilidad Civil Empresarial por accidentes del trabajo. La Prevención de Riesgos Laborales, una asignatura pendiente" 2006/2007
- 92.- Jordi Pozo Tamarit: "Gerencia de Riesgos de Terminales Marítimas" 2003/2004
- 93.- Francesc Pujol Niñerola: "La Gerencia de Riesgos en los grupos multisectoriales" 2003-2004
- 94.- M<sup>a</sup> del Carmen Puyol Rodríguez: "Recursos Humanos. Breve mirada en el sector de Seguros" 2003/2004

- 95.- Antonio Miguel Reina Vidal: "Sistema de Control Interno, Compañía de Vida. Bancaseguros" 2006/2007
- 96.- Marta Rodríguez Carreiras: "Internet en el Sector Asegurador" 2003/2004
- 97.- Juan Carlos Rodríguez García: "Seguro de Asistencia Sanitaria. Análisis del proceso de tramitación de Actos Médicos" 2004/2005
- 98.- Mónica Rodríguez Nogueiras: "La Cobertura de Riesgos Catastróficos en el Mundo y soluciones alternativas en el sector asegurador" 2005/2006
- 99.- Susana Roquet Palma: "Fusiones y Adquisiciones. La integración y su impacto cultural" 2008/2009
- 100.- Santiago Rovira Obradors: "El Servei d'Assegurances. Identificació de les variables clau" 2007/2008
- 101.- Carlos Ruano Espí: "Microseguro. Una oportunidad para todos" 2008/2009
- 102.- Mireia Rubio Cantisano: "El Comercio Electrónico en el sector asegurador" 2009/2010
- 103.- María Elena Ruíz Rodríguez: "Análisis del sistema español de Pensiones. Evolución hacia un modelo europeo de Pensiones único y viabilidad del mismo" 2005/2006
- 104.- Eduardo Ruiz-Cuevas García: "Fases y etapas en el desarrollo de un nuevo producto. El Taller de Productos" 2006/2007
- 105.- Pablo Martín Sáenz de la Pascua: "Solvencia II y Modelos de Solvencia en Latinoamérica. Sistemas de Seguros de Chile, México y Perú" 2005/2006
- 106.- Carlos Sala Farré: "Distribución de seguros. Pasado, presente y tendencias de futuro" 2008/2009
- 107.- Ana Isabel Salguero Matarín: "Quién es quién en el mundo del Plan de Pensiones de Empleo en España" 2006/2007
- 108.- Jorge Sánchez García: "El Riesgo Operacional en los Procesos de Fusión y Adquisición de Entidades Aseguradoras" 2006/2007
- 109.- María Angels Serral Floreta: "El lucro cesante derivado de los daños personales en un accidente de circulación" 2010/2011
- 110.- David Serrano Solano: "Metodología para planificar acciones comerciales mediante el análisis de su impacto en los resultados de una compañía aseguradora de No Vida" 2003/2004
- 111.- Jaume Siberta Durán: "Calidad. Obtención de la Normativa ISO 9000 en un centro de Atención Telefónica" 2003/2004
- 112.- María Jesús Suárez González: "Los Poolings Multinacionales" 2005/2006
- 113.- Miguel Torres Juan: "Los siniestros IBNR y el Seguro de Responsabilidad Civil" 2004/2005
- 114.- Carlos Travé Babiano: "Provisiones Técnicas en Solvencia II. Valoración de las provisiones de siniestros" 2010/2011
- 115.- Rosa Viciano García: "Banca-Seguros. Evolución, regulación y nuevos retos" 2007/2008
- 116.- Ramón Vidal Escobosa: "El baremo de Daños Personales en el Seguro de Automóviles" 2009/2010
- 117.- Tomás Wong-Kit Ching: "Análisis del Reaseguro como mitigador del capital de riesgo" 2008/2009
- 118.- Yibo Xiong: "Estudio del mercado chino de Seguros: La actualidad y la tendencia" 2005/2006
- 119.- Beatriz Bernal Callizo: "Póliza de Servicios Asistenciales" 2003/2004
- 120.- Marta Bové Badell: "Estudio comparativo de evaluación del Riesgo de Incendio en la Industria Química" 2003/2004
- 121.- Ernest Castellón Teixidó: "La edificación. Fases del proceso, riesgos y seguros" 2004/2005
- 122.- Sandra Clusella Giménez: "Gestió d'Actius i Passius. Inmunització Financera" 2004/2005
- 123.- Miquel Crespí Argemí: "El Seguro de Todo Riesgo Construcción" 2005/2006
- 124.- Yolanda Dengra Martínez: "Modelos para la oferta de seguros de Hogar en una Caja de Ahorros" 2007/2008
- 125.- Marta Fernández Ayala: "El futuro del Seguro. Bancaseguros" 2003/2004
