Universitat de Barcelona

185

Introducción del Ciber Riesgo en el Mundo Asegurador

Caso práctico: Plan de Prevención

Estudio realizado por: Marc Esteve Grau
Tutora: Amparo Zabala

Tesis del Máster en Dirección de Entidades Aseguradoras y Financieras

Curso 2014/2015

Esta publicación ha sido posible gracias al patrocinio de DAS Internacional

Presentación y agradecimientos

Mediante esta tesis he conocido la importancia que tiene el ciber riesgo en el mundo actual, pero sobretodo en el mundo asegurador. Considero este ramo de seguro muy complejo y al mismo tiempo muy interesante.

Es un tema de actualidad que está en su máxima expansión, creo que estamos al principio de lo que puede ser un ramo importante en el sector asegurador. Esta tesis me ha servido para mejorar y adquirir nuevos conocimientos que puedo poner en práctica a nivel profesional.

En primer lugar quisiera agradecer a Mercedes Ayuso y Jose Luis Pérez, ellos me brindaron la oportunidad de participar en este máster. Considero la experiencia muy satisfactoria y recomendable.

Agradecimientos también para mi tutora de la tesis Amparo Zabala. Amparo, como especialista en el seguro ciber, me ha guiado en todo momento para enfocar de la mejor manera el trabajo. Puedo considerarme afortunado por haber tratado con una especialista en este ramo.

Agradecimientos también para Casimiro Rey, profesor del máster y actual Director General de Willis S&Cc. Él me dio a conocer la existencia de este máster y al mismo tiempo recomendado a participarlo.

Para finalizar, agradecer también a aquellos especialistas del ramo que prestaron unos minutos de su tiempo para concederme la entrevista y responder a las preguntas planteadas.

Muchas gracias a todos.

Resumen

La evolución de los sistemas de información y de la tecnología en general, ha llevado a la aparición de un nuevo riesgo para las empresas y gobiernos.

Hoy en día, la información se almacena en ordenadores y/o diferentes dispositivos informáticos. Este cambio incentiva a ciber delincuentes o hackers a introducirse en los diferentes sistemas de información para poder obtener datos confidenciales. Ante el auge y la evolución creciente de esta ciber delincuencia, el sector asegurador ha desarrollado un nuevo producto que puede dar cobertura a las diferentes perdidas; sobre todo a aquellas que suponen un alto coste de reposición, como pueden ser los económicos.

Esta tesis pretende explicar la evolución del ciber seguro en los últimos años, las preocupaciones y costes producidos por este fenómeno hacia las diferentes instituciones, y el desarrollo de un nuevo producto asegurador que tiene por objetivo hacer frente a estas pérdidas.

Resum

L'evolució dels sistemes d'informació i de la tecnologia en general, a dut a terme l'aparició d'un nou risc per les empreses i governs.

Avui en dia, la informació s'emmagatzema en ordinadors i/o diferents eines informàtiques. Aquest canvi incentiva a ciber delinqüents o *hackers* a introduir-se en els diferents sistemes d'informació per obtenir dades confidencials. Davant l'auge i l'evolució creixent d'aquesta ciber delinqüència, el sector assegurador a desenvolupat un nou producte que pugui donar cobertura a les diferents pèrdues; sobre tot a aquelles que comporten un alt cost de reposició, com poden ser els econòmics.

Mitjançant aquesta tesis, es pretén explicar l'evolució del ciber risc en els últims anys, les preocupacions i costos que aquest fenomen comporten a les diferents institucions, i el desenvolupament del nou producte assegurador per fer front a aquestes pèrdues.

Summary

The evolution of the information systems and of technology, conducted to the appearance of a new risk for companies and governments.

Today, information is saved in computers and/or other information devices. This change encourages hackers or cyber felon to introduce their self's in the different information systems to obtain confidential details. Against the growth and evolution of this cyber felony, insurance industry has been able to develop a new product which can give coverage to the different lost caused; especially those which suppose a high replacement cost, such as the economic.

This thesis is intended to show the evolution of cyber insurance in the last years, concerns and costs produced to different institutions, and the development of a new insurer product.

Índice

Introducción del Ciber Riesgo en el Mundo Asegurador

1. Introducción

El mundo empresarial y político se está viendo afectado por un nuevo fenómeno: el Ciber Riesgo. Los avances en los sistemas de información llevados a cabo en los últimos años, ha dado lugar al desarrollo de un nuevo producto asegurador, el Ciber Seguro. El Ciber Seguro proviene eventualmente de los diferentes riesgos cibernéticos que puedan padecer las organizaciones.

Hace unos años las empresas no operaban a través de internet como lo hacen hoy en día. El desarrollo de nuevas tecnologías ha dado un paso importante para que organizaciones y gobiernos almacenen información confidencial.

Ante la preocupación de empresarios y políticos, a consecuencia de las grandes pérdidas económicas y por el desprestigio que puede conllevar el robo de información, el sector asegurador no se ha detenido y ha creado un nuevo producto, el cual da cobertura a las diferentes perdidas y daños.

1.1 La Evolución del Ciber Riesgo

En dos décadas Internet ha pasado de ser una curiosidad, a formar parte de nuestro día a día. Ha experimentado un rápido crecimiento como consecuencia de la globalización. El uso de esta herramienta ha aumentado de forma significativa. Con el incremento de sitios de comercio electrónico, servicios de pago y banca online, intercambio de información entre empresas, particulares, etc., internet se ha convertido en un sistema donde almacenar dinero e información, el cual ha resultado irresistible para que los delincuentes informáticos accedan a ella.

Actualmente, la amenaza más grave proviene del cibercrimen, entendido como un sinónimo de los diversos ataques a través de internet; robo de información, fraudes, sabotajes, delitos contra la imagen y la intimidad y propiedad industrial.

La expansión internacional de las empresas y la alta dependencia de éstas en sus operaciones con tecnologías de información, conlleva a que las organizaciones se sientan más amenazadas debido al aumento de exposición.

La información en la red se configura como uno de los activos más valiosos, y por ello es necesario comprender las exigencias y responsabilidades que las organizaciones adquieren.

Los delitos cibernéticos se han convertido en habituales para las organizaciones. La mayoría de ellas no disponen actualmente de una

infraestructura de gestión de riesgos que les permita combatir esas amenazas, por lo que los ataques, normalmente impredecibles, pueden convertirse en devastadores para las compañías.

Al tratarse de un fenómeno relativamente nuevo y en constante evolución, los hackers utilizan las redes para manipular la información ante el abanico de debilidades que presentan las empresas en sus plataformas tecnológicas. Cientos de empresas se ven afectadas cotidianamente por diversas amenazas, debido a la permanente actuación de los ciberdelincuentes, quienes son cada vez más propensos a infiltrarse en las redes corporativas. A raíz de estos hechos delictivos, las empresas pueden sufrir grandes pérdidas de credibilidad, como pueden ser los bancos, y también, puede llegar a afectar a su propia cuenta de resultados debido a las grandes pérdidas económicas.

Está muy extendida la idea de que solo las empresas de *e-commerce* son vulnerables a este fenómeno ya que al realizar transacciones en internet tienen que preocuparse en mayor medida de los ciber riesgos, pero la realidad es muy distinta. Todas las empresas que almacenan datos de carácter personal, y que además dependen de redes informáticas, manteniendo así cantidades importantes de información digital, deben afrontar estas exposiciones.
Según la información que hemos ido obteniendo a raíz de nuestra búsqueda, podemos afirmar que los sectores que más a menudo se enfrentan a riesgos de este tipo son: el sector hotelero, el aéreo, el financiero y el de la comunicación. El mundo empresarial juega un papel importante.

Según información obtenida de un artículo publicado el 18 de marzo de 2015 en el periódico *''El Correo''*, España es el país del mundo, por detrás de Estados Unidos y Reino Unido, que más ciber ataques recibe, como observaremos a continuación en la imagen expuesta. España corre el riesgo de quedarse atrás en la carrera de la ciber seguridad, mientras que países como Francia destinaron el pasado año 1.000 millones de euros a este sector. Félix Arteaga, investigador principal en materia de Seguridad y Defensa del Real Instituto Elcano, alerta sobre el peligro que a largo plazo puede suponer el ciber terrorismo. Grupos como el Estado Islámico ya evidencian un amplio control de la comunicación en la red, y así lo demostró, a principios de año, atacando a una empresa catalana de cierto renombre.

Por otro lado, Estados Unidos, considerado el país que recibe más ciber ataques del mundo, ha reconocido que los ciber ataques sustituyen al terrorismo como primera amenaza para el país. Según la publicación de el periódico *''El País''* del día 13 de marzo de 2013, los ciber ataques y el espionaje informático se han convertido en la principal preocupación de las distintas agencias de inteligencia y de seguridad de Estados Unidos, considerando así la ciber seguridad como una prioridad a combatir. Estos ataques informáticos han supuesto para el país pérdidas económicas multimillonarias en los últimos años. El ex secretario de Defensa, León Panetta, aseguró que cualquiera de los potenciales ataques a los que se exponen las instituciones estadounidenses podría convertirse en el *''próximo Pearl Harbour''*.

Mostramos a continuación el *ranking* de los países más afectados por este fenómeno:

Gráfico 1. Ranking de países más afectados

Fuente:http://www.infodefensa.com/es/2013/12/14/noticia-espana-peldano-lista-paises-ciberataques.html

Observando los antecedentes de algunos riesgos cibernéticos que hemos comentado y detallado en los párrafos anteriores, el sector financiero que ha actuado y que está actuando con mayor rapidez para evitar estos riesgos es la industria aseguradora. El mundo asegurador, liderado principalmente por el mercado americano, ha dedicado años a estudiar y desarrollar un producto específico que ayude a proteger las instituciones afectadas ante los riesgos informáticos expuestos. De ahí nace el llamado Ciber Seguro, *Cyber-Insurance* en términos anglosajones.

En conclusión, el ciber riesgo va en aumento año tras año y los países empiezan a ser conscientes de ello, por lo que poco a poco van tomando medidas al respecto.

Actualmente, como explicaremos con más detalle según vayamos avanzando con la tesis, la percepción de este fenómeno en Europa es aún escaso en comparación con EE.UU, dónde ya se han tomado medidas.

1.2 El Ciber Riesgo en el Ámbito Empresarial

En España se producen más de 70.000 ataques informáticos al año, siendo las empresas que venden a través de internet las más vulnerables.

Según un estudio del fabricante de antivirus, Symantec, en España las pérdidas anuales por robos de información en empresas alcanzan los 482

millones de euros. Según datos de la fiscalía General del Estado, las estafas informáticas han aumentado un 60% respecto al año anterior. Sabotajes en la red, accesos sin autorización, robo de contraseñas e información y falsificación de documentos, son otros delitos cada vez más comunes. Sectores como el financiero o empresas energéticas invierten enormes recursos en seguridad.

El sector que se dedica a ofrecer soluciones contra la ciberdelincuencia, según los expertos, factura aproximadamente 150 millones de euros en España. Al día se identifican 160.000 webs con escasa seguridad, y más de 320.000 direcciones IP registran actividad maliciosa. Según datos difundidos por la policía, el año pasado se registraron 70.000 ataques. Los incidentes más habituales analizados por el Instituto Español de Ciber seguridad consisten en accesos no autorizados a información relevante.

Pymes de producción y distribución de contenido audiovisual o editorial son las que más incidentes de seguridad presentan en España, detrás de las grandes tecnológicas, los bancos, de agencias de viajes y empresas de contenido científico o técnico. A diferencia de estos sectores, las microempresas del comercio y la hostelería, son las más despreocupadas por mantener a salvo información sensible.

Cualquier empresa que recoja, manipule o transmita datos está expuesta no sólo al ciber riesgo, sino también al robo físico. En la era digital los datos almacenados en soportes electrónicos suponen una amenaza para cualquier organización, es decir, que cualquier entidad, con independencia de su actividad, se encuentra expuesta. Para los brókers o mediadores de seguros este campo supone una enorme oportunidad de negocio.