- 126.- Antonio Galí Isus: "Inclusión de las Energías Renovables en el sistema Eléctrico Español" 2009/2010
- 127.- Gloria Gorbea Bretones: "El control interno en una entidad aseguradora" 2006/2007

- 128.- Marta Jiménez Rubio: "El procedimiento de tramitación de siniestros de daños materiales de automóvil: análisis, ventajas y desventajas" 2008/2009
- 129.- Lorena Alejandra Libson: "Protección de las víctimas de los accidentes de circulación. Comparación entre el sistema español y el argentino" 2003/2004
- 130.- Mario Manzano Gómez: "La responsabilidad civil por productos defectuosos. Solución aseguradora" 2005/2006
- 131.- Àlvar Martín Botí: "El Ahorro Previsión en España y Europa. Retos y Oportunidades de Futuro" 2006/2007
- 132.- Sergio Martínez Olivé: "Construcción de un modelo de previsión de resultados en una Entidad Aseguradora de Seguros No Vida" 2003/2004
- 133.- Pilar Miracle Vázquez: "Alternativas de implementación de un Departamento de Gestión Global del Riesgo. Aplicado a empresas industriales de mediana dimensión" 2003/2004
- 134.- María José Morales Muñoz: "La Gestión de los Servicios de Asistencia en los Multirriesgo de Hogar" 2007/2008
- 135.- Juan Luis Moreno Pedroso: "El Seguro de Caución. Situación actual y perspectivas" 2003/2004
- 136.- Rosario Isabel Pastrana Gutiérrez: "Creació d'una empresa de serveis socials d'atenció a la dependència de les persones grans enfocada a productes d'assegurances" 2007/2008
- 137.- Joan Prat Rifà: "La Previsió Social Complementaria a l'Empresa" 2003/2004
- 138.- Alberto Sanz Moreno: "Beneficios del Seguro de Protección de Pagos" 2004/2005
- 139.- Judith Safont González: "Efectes de la contaminació i del estils de vida sobre les assegurances de salut i vida" 2009/2010
- 140.- Carles Soldevila Mejías: "Models de gestió en companyies d'assegurances. Outsourcing / Insourcing" 2005/2006
- 141.- Olga Torrente Pascual: "IFRS-19 Retribuciones post-empleo" 2003/2004
- 142.- Annabel Roig Navarro: "La importancia de las mutualidades de previsión social como complementarias al sistema público" 2009/2010
- 143.- José Angel Ansón Tortosa: "Gerencia de Riesgos en la Empresa española" 2011/2012
- 144.- María Mercedes Bernués Burillo: "El permiso por puntos y su solución aseguradora" 2011/2012
- 145.- Sònia Beulas Boix: "Prevención del blanqueo de capitales en el seguro de vida" 2011/2012
- 146.- Ana Borràs Pons: "Teletrabajo y Recursos Humanos en el sector Asegurador" 2011/2012
- 147.- María Asunción Cabezas Bono: "La gestión del cliente en el sector de bancaseguros" 2011/2012
- 148.- María Carrasco Mora: "Matching Premium. New approach to calculate technical provisions Life insurance companies" 2011/2012
- 149.- Eduard Huguet Palouzie: "Las redes sociales en el Sector Asegurador. Plan social-media. El Community Manager" 2011/2012
- 150.- Laura Monedero Ramírez: "Tratamiento del Riesgo Operacional en los 3 pilares de Solvencia II" 2011/2012
- 151.- Salvador Obregón Gomá: "La Gestión de Intangibles en la Empresa de Seguros" 2011/2012
- 152.- Elisabet Ordóñez Somolinos: "El sistema de control Interno de la Información Financiera en las Entidades Cotizadas" 2011/2012
- 153.- Gemma Ortega Vidal: "La Mediación. Técnica de resolución de conflictos aplicada al Sector Asegurador" 2011/2012
- 154.- Miguel Ángel Pino García: "Seguro de Crédito: Implantación en una aseguradora multirramo" 2011/2012
- 155.- Genevieve Thibault: "The Customer Experience as a Source of Competitive Advantage" 2011/2012
- 156.- Francesc Vidal Bueno: "La Mediación como método alternativo de gestión de conflictos y su aplicación en el ámbito asegurador" 2011/2012
- 157.- Mireia Arenas López: "El Fraude en los Seguros de Asistencia. Asistencia en Carretera, Viaje y Multirriesgo" 2012/2013

- 158.- Lluís Fernández Rabat: "El proyecto de contratos de Seguro-IFRS4. Expectativas y realidades" 2012/2013