En términos generales, existe una concienciación general sobre los ciber riesgos aunque las empresas desconocen los peligros concretos a los que se enfrentan. A fecha de hoy, la gran mayoría de organizaciones siguen sin contar con un seguro específico que las proteja.

1.3 Caso Estudio EE.UU

Estados Unidos, el país más afectado y pionero en el desarrollo del Ciber Seguro, ha visto como el paisaje cibernético ha evolucionado rápidamente en una multitud de sectores. El gobierno americano se enfrenta a un nivel sin precedentes de ataques cibernéticos y amenazas.

El potencial de pérdidas económicas derivados de la amenaza cibernética no se puede subestimar. Expertos económicos americanos, han advertido de una desintegración digital, un escenario en el que el ciberespacio podría ser completamente debilitado debido al fortalecimiento de los ataques en Internet. Internet ya no es por tanto considerado como un medio fiable para la comunicación o el comercio. Durante los últimos años, se han detectado que los ciber ataques se están expandiendo por todo el sector industrial, y éstos están expuestos a grandes pérdidas económicas.

Organizaciones muy importantes se han visto afectadas durante la última década, es por ello que el mismo gobierno ha decidido tomar medidas al respecto, las cuales explicaremos más adelante.

Recientemente, tal como hemos mencionado en el párrafo anterior, organizaciones americanas de cierta relevancia mundial, han recibido ataques informáticos. La realidad es que la lista de los mismos es interminable, pero me gustaría hacer hincapié en los casos que considero más importantes. Marcas como eBay, JPMorgan, Yahoo! y The Home Depot, forman parte de este amplio listado, y ya se han avanzado a formalizar una póliza de Ciber Seguro para cubrir las pérdidas causadas.

Caso eBay:

La empresa de compras online, eBay, recibió un ataque cibernético que jaqueó la base de datos que contiene claves y datos financieros.
El ataque ocurrió después de que los hackers obtuvieran las contraseñas de algunos empleados, con lo que pudieron acceder a entrar en la red corporativa.
EBay trabajó con la policía y expertos en seguridad para investigar el caso, y aplicando las prácticas y las herramientas necesarias para proteger a los clientes.

Caso JP Morgan

Datos bancarios de 76 millones de hogares y 7 millones de negocios fueron robados por hackers debido a la vulnerabilidad del sistema de JP Morgan Chase.
En su documento ante la Comisión de Bolsa y Valores de EE.UU. (SEC), JP Morgan dijo que la información robada incluía nombres, direcciones, números de teléfono, direcciones de correo electrónico y datos de clientes internos. No hay evidencia, sin embargo, que los números de cuenta, contraseñas, nombres de usuario, fechas de nacimiento o números de seguro social fueran jaqueados.

Caso Yahoo!:

Yahoo!, en Japón, fue atacado por hackers, que consiguieron robar archivos con 22 millones de nombres y datos sobre las cuentas personales. La compañía aconsejó en aquel momento a sus usuarios que cambiaran de contraseña. Según informó la BBC, en cuanto se detectó la intrusión, la empresa cortó el acceso a la red y comenzó a investigar lo sucedido. Tras el ataque, la compañía reforzó su seguridad para garantizar que los hackers no pudieran volver a acceder a los datos personales de las cuentas.
Caso The Home Depot:

El proveedor de equipos para la construcción, Home Depot, informó que sus sistemas de pago fueron atacados por piratas informáticos, provocando una filtración de datos que afectaría a millones de clientes.

La empresa confirmó que “su sistema de pagos había sido violado, lo que podría potencialmente afectar a clientes que usen tarjetas de pago en tiendas canadienses y estadounidenses”, informó en un comunicado.
Estas informaciones llegaron días después de que el investigador en seguridad informática, Brian Krebs, dijera que piratas informáticos habían puesto en venta tarjetas de crédito y débito robadas que aparentemente provenían de Home Depot.

Caso Ashley Madison:

Aunque ubicada en Canadá, la web de contactos Ashley Madison es el caso más reciente de grave ataque ciber.
Los hackers han filtrado cantidad de datos e información confidencial perteneciente a los usuarios.
Si ya resulta grave y criminal la publicación de esta información más aún cuando su éxito está basado en las infidelidades de los clientes.
Todo ello ha llevado a que dos usuarios se hayan suicidado después de que sus datos personales y contactos fueran filtrados y expuestos públicamente
El impacto social de esta publicación está siendo enorme.
La compañía propietaria de la web está ofreciendo ya una recompensa para cualquier información que pueda llevar a la detención de los hackers.
Ya que por su parte está afrontando una demanda, a día de hoy, de 576 millones de dólares que han interpuesto los supuestos clientes.

Las grandes empresas son normalmente los grandes objetivos de los ciber delincuentes. Éstas gestionan grandes volúmenes de datos. Un gran volumen de datos implica que una fuga pueda conducir al robo de un mayor número de registros, lo que supone un elevado coste para mitigar la gestión de crisis, además de ser susceptibles de recibir acciones sociales de responsabilidad por parte de accionistas, en el caso que la acción pierda valor tras haber recibido un ataque.

Las grandes compañías son conscientes que la gestión y control de cientos y miles de empleados resulta farragosa. Monitorizar y controlar los actos mal intencionados y negligentes de los empleados, así como el robo y pérdida de dispositivos electrónicos en tránsito, resulta difícil de controlar y la resolución de las violaciones de seguridad en grandes empresas pueden dilatarse en el tiempo.

Aquellas entidades que llevan a cabo operaciones internacionales se enfrentan a dificultades añadidas si sufren una violación de seguridad. La transmisión global de datos implica grandes costes de mitigación en servicios de consultoría legal y forense ya que los expertos de cada país deben coordinarse para proveer la mejor solución al cliente.

Diferentes instituciones americanas y sectores industriales han dado a conocer públicamente las violaciones de datos en 2013. En total, se registraron 614 ataques de cierta relevancia en diferentes sectores empresariales, así como: el financiero, educativo, industrial, etc. según el *Identity Theft Resource Center.* Estos datos pueden ser comparables con los detectados en años anteriores.

En 2012, por ejemplo, se notificaron 449 violaciones de datos, cifra inferior a las recibidas en 2013. Hasta el momento, en 2015, se han registrado 311 ataques cibernéticos, los cuales se dieron a conocer públicamente el pasado 27 de mayo. Sin embargo, a pesar del aumento de registros expuestos y de los reportados, se considera que el número real de infracciones es sin duda mucho más elevado, ya que muchas compañías, sino la mayoría, no denuncian los ataques.

En octubre de 2011, la Comisión de Bolsa y Valores (SEC), emitió un comunicado instando a las empresas que cotizan en bolsa a revelar los casos importantes de riesgos cibernéticos. Esta comunicación fue un paso importante para que grandes compañías decidieran protegerse mediante la cobertura del seguro.

Las empresas europeas con operaciones o con datos en los EE.UU. deben cumplir con las 46 legislaciones estatales que regulan la transmisión de datos, cada una con requisitos de seguridad y con procesos de notificación a los individuos afectados distintos. La normativa se extiende más allá de los requerimientos estatales y las empresas deben adherirse a las leyes específicas de cada sector. Asimismo, la SEC requiere a las empresas que coticen en Bolsa que revelen sus riesgos operacionales y financieros en el caso de sufrir un ciber ataque o incidente de seguridad de datos.

Debido al aumento considerable de delitos cibernéticos, dirigidos principalmente a empresas americanas o compañías europeas con exposición en EE.UU., el gobierno de Estados Unidos ha llevado a cabo una serie de medidas sustantivas de seguridad cibernética a nivel nacional.
El robo de secretos militares y comerciales es una de las principales preocupaciones del gobierno. Cabe recordar el episodio vivido entre el gobierno americano y chino el pasado año. En mayo de 2014, Estados Unidos denuncio a cinco miembros del ejército chino por realizar actividades de espionaje cibernético. Como también, cabe recordar, el episodio vivido por las filtraciones del ex empleado de la CIA, Edward Snowden, en 2013. Mención, también, para el grupo de hackers de mayor notoriedad, Anonymous, los cuales se dedican a infiltrarse en sistemas informáticos gubernamentales, con objetivos claramente identificados: como es el caso de Occupy Wall Street en Estados Unidos y en países Árabes.

En febrero de 2014, el Instituto Nacional de Estándares y Tecnología (NIST), dio a conocer un nuevo marco para la mejora de la seguridad cibernética. El marco existente reúne las normas y prácticas mundiales para ayudar a las organizaciones a entender, comunicar y gestionar sus riesgos cibernéticos. La NIST siguió una orden ejecutiva emitida hace un año por el presidente Obama que promueve el intercambio de información. Debido al aumento de intercambio de información, los riesgos cibernéticos aumentaron entre empresas públicas y privadas.

Una serie de propuestas federales legislativas / reglamentarias sobre ciber seguridad están actualmente bajo consideración del congreso americano. A

nivel estatal, 47 estados ya tienen leyes de notificación de incumplimiento vigentes.

1.3.1. Ciber Seguridad: Preocupaciones y Costes

La seguridad y las pérdidas económicas son preocupaciones crecientes entre las empresas debido a la violación de datos.

Según un informe de Allianz, el Barómetro de Riesgos, que sondeó a más de 400 expertos en seguros corporativos de 33 países, encontró otros riesgos emergentes relacionados entre sí, como la pérdida de problemas de reputación y los cambios en la legislación.

Una señal de que las organizaciones están tomando medidas a esta amenaza, se puede reflejar en la encuesta de PWC, la cual encontró que la percepción del riesgo de la delincuencia informática está aumentando a un ritmo más acelerado que el de las ocurrencias reales presuntamente notificadas. Aproximadamente el 48% de los encuestados dijo que su percepción del riesgo de ciberdelincuencia en su organización aumentó en 2014, por encima del 39% en 2011. Reforzando esta evidencia, PWC señaló que un porcentaje idéntico (48%) de los directores generales, en su estudio de Global CEO, dijo que estaban preocupados por las amenazas cibernéticas, incluyendo la falta de seguridad de los datos.

Los ataques cibernéticos siguen siendo muy costosos para las organizaciones y los costes van en aumento año tras año. Un estudio anual de las empresas estadounidenses, realizadas en este caso por el Instituto Ponemon, estima que el coste promedio anual causado por delitos cibernéticos, se situó alrededor de 11,6 millones dólares anuales, considerado un aumento del 30% de los $ 8.9 millones reportados el año anterior.

El robo de información sigue representando los costes externos más altos para las empresas que experimentan ataques, seguido de los costes asociados con la pérdida de beneficios, según el estudio de Ponemon.

Los ataques cibernéticos pueden provocar pérdidas económicas adulteradas si no se resuelven rápidamente.

1.3.2. Amenazas del Ciber Crimen y Ciber Terrorismo

La amenaza, tanto para la seguridad nacional y la economía, que representa la delincuencia cibernética y el ciberterrorismo, se ha convertido en una preocupación creciente para los gobiernos.

El Instituto Internacional de investigación del Terrorismo (ICT) informa de que los grupos como el ISIS (Estado Islámico) y otras organizaciones terroristas, se están aventurando cada vez más en el ciberespacio, la llamada "yihad electrónica", basada en atacar al enemigo saboteando su infraestructura y utilizando información para causar el caos.

En los últimos años también ha habido un creciente número de ataques cibernéticos contra objetivos políticos, atacando la infraestructura crítica (incluyendo agua, electricidad y gas), y los sitios web de las empresas comerciales. De acuerdo con las ICT, estos ataques son perpetrados por: estados, grupos de hackers (como Anonymous), organizaciones criminales y hackers solitarios.

El propio Instituto hace referencia a una serie de acontecimientos recientes, entre ellos: la creciente popularidad de la moneda digital, como el Bitcoin, que resulta ser aceptado como pago por un número creciente de establecimientos, a pesar de los riesgos potenciales y los usos ilegales.