- 159.- Josep Ferrer Arilla: "El seguro de decesos. Presente y tendencias de futuro" 2012/2013
- 160.- Alicia García Rodríguez: "El Cuadro de Mando Integral en el Ramo de Defensa Jurídica" 2012/2013
- 161.- David Jarque Solsona: "Nuevos sistemas de suscripción en el negocio de vida. Aplicación en el canal bancaseguros" 2012/2013
- 162.- Kamal Mustafá Gondolbeu: "Estrategias de Expansión en el Sector Asegurador. Matriz de Madurez del Mercado de Seguros Mundial" 2012/2013
- 163.- Jordi Núñez García: "Redes Periciales. Eficacia de la Red y Calidad en el Servicio" 2012/2013
- 164.- Paula Núñez García: "Benchmarking de Autoevaluación del Control en un Centro de Sinistros Diversos" 2012/2013
- 165.- Cristina Riera Asensio: "Agregadores. Nuevo modelo de negocio en el Sector Asegurador" 2012/2013
- 166.- Joan Carles Simón Robles: "Responsabilidad Social Empresarial. Propuesta para el canal de agentes y agencias de una compañía de seguros generalista" 2012/2013
- 167.- Marc Vilardebó Miró: "La política de inversión de las compañías aseguradoras ¿Influirá Solvencia II en la toma de decisiones?" 2012/2013
- 168.- Josep María Bertrán Aranés: "Segmentación de la oferta aseguradora para el sector agrícola en la provincia de Lleida" 2013/2014
- 169.- María Buendía Pérez: "Estrategia: Formulación, implementación, valoración y control" 2013/2014
- 170.- Gabriella Fernández Andrade: "Oportunidades de mejora en el mercado de seguros de Panamá" 2013/2014
- 171.- Alejandro Galcerán Rosal: "El Plan Estratégico de la Mediación: cómo una Entidad Aseguradora puede ayudar a un Mediador a implementar el PEM" 2013/2014
- 172.- Raquel Gómez Fernández: "La Previsión Social Complementaria: una apuesta de futuro" 2013/2014
- 173.- Xoan Jovaní Guiral: "Combinaciones de negocios en entidades aseguradoras: una aproximación práctica" 2013/2014
- 174.- Àlex Lansac Font: "Visión 360 de cliente: desarrollo, gestión y fidelización" 2013/2014
- 175.- Albert Llambrich Moreno: "Distribución: Evolución y retos de futuro: la evolución tecnológica" 2013/2014
- 176.- Montserrat Pastor Ventura: "Gestión de la Red de Mediadores en una Entidad Aseguradora. Presente y futuro de los agentes exclusivos" 2013/2014
- 177.- Javier Portalés Pau: "El impacto de Solvencia II en el área de TI" 2013/2014
- 178.- Jesús Rey Pulido: "El Seguro de Impago de Alquileres: Nuevas Tendencias" 2013/2014
- 179.- Anna Solé Serra: "Del cliente satisfecho al cliente entusiasmado. La experiencia cliente en los seguros de vida" 2013/2014
- 180.- Eva Tejedor Escorihuela: "Implantación de un Programa Internacional de Seguro por una compañía española sin sucursales o filiales propias en el extranjero. Caso práctico: Seguro de Daños Materiales y RC" 2013/2014
- 181.- Vanesa Cid Pijuan: "Los seguros de empresa. La diferenciación de la mediación tradicional" 2014/2015.
- 182.- Daniel Ciprés Tiscar: "¿Por qué no arranca el Seguro de Dependencia en España?" 2014/2015.
- 183.- Pedro Antonio Escalona Cano: "La estafa de Seguro. Creación de un Departamento de Fraude en una entidad aseguradora" 2014/2015.
- 184.- Eduard Escardó Lleixà: "Análisis actual y enfoque estratégico comercial de la Bancaseguros respecto a la Mediación tradicional" 2014/2015.
- 185.- Marc Esteve Grau: "Introducción del Ciber Riesgo en el Mundo Asegurador" 2014/2015.
- 186.- Paula Fernández Díaz: "La Innovación en las Entidades Aseguradoras" 2014/2015.
- 187.- Alex Lleyda Capell: "Proceso de transformación de una compañía aseguradora enfocada a producto, para orientarse al cliente" 2014/2015.



- 188.- Oriol Petit Salas: "Creación de Correduría de Seguros y Reaseguros S.L. Gestión Integral de Seguros" 2014/2015.
- 189.- David Ramos Pastor: "Big Data en sectores Asegurador y Financiero" 2014/2015.
- 190.- Marta Raso Cardona: "Comoditización de los seguros de Autos y Hogar. Diferenciación, fidelización y ahorro a través de la prestación de servicios" 2014/2015.