Una encuesta reciente realizada por Tenable Network Security, encontró que la mayoría de los estadounidenses temen que la guerra cibernética sea inminente y que el país sea atacado de forma exponencial en la próxima década. Un abrumador 93% de los encuestados creen que las corporaciones y empresas de Estados Unidos son vulnerables a recibir ataques. El 95% cree que las agencias del gobierno son, también, muy vulnerables a los ataques cibernéticos.

La encuesta reveló resultados contradictorios sobre quién debe ser considerado responsable de la protección de las redes corporativas, si el sector público o privado.

Cerca del 66% de los encuestados creen que las empresas deben ser consideradas responsables de las infracciones cibernéticas. Pero un número casi igual de los estadounidenses - 62% - afirman que el gobierno debe ser responsable de proteger a las empresas estadounidenses de dichos ataques.

A pesar de que los riesgos cibernéticos y seguridad cibernética son ampliamente reconocidos como una amenaza seria, muchas empresas no son conscientes del peligro que éste puede suponer y es por este motivo que aún no compran el seguro. Sin embargo, esto está cambiando. Desarrollos legales recientes ponen de relieve el hecho de que la dependencia en las pólizas de seguros tradicionales no es suficiente, ya que las empresas se enfrentan a nuevas responsabilidades. Es importante destacar que el seguro de ciber, hasta la fecha, no da cobertura a los ataques informáticos recibidos por grupos terroristas; es una exclusión habitual de la póliza.

2. Plan de Prevención

2.1. Antecedentes y Objetivos

Desde los departamentos de Gerencia de Riesgos se proponen los esquemas de trabajo para el análisis de los principales ciberriesgos que afectan o pueden llegar a afectar a la actividad de una organización. Mediante el siguiente caso práctico, el cual explicaremos a continuación, se desarrolla un trabajo de consultoría apoyándose en la herramienta de GlobalRisk. Siempre desde la visión o el punto de vista de un mediador.

El caso práctico está enfocado principalmente a grandes corporaciones, pero también podría adaptarse a pequeñas y medianas empresas. El plan de prevención descrito trata de Identificar, analizar y evaluar los riesgos para diseñar un plan de acción que defina y aplique las medidas más adecuadas para minimizar y/o eliminar los riesgos detectados.

OBJETIVO:

Realizar un análisis de ciberriesgos sobre los procesos y sus principales activos que nos dé un estado de situación claro respecto a la exposición de la organización ante incidentes de ciberriesgo.

Una vez realizados los trabajos de consultoría, se recomienda continuar implementando las fases de un Sistema de Gestión de Aseguramiento de Ciberriesgos - SGAC:

- Establecer un plan de acción para reducir los niveles de riesgo obtenidos en el análisis a niveles aceptables por la organización.

- Realizar acciones proactivas encaminadas a la reducción de incidentes de ciberriesgo.

- Reducir los costes derivados de ataques de ciberriesgo.

- Realizar una correcta transferencia de aquellos ciberriesgos detectados que sean asegurables.

2.2. Mapa de Ciberriesgos

2.2.1. Introducción General

En el presente documento se detalla la sistemática para realizar un análisis de riesgos cibernéticos para una organización, obteniendo así un mapa que se contiene todas las situaciones de riesgo a la que está sometida la compañía desde el punto de vista cibernético, ya sea de forma interna o externa, por ataques o por errores.

Una vez analizados los ciberriesgos se elaborará un informe con las oportunidades de mejora detectadas en base al estado actual del mercado para reducir esos niveles de riesgo a niveles aceptables por la organización.

Los ciberriesgos analizados se clasifican por su gravedad, desde Muy Altos (considerados como intolerables) a Bajos o Muy Bajos (entendidos como aquellos controlados por la organización).
La clasificación es el resultado, para cada riesgo, del análisis de dos factores:

- Probabilidad de ocurrencia.

- Impacto sobre la organización, en caso de materialización del ciberriesgo.

Adicionalmente, se valoran también las medidas de control y mitigación existentes.

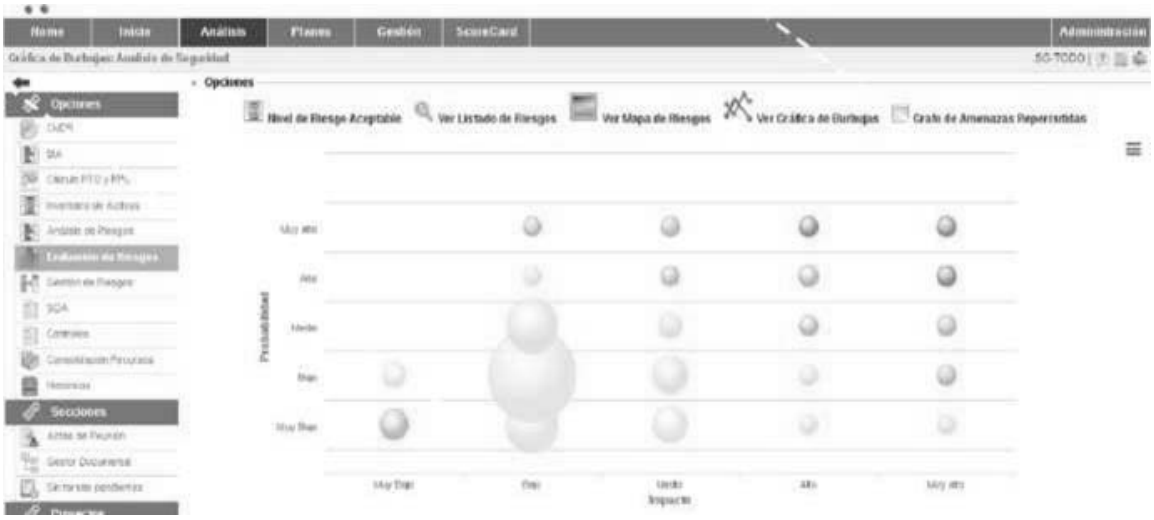
2.2.2. Metodología

Tras el análisis de estos factores se obtiene el Mapa de Ciberriesgos actual de la organización, que se representan en el diagrama correspondiente denominado Matriz de Riesgos. La posición que ocupa cada ciberriesgo en estos diagramas determina el tipo de acción que debería realizarse para la mitigación o reducción de los mismos. A modo de ejemplo con datos ficticios:

Figura 1 Mapa de Riesgos

En la siguiente figura se muestra el diagrama de burbujas que representaría la distribución de los ciberriesgos:

Figura 2 Diagrama de Burbujas



El tamaño de las burbujas representa el número de riesgos que comparten la misma clasificación, tras evaluar factores de probabilidad de ocurrencia e impacto sobre la organización. En este sentido puede apreciarse una concentración significativa de riesgos en la zona intermedia y superior del diagrama, correspondiente a Riesgos Medios (potenciales) en su mayoría y Altos (severos).

Para la evaluación de ciberriesgos, utilizamos la herramienta GlobalRisk que tiene en cuenta la posibilidad de ocurrencia, la severidad esperada y los medios de protección o controles existentes en la actualidad. Tras esta evaluación se obtiene un Mapa de Riesgos que permite dar una visión global de los ciberriesgos que afectan a la organización, así como su criticidad y su impacto económico.

2.2.3. Fases

1. Identificación de ciberriesgos. Se realiza en base a:

- Identificación de servicios, procesos y activos: debe realizarse un mapa en el que queden documentados tantos los servicios/actividades principales de la compañía como los procesos internos que dan soporte a esos servicios/actividades. A su vez deben identificarse los activos (instalaciones, hardware, software, aplicaciones, infraestructura tecnológica, etc.) que son necesarios en la operación de los diferentes procesos y que pueden ser objeto de la materialización de amenazas de ciberriesgo. Sobre ese mapa de servicios, procesos y activos se analizarán los ciberriesgos.

Identificación de amenazas y vulnerabilidades: para cada servicio, proceso y activo se determinan las amenazas que pueden afectarle. Las amenazas son eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales. La consecuencia de una amenaza, si se materializa, es un incidente que modifica el estado de riesgo

(ciberriesgo) de la organización. Se van a definir al menos los siguientes tipos de amenazas, pudiéndose contemplar tipologías adicionales:

- Intencionadas
- No intencionadas
- Internas
- Externa
- Accesos no autorizados
- Suplantación identidad de los usuarios
- Escalado de privilegios
- Vulnerabilidades de los sistemas
- Denegación de servicio

Se asocia a cada amenaza la vulnerabilidad que puede explotarla, es decir, la debilidad que tiene el servicio, proceso o activo para que la amenaza pueda materializarse y derivar en un incidente de ciberriesgo.

2. Evaluación de los ciberriesgos:

De acuerdo a parámetros que miden la posibilidad de ocurrencia y la intensidad. En este punto se obtiene la "foto actual" de la organización (Mapa de ciberriesgos).

Debe definirse un nivel de riesgo aceptable, por encima del cual la organización debe gestionar sus riesgos. Los riesgos que queden por debajo o en dicho nivel no será necesario reducirlos, aunque podría plantearse como una mejora del mapa de riesgos.

En el siguiente apartado "Evaluación de Riesgos con GlobalRisk" se desglosa la sistemática para realizar dicho estudio con GlobalRisk.

2.2.4. Evaluación de riesgos con GlobalRisk

La herramienta GlobalRISK se basa en los siguientes factores:

1. Posibilidad de ocurrencia: Medida cualitativa de materialización del riesgo de acuerdo al estado de controles existente. Clasificación según la siguiente tabla:

Cuadro 1.

Probabilidad	Descripción
Muy Alta	Altamente probable. Ha ocurrido varias veces en el seno de la organización.
Alta	Probable. Ha ocurrido al menos una vez en la organización.
Media	Posible. Puede ocurrir ocasionalmente.
Baja	Improbable. No ha ocurrido en PORTAVENTURA pero ha sucedido al menos una vez en organizaciones similares.
Muy Baja	Muy improbable. No hay información de que haya ocurrido, pero es un escenario verosímil.

2. Impacto de las consecuencias tras la materialización del riesgo. Esta variable indica la intensidad del riesgo, atendiendo a su severidad y

capacidad de afectación sobre la organización. Puede ser medida en base a diversos parámetros, como podrían ser por ejemplo: tecnológico, nivel de servicio, reputación y financiero, optando siempre por el de peores consecuencias para la organización. A largo plazo, todos estos indicadores tienen un componente financiero, ya que conllevan a una posible afectación a la cuenta de resultados de las empresas. La tabla utilizada para la cuantificación de este factor es la siguiente:

Cuadro 2.

Impacto	Descripción	Tecnológico	Finanzas	Servicios	Reputación
Muy Alto	Si este riesgo se materializase, sería casi imposible para la organización recuperarse.	Ej. Caída total de los sistemas principales, con impacto operativo. Robo y pérdida de información confidencial y/o estratégica y de clientes para usos maliciosos.	Pérdida de más de un año de ganancias	Ej. *Caída catastrófica en los niveles de servicio, pérdida definitiva de clientes principales, completo fracaso en los estándares de calidad, máxima penalización financiera.*	Grave protesta pública o de medios de comunicación a nivel internacional. Se requiere intervención de la Alta Dirección y reducción del daño
Alto	Las consecuencias de la materialización del riesgo, aunque severas, pueden ser resueltas hasta un cierto punto.	Ej. Caída de sistemas principales. Robo de información sensible y de clientes.	Pérdida de más de la mitad de un año de ganancias	Ej. *Significativa caída en los niveles de servicio, incumplimiento plazos en los proyectos, pérdida de clientes , importante penalización financiera*	Importante y adversa cobertura pública o de medios de comunicación a nivel nacional. Se requiere una declaración pública para hacer frente a la situación
Medio	Las consecuencias de la materialización del riesgo no son severas y, si se materializaran, pueden ser resueltas.	Ej. Caída o degradación de algunos sistemas de información. Acceso a información corporativa y/o de clientes.	Pérdida de más de un 0.25 de ganancias anuales	Ej. *Caída moderada en los niveles de servicio, relaciones tirantes con los clientes, retraso en los proyectos. Posibles penalizaciones financieras y/o sanciones administrativas.*	Atención de los medios de comunicación o pública a nivel local - Relaciones con la comunidad en peligro pero sin daño a nivel nacional
Bajo	Las consecuencias de la materialización del riesgo se consideran relativamente sin importancia.	Ej. Degradación de algún sistema de información, sin llegar a caer.	Pérdida de más de un 0,1 anual de ganancias	Ej. *Caída leve en los niveles de servicio, algún estándar de calidad no alcanzado. Sin penalización financiera*	Leve repercusión pública o de los medios de comunicación - No se requieren medidas especiales más allá de las operaciones normales
Muy Bajo	No se detectan consecuencias de la materialización de este riesgo.	Ej. Mínima degradación con solución inmediata.	Pérdidas de baja cuantía o no significativas	Ej. *Alguna interrupción de los servicios pero que podría ser solucionada sin involucrar a terceros.*	Es improbable que la inquietud pública provoque efectos duraderos. No se requieren medidas para corregir la situación

2.2.5. GlobalRisk

GlobalRisk es la plataforma que permite a empresas y a sus consultoras la implantación, identificación, análisis y gestión de Riesgos colaborativos basándose en la actual norma sobre gestión del riesgo ISO 31000.

A través de GlobalRisk dispondrá de una solución integrada que permitirá desarrollar un sistema completo de apreciación del riesgo basándose en la norma ISO 31000 para la Gestión del Riesgo

.

GlobalRisk permite la gestión integral de la norma y el cumplimiento del ciclo completo de la misma, desde las fases de inicio y planificación del proyecto hasta el mantenimiento y mejora continua, pasando por las fases de identificación del riesgo, análisis de riesgos, evaluación del riesgo, gestión del riesgo así como el cuadro de mando necesario para la monitorización del sistema.

Como factor diferencial, permite realizar dichos análisis de riesgos con cualquier metodología gracias a las opciones de parametrización que posee, y

ofrece al usuario de realizar análisis económicos de los riesgos así como estudios del retorno de inversión de los planes de tratamiento de riesgo.

2.2.5.1. Características y funcionalidades de GlobalRisk

Descripción de la herramienta:

GlobalRisk dispone de los módulos básicos que compone la plataforma más los módulos específicos para la implantación de la norma ISO 31000. Estas funcionalidades se incluyen en dos soluciones principales:

- Plataforma GlobalSuite. Al igual que el resto de herramientas incluidas en la plataforma GlobalSuite, GlobalRisk dispone de todos los módulos comunes de la plataforma además del módulo PDCA para la gestión de la mejora continua.

- Módulo Análisis y Gestión de Riesgos (Solución AGR). Esta solución permite identificar, analizar, evaluar y gestionar todos los riesgos de una organización. Esta solución permite realizar desde una identificación del riesgo a medida para cada tipo de riesgo analizado, como diferentes análisis y evaluaciones del riesgo para cada uno de los tipos de riesgos seleccionados (financiero, operacional, legal, industrial, etc.). Se podrá disponer de diferentes planes de tratamiento del riesgo para cada tipo de riesgos y evaluar dichos riesgos de manera individual o consolidada para todos los riesgos.

Generalidades

Se describe a continuación la herramienta software GlobalRisk para la implantación, gestión y mantenimiento de Sistemas de Gestión basados en el cumplimiento de la Norma ISO 31000.

Cuadro 3.

SEGURIDAD	Conexión HTTPS entre cliente web y servidor web. Conexiones cifradas entre los diferentes servidores que conforman la plataforma. Certificados Digitales: Las conexiones con la herramienta son conexiones SSL, por lo que es necesario instalar un Certificado Digital que permita este tipo de conexiones. Módulo interno de seguridad para el control de todas las entradas, salidas y operaciones internas de datos.
CERTIFICACIONES (sólo en modo SAAS)	PRODUCTO: Certificación ISO 27001 que asegura una correcta gestión de la seguridad de la información de la plataforma. SERVICIO: normas ISO 27001 (seguridad de la información), ISO 20000 (gestión del servicio) e ISO 22301 (gestión de la continuidad de negocio), asegurando una correcta gestión de la disponibilidad y la continuidad de la plataforma Además hay un estricto cumplimiento de la legislación española referente a protección de datos de carácter personal (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, LOPD)
DISPONIBILIDAD (sólo en modo SAAS)	Disponibilidad 24 horas los 365 días del año. 95% anual. Plataforma con todos sus servidores, bases de datos y electrónica de red redundada y balanceada. Acceso a Internet multi-homed, es decir, la conexión se realiza a través de varios operadores y emplea el protocolo de enrutación dinámica BGP4 para optimizar su tráfico a la vez que obtiene redundancia Se dispone de un sistema redundante ininterrumpible de Energía en el CPD.

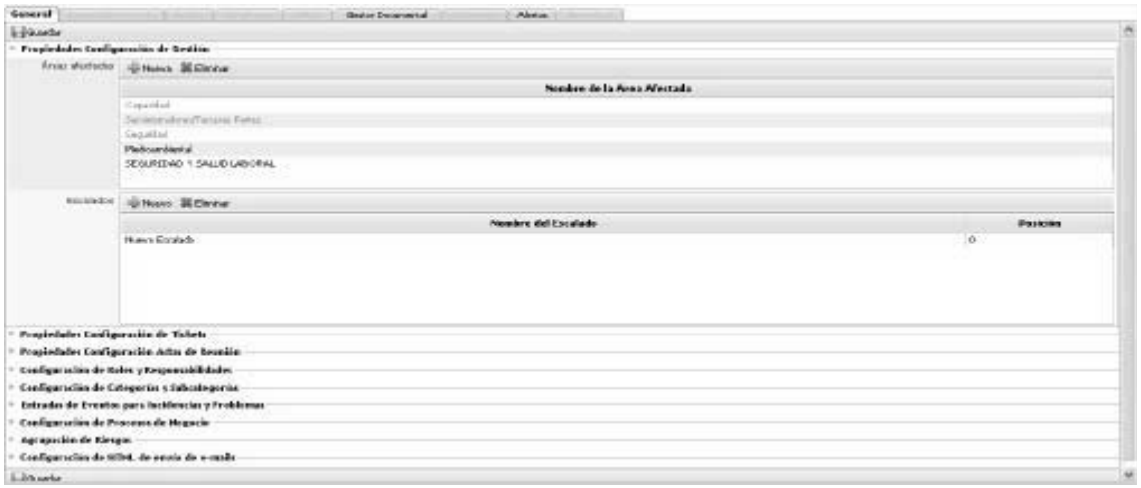
Funcionalidades

Cuadro 4.

CATEGORÍA	DESCRIPCIÓN
CONFIGURACIÓN	1. Permite definir y configurar cualquier tipo de metodología, diferentes modelos de madurez, rangos y niveles 2. Permite la configuración de Actas de reunión, destacando el registro de acciones del Comité de Seguridad, envío automático de actas a todos los asistentes y el archivo directo en el gestor documental. 3. Permite configurar los valores por defecto que presentarán los formularios para la gestión del sistema. Propone valores por defecto, necesarios para la correcta gestión y pueden ser ampliados en función de las necesidades de cada organización. Se pueden definir niveles de escalado para las incidencias existiendo la posibilidad de priorizarlas. 4. La herramienta permite configurar los diferentes roles de los que cada empresa dispone; las solicitudes; categorías; riesgos; procesos; y envío de notificaciones. 5. Permite configurar el inventario de activos en función de las categorías, dimensiones y niveles. 6. Permite configurar los controles referentes a la gestión del riesgo. 7. Permite definir el tipo de control documental que dispondrá la empresa, así como los estados por los que puede pasar la documentación y la necesidad de control de versiones. 8. Permite configurar las alertas que quiera recibir sobre el funcionamiento y gestión del SG.

Ejemplos de configuración (gestor documental, alertas, análisis)

Cuadro 5.



Cuadro 6.

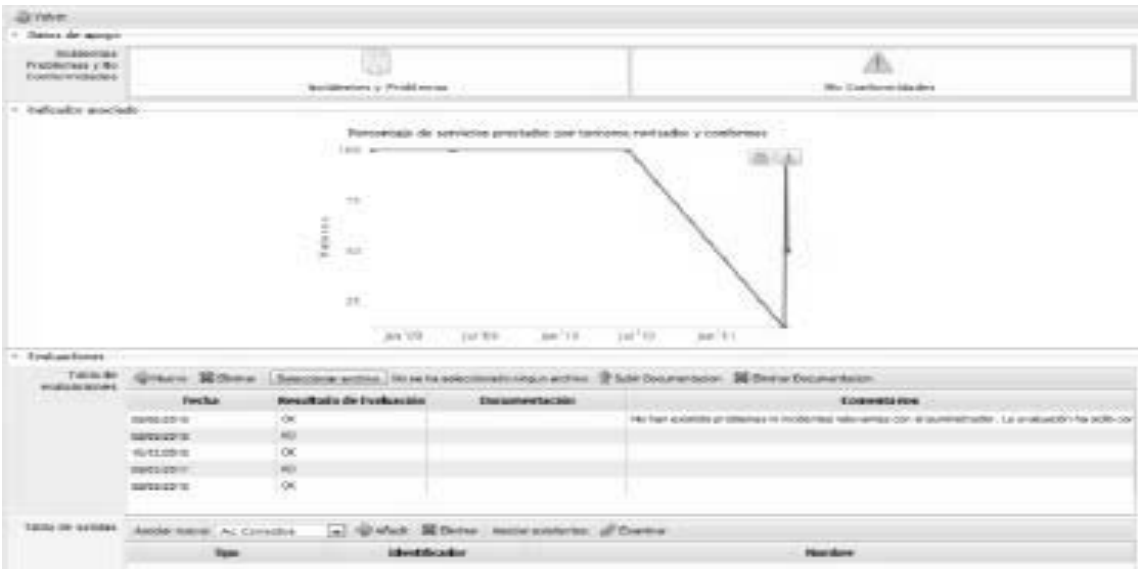
CATEGORÍA	DESCRIPCIÓN
INICIO DEL PROYECTO	1. La herramienta puede definir el alcance, el comité, organigrama y diagrama de red entre otros. Una vez definidos todos los campos del alcance, el documento puede descargarse para ser aprobado. 2. Permite determinar los objetivos del sistema para un periodo determinado. Los objetivos pueden categorizarse o asociarse a servicios o productos. Se pueden definir objetivos específicos y establecer qué metas se propone la empresa para conseguir cada objetivo. 3. Permite la asociación de roles a los empleados de la organización así como sus competencias, consiguiendo la trazabilidad entre los roles, los empleados, la capacitación de dichos empleados y las competencias de los puestos de trabajo. Ayudará a poder definir planes de formación / capacitación. 4. Permite definir los servicios, productos o procesos de negocio implicados en el alcance. Los servicios y productos que se definan en el catálogo, pasarán a formar parte del sistema (se convertirán en activos para su posterior análisis) y permitirán categorizar y tipificar todo el sistema capilarizando todo el sistema en estos servicios y productos. 5. Permite definir los acuerdos de nivel de servicio y asociarlos al servicio o producto correspondiente del catálogo. 6. Permite la definición de los proveedores (suministradores), datos de contacto, contratos o incluso definir los SLAs además de evaluar el desempeño. 7. Permite descargar informes editables de cada opción.

Definición de objetivos

Cuadro 7.

Gestión de suministradores

Cuadro 8.