- 191.- David Ruiz Carrillo: "Información de clientes como elemento estratégico de un modelo asegurador. Estrategias de Marketing Relacional/CRM/Big Data aplicadas al desarrollo de un modelo de Bancaseguros" 2014/2015.
- 192.- Maria Torrent Caldas: "Ahorro y planificación financiera en relación al segmento de jóvenes" 2014/2015.
- 193.- Cristian Torres Ruiz: "El seguro de renta vitalicia. Ventajas e inconvenientes" 2014/2015.
- 194.- Juan José Trani Moreno: "La comunicación interna. Una herramienta al servicio de las organizaciones" 2014/2015.
- 195.- Alberto Yebra Yebra: "El seguro, producto refugio de las entidades de crédito en épocas de crisis" 2014/2015.
- 196.- Jesús García Riera: "Aplicación de la Psicología a la Empresa Aseguradora" 2015/2016
- 197.- Pilar Martínez Beguería: "La Función de Auditoría Interna en Solvencia II" 2015/2016
- 198.- Ingrid Nicolás Fargas: "El Contrato de Seguro y su evolución hasta la Ley 20/2015 LOSSEAR. Hacia una regulación más proteccionista del asegurado" 2015/2016
- 199.- María José Páez Reigosa: "Hacia un nuevo modelo de gestión de siniestros en el ramo de Defensa Jurídica" 2015/2016
- 200.- Sara Melissa Pinilla Vega: "Auditoría de Marca para el Grupo Integra Seguros Limitada" 2015/2016
- 201.- Teresa Repollés Llecha: "Optimización del ahorro a través de soluciones integrales. ¿cómo puede la empresa ayudar a sus empleados?" 2015/2016
- 202.- Daniel Rubio de la Torre: "Telematics y el seguro del automóvil. Una nueva póliza basada en los servicios" 2015/2016
- 203.- Marc Tarragó Diego: "Transformación Digital. Evolución de los modelos de negocio en las compañías tradicionales" 2015/2016
- 204.- Marc Torrents Fábregas: "Hacia un modelo asegurador peer-to-peer. ¿El modelo asegurador del futuro?" 2015/2016
- 205.- Inmaculada Vallverdú Coll: "Fórmulas modernas del Seguro de Crédito para el apoyo a la empresa: el caso español" 2015/2016
- 206.- Cristina Alberch Barrio: "Seguro de Crédito. Gestión y principales indicadores" 2016/2017
- 207.- Ian Bachs Millet: "Estrategias de expansión geográfica de una entidad aseguradora para un mercado específico" 2016/2017
- 208.- Marta Campos Comas: "Externalización del servicio de asistencia" 2016/2017
- 209.- Jordi Casas Pons: "Compromisos por pensiones. Hacia un nuevo modelo de negociación colectiva" 2016/2017
- 210.- Ignacio Domenech Guillén: "El seguro del automóvil para vehículos sostenibles, autónomos y conectados" 2016/2017
- 211.- María Luisa Fernández Gómez: "Adquisiciones de Carteras de Seguros y Planes de Pensiones" 2016/2017
- 212.- Diana Heman Hasbach: "¿Podrán los Millennials cobrar pensión?: una aplicación al caso de México" 2016/2017
- 213.- Sergio López Serrano: "El impacto de los Ciberriesgos en la Gerencia de Riesgos Tradicional" 2016/2017
- 214.- Jordi Martí Bernaus: "Dolencias preexistentes en el seguro de Salud: exclusiones o sobreprimas" 2016/2017
- 215.- Jéssica Martínez Ordóñez: "Derecho al honor de las personas jurídicas y reputación online" 2016/2017
- 216.- Raúl Monjo Zapata: "La Función de Cumplimiento en las Entidades Aseguradoras" 2016/2017

- 217.- Francisco José Muñoz Guerrero: "Adaptación de los Productos de Previsión al Ciclo de Vida" 2016/2017
- 218.- Mireia Orenes Esteban: "Crear valor mediante la gestión de siniestros de vida" 2016/2017
- 219.- Oscar Pallisa Gabriel: "Big Data y el sector asegurador" 2016/2017
- 220.- Marc Parada Ricart: "Gerencia de Riesgos en el Sector del Transporte de Mercancías" 2016/2017
- 221.- Xavier Pérez Prado: "Análisis de la mediación en tiempos de cambio. Debilidades y fortalezas. Una visión de futuro" 2016/2017
- 222.- Carles Pons Garulo: "Solvencia II: Riesgo Catastrófico. Riesgo Antropógeno y Reaseguro en el Seguro de Daños Materiales" 2016/2017
- 223.- Javier Pulpillo López: "El Cuadro de Mando Integral como herramienta de gestión estratégica y retributiva" 2016/2017