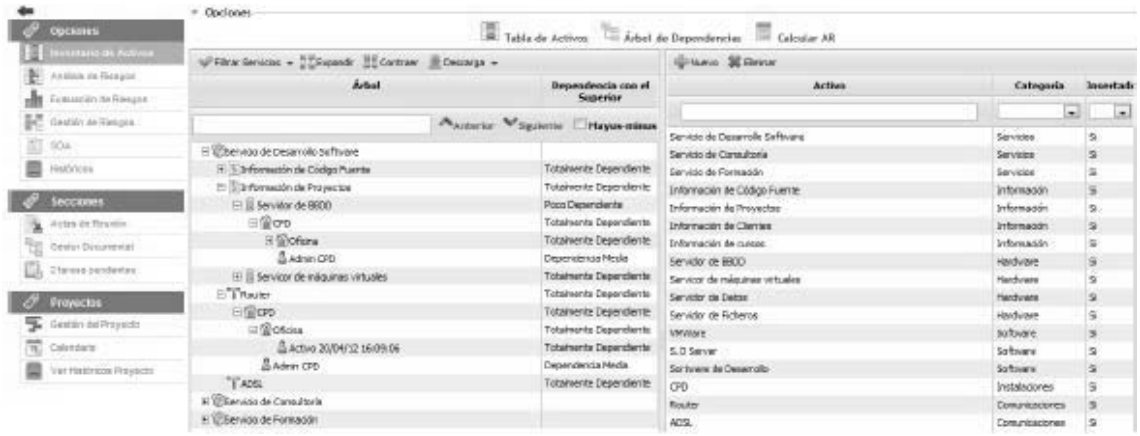


Cuadro 9.

CATEGORÍA	DESCRIPCIÓN
ANÁLISIS Y GESTIÓN DE RIESGOS	1. Permite definir la estructura asociada al alcance del proyecto, a través del inventario de activos. 2. Permite calcular la IMPORTANCIA de cada activo y el RIESGO 3. Permite el envío de encuestas personalizadas para la identificación de los Riesgos 4. Permite la configuración de dimensiones y de metodologías para el cálculo de los riesgos. 5. Permite determinar el nivel de riesgo aceptable. 6. Permite el registro de los controles necesarios para el tratamiento del riesgo. 7. Brinda indicadores personalizables para el Análisis y Gestión de los Riesgos. 8. Módulo de dependencias entre Activos. 9. Permite la posibilidad de realizar diferentes Planes de Tratamiento de Riesgos para los activos que se vayan a tratar, así como su seguimiento 10. Permite la generación de históricos para comparar la evolución del análisis y gestión de riesgos. 11. Se establecen filtros de ayuda para búsquedas.

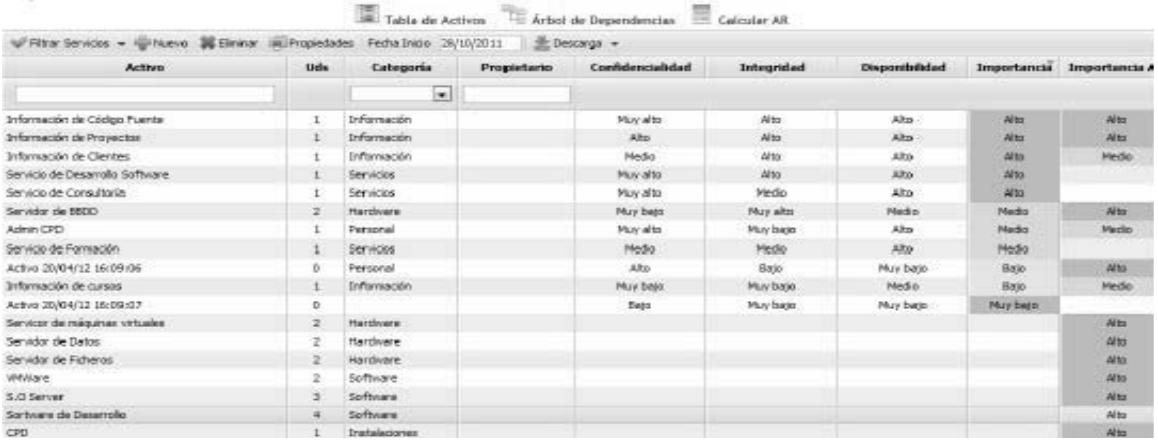
Dependencias

Cuadro 10.



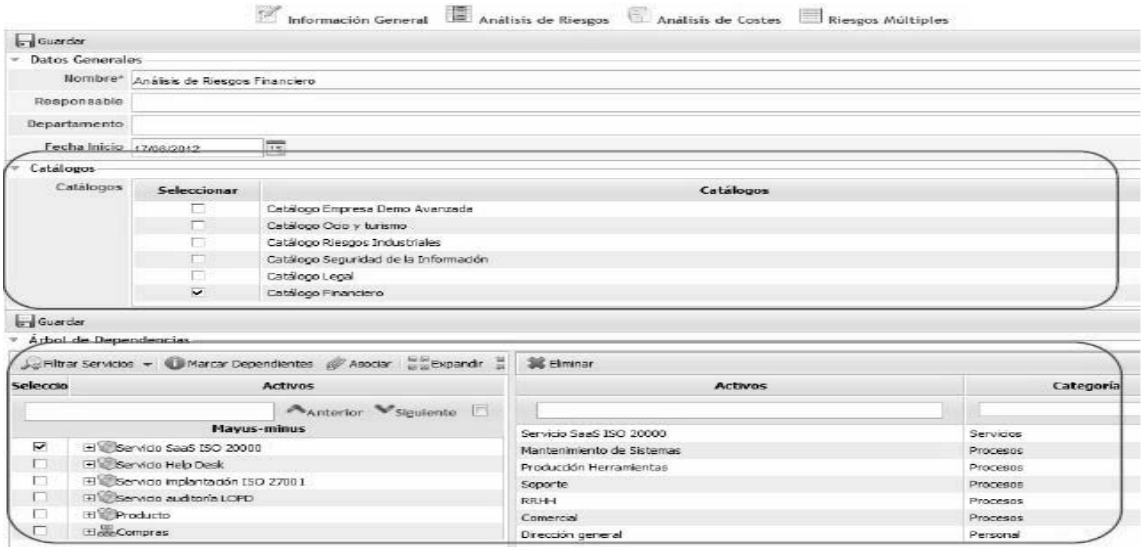
Importancias

Cuadro 11.

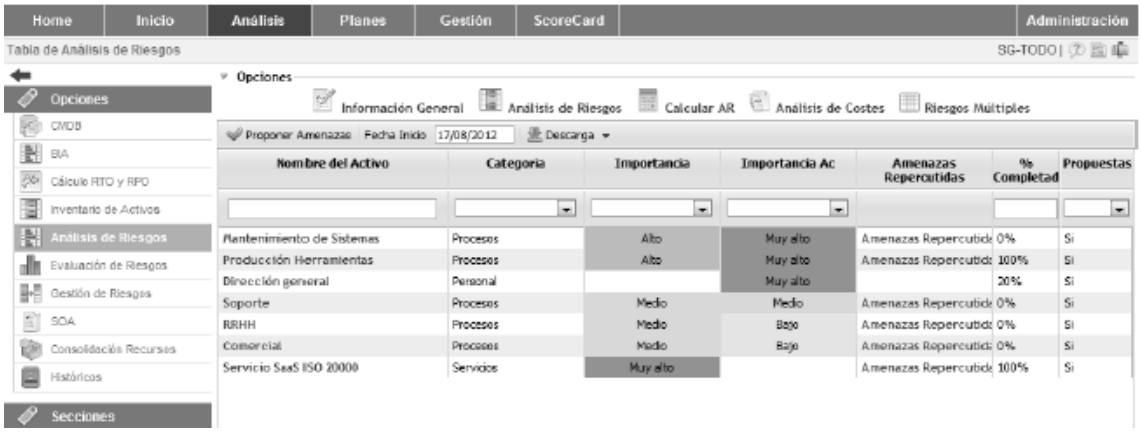


Análisis

Cuadro 12.

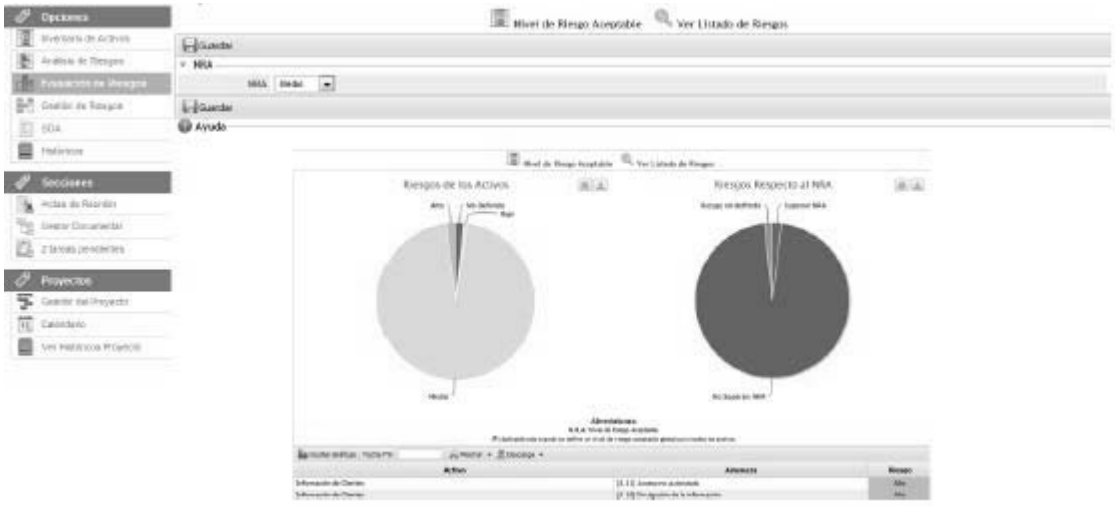


Cuadro 13.



Evaluación de riesgos

Cuadro 14.

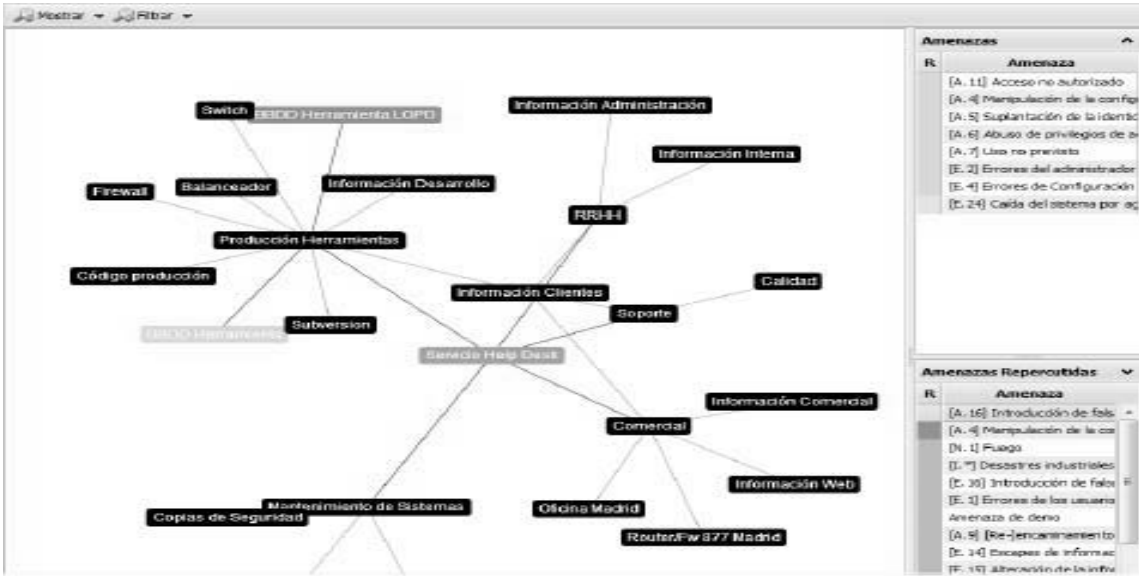


Mapa de riesgos

Cuadro 15.

Mapa de amenazas

Cuadro 16.

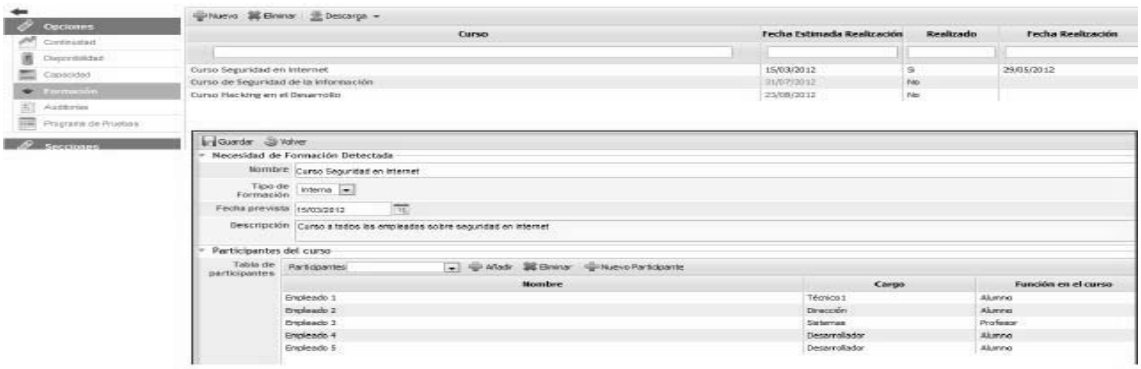


Cuadro 17.

CATEGORÍA	DESCRIPCIÓN
PLANES	1. Permite el control de cada uno de los procesos y aspectos que deben generarse a lo largo de los ciclos de mejora. 2. Permite la gestión de planificaciones y calendarios exigidos en los sistemas de gestión. 3. Permite la gestión de la capacidad y disponibilidad, y establecimiento de planes que permitan su seguimiento. 4. Permite la gestión de formación o capacitación y la concienciación del personal. Desarrollo de planes que permitirán el seguimiento de la formación, análisis de resultados y posibles desviaciones. 5. Permite la planificación de auditorías tanto internas como de certificación.

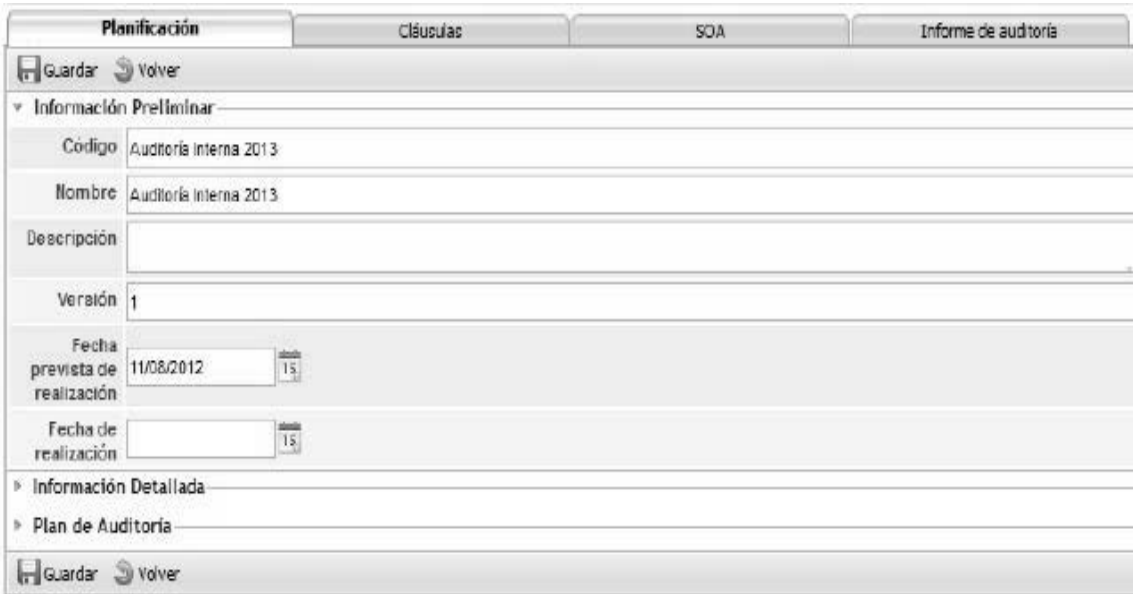
Plan de formación

Cuadro 18.



Plan de auditoria

Cuadro 19.

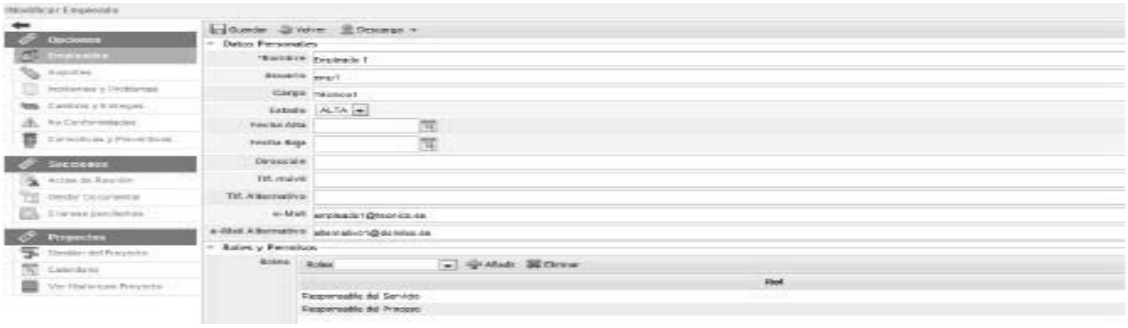


Cuadro 20.

CATEGORÍA	DESCRIPCIÓN
PROCESOS	1. Proporciona los procesos asociados al ciclo PDCA y que proporcionan una correcta gestión de la mejora continua del sistema. 2. La herramienta proporciona la gestión integral de los empleados de la organización. Altas y bajas, roles y responsabilidades, y permisos de información. 3. Se podrán importar y exportar listados de empleados o sincronizar con sistemas de gestión de usuarios. 4. Permite la gestión de soportes, control de entradas, control de salidas y la asignación a empleados. 5. Permite la gestión de incidentes y problemas. Dispone de varios estados para los incidentes y problemas, permite asociarles categorías, servicios o priorizarlos. Además se podrá llevar un seguimiento pormenorizado de cada uno de ellos, enviar emails a los responsables y tomar decisiones. 6. Permite el registro y la gestión de reclamaciones. Su operativa es similar a la llevada a cabo en los incidentes y problemas 7. Se podrán crear, revisar y gestionar todas las no conformidades tanto derivadas de auditorías como de la propia mejora continua del sistema. Asociada a estas No Conformidades se podrán crear Acciones Correctivas, consiguiendo la trazabilidad necesaria. 8. Permite la gestión de Acciones Correctivas y Preventivas, su definición y relación con Incidencias, Problemas, Cambios y Entregas, No Conformidades, etc.

Gestión de empleados

Cuadro 21.



Incidencias

Cuadro 22.

ID	Nombre	Tipo	Estado	Fecha Registro	Servicios	Prioridad
120719162324	Discos de copias de seguridad sin capacidad de almacenamiento s	Incidente	Abierto	19/07/2012 16:23:24		Muy alta
120719162324	Incidente producido en la ampliación de la memoria.	Incidente	Abierto	19/07/2012 16:23:24		Alta
120719165601	Robo de Contraseñas	Incidente	Investigacion	09/07/2012 16:56:01		Alta
120315165106	Incidente de Continuidad	Incidente	Abierto	15/03/2012 16:51:06		Muy baja

Cuadro 23.

CATEGORÍA	DESCRIPCIÓN
AUDITORÍA	1. Brinda soporte para automatizar las Auditorías del cumplimiento a evaluar, permitiendo accesos rápidos a: - Generación de Planes de auditoría, y programas de auditoría - Revisiones de los Planes - Control de los papeles de trabajo - Documentaciones de Eventos - Realización de informes de auditoría

Ejemplo de auditoria

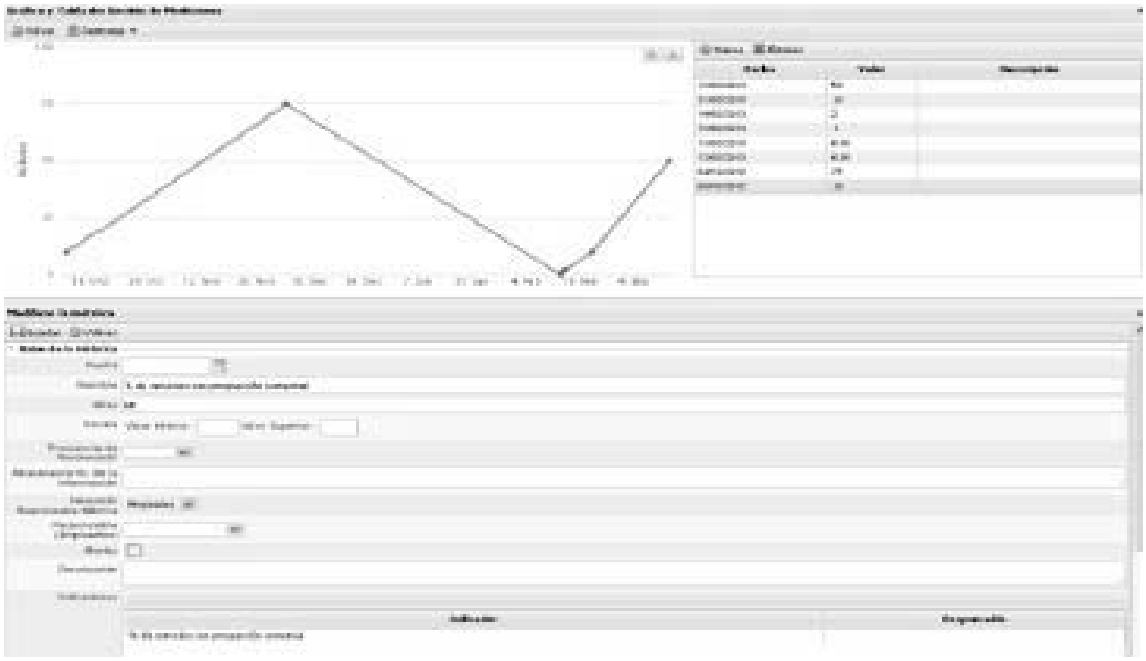
Cuadro 24.

Cuadro 25.

CATEGORÍA	DESCRIPCIÓN
MÉTRICAS E INDICADORES	1. Brinda una interfaz personalizable de Indicadores y Métricas. 2. Permite el Control y Seguimiento de los objetivos. 3. Propone indicadores que se alimentan automáticamente de otras opciones de la herramienta. 4. Indicadores automáticos a partir de la asignación de métricas para su cálculo. 5. Brinda la posibilidad de enlazar dichos indicadores y métricas con los objetivos estratégicos de la organización a través del módulo BSC (Balance ScoreCard). 6. Visualización del mapa estratégico de la organización a través de objetivos, indicadores y métricas.

Métricas

Cuadro 26.



Cuadro 27.

CATEGORÍA	DESCRIPCIÓN
GESTORES	1. La herramienta cuenta con un gestor documental que estructura la documentación por cláusulas y procedimientos y con un control de versiones. Dispone de capacidad ampliable y estructura modificable en función de las necesidades de negocio. 2. Permite la elaboración de Actas de reunión, destacando el registro de acciones del Comité de Seguridad, envío automático de actas a todos los asistentes y el archivo directo en el gestor documental.
NOTIFICACIONES	1. Permite notificaciones a los miembros de los equipos de recuperación y personal de la organización o fuera de la organización, y a través de diferentes medios de comunicación. 2. Permite la notificación automática a los responsables de los Planes en caso de revisiones y mantenimiento de los Planes 3. Realiza notificaciones para facilitar la gestión global del sistema.
REPORTES	1. Dispone de reportes genéricos que permiten visualizar la información relevante. 2. Permite la edición de reportes en formatos Word, Excel y PDF. 3. Dispone de interfaz para diseño de reportes a requerimientos del usuario. 4. Generación de Informes.
SEGURIDAD	1. Brinda flexibilidad a la hora de definir los perfiles de los usuarios de acuerdo a sus roles y/o responsabilidades. 2. Permite la integración con el Directorio Activo. 3. Permite el registro de las actividades de los diferentes usuarios. 4. Permite definir perfiles para el control documentario (desarrollador, ejecutor, revisor, aprobador) 5. Seguridad lógica de la herramienta.
INTEGRACIÓN	1. Permite la integración con otras fuentes de información de la organización, mediante diferentes mecanismos como Web Services, APIs, Import/Export de distintos tipos de archivos. 2. Permite la integración entre todas las herramientas de gestión que conforma GlobalSuite. 3. Entre las herramientas y plataformas incluidas para la integración cabe destacar: herramientas de monitorización (OSSIM), ticketing (REDMINE), CMDBs e inventariado de activos (OCS, CMDBBuilder, ATRIUM CMDB), cuentas de correo electrónico o sincronización con el Directorio Activo y LDAP.
ACCESIBILIDAD	1. Permite el acceso a través de diferentes medios, incluidos PCs, Laptops, Tablets, Smartphones. 2. Accesible desde cualquier soporte que tenga acceso a Internet y navegador Web.
LICENCIAMIENTO	1. Dispone de un esquema de licenciamiento competitivo a nivel de costo/beneficio y que brinda flexibilidad en la distribución de la aplicación en la organización. El licenciamiento se efectúa por empresa sin límite de usuarios, actividades, procesos, activos, etc.

Cuadro 28.

CATEGORÍA	DESCRIPCIÓN
FACILIDADES DE USO	1. La herramienta tiene sus paneles de opciones e información adicional en idioma Español. 2. Tiene un esquema intuitivo que asegura una mínima curva de aprendizaje. 3. Herramienta estructurada para seguir una secuencia lógica a la hora de implantar y mantener un sistema de gestión de continuidad de negocio. 4. La herramienta dispone de ayuda integrada en el propio entorno Web
ESCALABILIDAD FUNCIONAL	1. Permite adecuaciones a las funcionalidades del sistema de una forma eficiente en tiempos, costos y aprendizaje, según la necesidad del negocio en un momento determinado. 2. El software proporciona numerosas opciones de configuración para adaptar la funcionalidad a las necesidades del cliente a través de la propia interfaz web de la herramienta.
ESCALABILIDAD TÉCNICA	1. Permite una configuración que brinda una performance óptima de la aplicación a los usuarios. 2. Permite la instalación de la aplicación en configuración de Alta Disponibilidad en más de un Centro de Datos. 3. Manejar esquema de crecimiento de la plataforma tecnológica del sistema sin incurrir en costos y tiempos excesivos, según la necesidad del negocio en un momento determinado. 4. Posibilidad de monitorización en tiempo real del rendimiento y el estado de la plataforma tecnológica.
SOPORTE TÉCNICO	1. Cuenta con servicio de soporte remoto en caso de incidentes con la aplicación. 2. Permite el establecimiento de SLAs para la atención de solicitudes de soporte técnico en situaciones normales y en situaciones de emergencia o desastre.

2.3 Presupuesto

A continuación se muestra ejemplo de cuadro con el coste asociado al plan de trabajo descrito en la presente propuesta:

Actividad	Jornadas	Precio (€)
INICIO Y PLANIFICACIÓN	5	4.900 €
ANÁLISIS Y TRATAMIENTO DE CIBERRIESGOS	9	9.000 €
TOTAL	**14**	**13.900 €**

Observaciones:

- El plan de trabajo incluye tiempo presencial en las oficinas del Tomador/Asegurado y trabajo de gabinete en las oficinas del Bróker.

- Sobre los precios indicados se aplicará el tipo porcentual de IVA correspondiente a cada tipo de operación.

- Los precios NO incluyen gastos de desplazamiento, alojamiento y manutención del equipo del bróker.

- Forma de pago:
  - 50% al inicio de los trabajos
  - 50% a la finalización de los trabajos

- Los pagos se realizarán mediante talón o transferencia de acuerdo con las condiciones establecidas entre el Tomador/Asegurado y el bróker.

- Las posibles desviaciones que puedan producirse como consecuencia del no cumplimiento del plan de trabajo/cronograma por causas ajenas al bróker, serán abonadas en adición y al precio establecido por Jornada en este documento.

- Tanto la documentación como la información facilitada por el Tomador/Asegurado al bróker necesaria para el desarrollo del proyecto, serán tratadas con carácter confidencial. El bróker no reproducirá ni transmitirá a terceros ningún documento o información propia del Tomador/Asegurado sin su autorización expresa.

3. Ciber Seguro, solución al Ciber Riesgo

3.1. ¿Qué es el Ciber Seguro?

A principios del 2000, a raíz de la burbuja ‘’dot.com’’, algunas aseguradoras comenzaron a desarrollar un producto diseñado para hacer frente a la pérdida financiera que pudiera surgir de una violación de datos. Esta fue una época donde la mayoría de las empresas se beneficiaron del uso de internet con el fin de aprovechar el potencial económico del momento. En ese contexto, las aseguradoras vieron como clientes potenciales las grandes empresas "dot.com", como Amazon, Yahoo!, eBay, Google, etc., y otras compañías pioneras en el comercio electrónico. No obstante, el desarrollo de este nuevo producto no ha sido fácil, y sí difícil de convencer al propio consumidor para que acceda a su compra.

A lo largo de los años 90 y principios del 2000, la ausencia de datos actuariales confiables para calcular las primas, la falta de conciencia del consumidor en la contratación del seguro, la escasa demanda, así como los obstáculos jurídicos, han sido elementos claves en su desarrollo. Según han ido avanzando los años, la industria empresarial se ha visto obligada a estudiar su posible contratación. Básicamente, el ciber seguro tiene la finalidad de proteger a las empresas y usuarios individuales de los riesgos que provienen de internet, y más en general de los riesgos relativos a la información sobre las actividades tecnológicas. Los diferentes riesgos cibernéticos, por naturaleza, son excluidos de las pólizas de seguros generalistas, así como los seguros de responsabilidad civil general y todo riesgo daño material.

Dos hechos hicieron que este seguro creciera de forma exponencial:

En primer lugar, el 1 de julio de 2003, se aprobó en California la ley sobre notificación de la vulneración de las medidas de seguridad. Aunque se trataba de una ley de rango estatal, sus efectos se externalizaron a un amplio abanico de empresas. En virtud de dicha ley, toda empresa que diera a conocer de forma accidental o de cualquier otra forma "información personal" de cualquier residente de California, debía revelar este hecho a la persona afectada.

El Acta de Notificación de Violaciones a la Seguridad indicaba lo siguiente:

- La revelación de los datos puede realizarse en cualquier momento que se estime oportuno.

- Las compañías no pueden compartir los datos con sus filiales sin el consentimiento del consumidor.

Con esta ley se pretende asegurar de que el consumidor este informado de que sus datos están siendo recibidos por personas no autorizadas. La ley SB 1386 provee al consumidor del “derecho de actuación”, con el fin de presentar una demanda civil contra cualquier organización que no cumpla la ley. Esta medida legal de presión es única para este estado, ya que la mayoría de las demandas federales no proveen al consumidor del “derecho de actuación”.

Con la SB 1386 y la posterior aprobación de las leyes de notificación de otros 45 estados, se acabó con la práctica habitual de ocultar estas violaciones de seguridad. Se exigió a las empresas a incurrir en gastos directos significativos para investigar las violaciones de seguridad y cumplir con las leyes aplicables. Como resultado comenzó la presentación de gran cantidad de demandas colectivas después de la comunicación de grandes brechas de seguridad. Como tal, la cobertura del seguro cibernético pasó de ser una cobertura frente a un riesgo hipotético de futuras demandas, a una cobertura frente a un riesgo real. Además, poco después de la aprobación de la SB 1386 muchas pólizas de seguro cibernéticos comenzaron a incluir entre sus coberturas los costes directos asociados con el cumplimiento de las leyes de notificación, incluyendo honorarios de abogados , gastos de investigación forense, costos de impresión y envío, gastos de los call center, etc. ya que todos estos gastos de notificación son directos e inevitables, por lo tanto, independientemente del contenido de las demandas, una justificación económica directa para la cobertura del seguro cibernético ya existía.

El otro cambio, que se ha producido de manera gradual en el tiempo, pero que ha tenido un impacto significativo sobre la frecuencia y magnitud de las violaciones de datos, ha sido la aparición del crimen organizado en la red. A principios del año 2000, la piratería no era más que una pequeña molestia de unos pocos individuos. Los hackers de la época querían que se hablara de sus hazañas. Sin embargo, en nuestros días hablamos de verdaderos criminales, a los que se les ha abierto la posibilidad de realizar sus delitos a miles de km de distancia con casi ninguna posibilidad de ser descubiertos.

Por lo tanto, el mercado de seguros ciber es un mercado que está mucho más establecido. Empresas de todos los tamaños suscriben este tipo de pólizas ya que son conscientes de los riesgos de la red y empiezan a considerarlas una compra obligatoria. La fuerte competencia entre aseguradoras ha hecho que las primas disminuyan y por tanto sean accesibles a empresas de cualquier tamaño. Según datos extraídos de Willis, mediador de seguros, el número de clientes que ha suscrito el seguro de ciber a nivel mundial ha aumentado un 33% en 2014, respecto 2013, con los mayores incrementos en el sector servicios, con un 76%, y en educación, con un 72%, respectivamente. Con un mercado en pleno desarrollo, no es extraño encontrar innumerables ejemplos de compañías que ofrecen estas pólizas, como: Zurich, AIG, Chubb Insurance, ACE, Allianz Global, entre otras.

3.1.1. ¿Qué perfil tienen los clientes potenciales?

El abanico de potenciales clientes es enorme ya que cualquier entidad que almacene, manipule o transmita datos se encuentra expuesta al ciber riesgo así como a sufrir un robo de datos. A continuación haremos mención a aquellos sectores que se consideran más vulnerables:

Empresas de telecomunicación:

Procesan y transmiten gran cantidad de información personal y financiera a través de sus servidores. Son responsables de la seguridad de dicha información. De acuerdo a una Directiva Europea, en muchos países de la UE, como ocurre en España, las empresas de telecomunicación tienen la obligación legal de notificar cualquier violación en la seguridad de datos, lo que supone unos gastos de notificación elevados, además de incrementarse la probabilidad de recibir multas y/o sanciones administrativas y reclamaciones de terceros.

Si la empresa recoge y procesa transacciones con tarjetas de crédito, ha de cumplir con los requisitos específicos de la Industria de Medios de pago por tarjeta y sus medidas de seguridad (Payment Card Industry Data Security Standards).

Adicionalmente se enfrentan a la aparición de virus informáticos altamente sofisticados, con el riesgo de ver paralizada su actividad y sufrir una pérdida de ingresos fruto de dicha interrupción.

Empresas de Servicios:

Muchas empresas relacionadas con la gestión de energía han visto reducidos sus costes considerablemente gracias al control remoto y a los sistemas de monitorización lo que ha sumado a una práctica de seguridad precarias supone que su exposición al ciber riesgo se haya incrementado considerablemente. El estudio de KPMG sobre vulnerabilidad, estima que las empresas proveedoras de servicios son las más vulnerables al ciber riesgo debido a las particularidades del software de sus servidores web. Además, este tipo de compañías recogen centenares de miles de datos personales, incluyendo datos bancarios.

Hoteles y Ocio:

Estos sectores se encuentran expuestos a numerosos riesgos, entre los que se incluyen: responsabilidad en materia de seguridad y privacidad asociada a una base de datos de consumidores global vinculado a las ventas y reservas online; ataques de denegación de servicio por hackers y ciber terroristas; cumplimiento de la normativa relativa a la industria de tarjetas de crédito.

Las empresas basadas en franquicias deben asegurarse de que los franquiciados mantienen las normas de seguridad exigidas con el fin de proteger a la marca de cualquier daño reputacional asociado a un fallo en la seguridad de los datos o una violación de la privacidad.

Instituciones Financieras:

Las instituciones financieras representan uno de los sectores más atacados por los hackers y son las que padecen más violaciones de seguridad.

Poseen información personal relevante: nombres, números de teléfono, direcciones, detalles de tarjetas e historiales de crédito, además de otros datos financieros.

El crecimiento de la banca por internet y por teléfono móvil ha abierto el sector a nuevas amenazas de intrusión cibernética.

Son un blanco habitual para los hackers debido al volumen y el tipo de datos almacenados.

La actividad de hackers informáticos ha dado lugar a un aumento de ataques de denegación de servicio contra procesadores de pagos y otros servicios financieros.

Centros Educativos:

Recogen gran magnitud de información confidencial: números de tarjetas de crédito de los solicitantes, expedientes académicos, datos de proveedores, información contractual, datos de investigación y expedientes médicos. Gran cantidad de esta información se almacena en ordenadores portátiles y dispositivos móviles que viajan por el mundo con sus profesores, personal y estudiantes y pueden ser fácilmente extraviados. La creciente presencia de accesos remotos a los campus, redes sociales, programas académicos de gestión de transacciones y otros sistemas, contribuyen también al ciber riesgo. Con una rotación de empleados superior a la media y presupuestos anuales cada vez más reducidos, los centros se enfrentan al desafío de asegurarse de que todos los empleados están formados adecuadamente en las últimas políticas de gestión y tratamiento de datos. Los hackers los consideran objetivos sencillos y lucrativos al no contar normalmente con niveles altos de seguridad.

Comercios:

Los comercios tienen acceso a una gran magnitud de información de clientes incluyendo datos de identificación personal y números de tarjetas de crédito. Si por una parte las ventas online han crecido significativamente, estas páginas web son susceptibles de sufrir ciber ataques, lo que a la larga se traduce en una pérdida de ingresos debido a la caída de ventas.

El robo de datos de tarjetas de crédito se ha incrementado notablemente y puede afectar a cualquier comercio que acepte transacciones mediante este sistema de pago.

3.1.2. Análisis de mercado según los brókers

En 2013, Willis facilitó al mercado asegurador dos informes basados en encuestas sobre ciber riesgo. Fueron dirigidas a las primeras 1.000 organizaciones de mayor tamaño en EE.UU (lista Fortune 500 y Fortune 501-1.000). En ambos informes, sólo el 6% de las empresas revelaron que compran el seguro de ciber. Lo que representa, sin duda, una cifra muy reducida.

Durante 2013, las tasas de renovación para estas pólizas se mantuvieron generalmente estables. Willis informa que los aumentos fueron mínimos con un promedio de aumento anual de alrededor del 2% y 3% respecto al año anterior.

Según un análisis de Marsh & Mc Lennan, indica que la tendencia a adquirir ésta póliza va en aumento. Marsh señala que los recientes ataques cibernéticos en el mundo, la creciente preocupación de las organizaciones en mantener una buena imagen de marca, y la creciente vulnerabilidad de internet, parecen estar influyendo en las decisiones de compra. El número de clientes que compra este seguro, según Marsh, ha aumentado un 21% entre 2012 y 2013. Sectores como instituciones financieras y aquellos relacionados con servicios profesionales, aumentaron su nivel de compra un 13% en 2013 respecto a 2012. Industrias que representan a sectores emergentes para la compra cibernética, como la energía y los servicios públicos, también siguen una tendencia al alza.

3.2. Traslado al mercado asegurador: Solución Aseguradora

El Plan de Prevención descrito en el punto dos de la tesis va muy ligado a la Solución Aseguradora.

Previo a la adquisición de la póliza se realizan trabajos de consultoría y gerencia de riesgos, todo ello mediante una consultora y un mediador de seguros, que determinaran y/o detectaran los posibles riesgos a los que la empresa en cuestión puede estar expuesta.

Es importante recalcar que este ramo solo es comercializado por los considerados especialistas, no puede tratarse como un seguro tradicional, como pueden ser el de Daños Materiales o Responsabilidad Civil, entre otros.

El seguro de ciber carece de coberturas consideradas como ‘genéricas’, pero sí podemos mencionar las propias de este ramo.

Debe tenerse en cuenta que se trata de una síntesis del producto y que en cualquier caso las coberturas de este seguro se encuentran sujetas a los términos y condiciones de la póliza.

No todas las compañías aseguradoras que ofrecen este ramo de seguro dan cobertura a los mismos riesgos u ofrecen las mismas coberturas y limites, casi bien todas quieren diferenciarse una de las otras y ofrecen al mercado asegurador coberturas y límites diferentes. No obstante, a medida que pasa el tiempo y el seguro de ciber va siendo más conocido y se va desarrollando, la diferencia entre compañías puede quedar muy reducida.

¿Cuáles son las coberturas del seguro ciber?

Daños Propios

Perjuicios a terceros causados por la compañía:

- Gastos de notificación a los afectados (o a la autoridad reguladora) informando que los datos han sido expuestos como consecuencia de una violación de seguridad.

- Gastos de defensa si la empresa (o la empresa subcontratada que presta el servicio) causa una violación de seguridad en datos personales o industriales.

- Gastos de defensa en el caso de contaminar los datos o información de un tercero con un virus.

- Gastos de defensa si la empresa sufre un robo de hardware conteniendo datos de carácter personal.

- Gastos de defensa si un empleado divulga los datos de la empresa para la que trabaja.

Perjuicios financieros derivados del incumplimiento de la normativa de protección de dato:

- Gastos de asesoramiento jurídico y representación en relación con una investigación de la Agencia de Protección de Datos.

- Sanciones administrativas impuestas por la autoridad reguladora en materia de protección de datos personales.

Servicios de Consultoría

Expertos en consultoría informática para la empresa durante y después de sufrir una fuga de seguridad:

- Equipo de respuesta ante un incidente cibernético para asesorar al cliente en el caso de esta siendo *hackeado*.

- Asistencia de expertos al asegurado después de haber sufrido una violación de seguridad de sus datos para así restaurar sus sistemas y servidores de seguridad de manera que permitan volver al día a día de su negocio.

- Gastos de honorarios profesionales que se generen para determinar si los datos electrónicos pueden o no ser recuperados o restaurados.

Expertos consultores para restituir la imagen de la compañía tras haber sufrido una fuga de seguridad:

- Gastos de consultoría profesional para prevenir o minimizar los efectos adversos ante informaciones que pongan en duda los sistemas de seguridad de las redes a la hora de hacer frente a fugas de seguridad.

- Gastos de consultoría profesional para minimizar el daño potencial a la reputación de cualquier persona de la empresa.

Coberturas Opcionales

Pérdida de beneficios por los fallos en seguridad en las redes:

- Se cubre la pérdida del beneficio neto del asegurado que resulte de una interrupción material en sus redes como consecuencia de una violación de la seguridad.

Extorsión cibernética:

- Se cubre el pago de extorsión a terceros en el que se incurra con el fin de concluir una amenaza de seguridad.

Responsabilidad por actividades multimedia:

- Hacemos frente a los perjuicios y gastos de defensa incurridos en relación con una violación de la propiedad intelectual de un tercero, o actos negligentes en relación con contenidos digitales.

No obstante lo explicado anteriormente, hay otras compañías que ofrecen coberturas distintas y/o adicionales a las desarrolladas, como pueden ser:

Siniestros en la propia red

- Daños a activos digitales: costes de recabar de nuevo, recrear y restituir los activos digitales de un asegurado que hubieran resultado dañados o que hubieran sido destruidos, modificados, adulterados, distorsionados o robados o cualesquiera otros costes destinados a prevenir , mitigar o minimizar cualquier daño adicional.

- Pérdida de beneficio no tangible y coste incrementado del trabajo: pérdida de ingresos y gastos de interrupción de la actividad en los que el asegurado hubiera incurrido durante el periodo de restitución de la red directamente a resultas de la interrupción total o parcial de esa red, de la degradación del servicio o de fallos en la red informática.

RC de Privacidad y Seguridad

- RC de Responsabilidad de Terceros y Empleados: daños y perjuicios y gastos legales resultantes de una violación de la privacidad o de confidencialidad.

- RC de Seguridad: daños a terceros y gastos legales a resultas de un uso no autorizado, de la transmisión de un virus, de ataques de denegación de servicios y otros delitos informáticos.

Gastos de defensa, sanciones y fallos derivados de la normativa sobre privacidad:

- Investigación y defensa de la normativa sobre privacidad: gastos resultantes de la investigación, peritaje, defensa y apelación de procedimientos administrativos.

- Multas y sanciones administrativas por asuntos de privacidad: cuando sean asegurables por ley.

Gastos de crisis y Gastos reputacionales:

- Costes de emplear a peritos, expertos, y abogados en la investigación y respuesta de una violación de la privacidad o un fallo del sistema.

- Costes de notificación a las víctimas de infracciones de privacidad, costes de asistencia en asuntos de robo de identidad y costes de los servicios de RRPP para mitigar el daño reputacional.

3.3. Ejemplos de Reclamación

A continuación se detallan ejemplos de reclamación basados en situaciones reales que ilustran el espectro de coberturas.

Empleado Malintencionado: un empleado de una gran compañía de atención al consumidor roba información personal de millones de clientes.

Cobertura:

- Gastos de expertos especializados para determinar qué tipo de datos han sido robados a cada persona.

- Gastos de notificación de millones de personas cuyos datos han sido robados.

- Costes de control de identidad para los individuos afectados para asegurar que no siguen sufriendo pérdidas después del robo de información.

- Costes de un experto legal para preparar a la empresa ante una más que probable investigación por parte de la administración.

- Gastos de representación y defensa de la compañía ante reclamaciones de terceros.

- Pago de perjuicios e indemnizaciones a terceros por el daño causado.

Pérdida en manos de un tercero: el servidor de correo electrónico y el disco duro de una empresa son robados mientras se encuentran en posesión de un proveedor externo.

Cobertura:

- Gastos de expertos especializados para determinar qué tipo de datos han sido robados a cada persona.

- Gastos de notificación a las personas cuyos datos han sido robados.

- Gastos de control de identidad para los individuos afectados para asegurar que no siguen sufriendo pérdidas después del robo de información.

- Gastos de un experto legal para preparar a la empresa de cara a una más que probable investigación por parte de la Administración.

- Gastos de consultoría de Relaciones Públicas para aconsejar y guiar a la empresa en sus comunicaciones externas a los medios de comunicación.

Ataque *hacker* a una cadena hotelera: un grupo de hackers logra acceder a los sistemas informáticos de una cadena hotelera con varios establecimientos.

Cobertura:

- Gastos de expertos especializados para determinar qué tipo de datos han sido robados a cada persona (números de tarjetas de crédito e información personal de los titulares).

- Gastos de notificación a las personas cuyos datos han sido robados.
- Gastos de control de identidad para los individuos afectados para garantizar que no sigan sufriendo pérdidas después del robo.

- Gastos de un experto legal para preparar a la empresa de cara una previsible investigación por parte de la Administración.

- Consultoría de Relaciones Públicas para aconsejar a la empresa sobre cómo mitigar el daño reputacional después de lo sucedido.

Ataque *hacker* a procesador de datos: un sistema de procesamiento de pagos para tarjetas de crédito es *hackeado* comprometiendo los datos contenidos en las mismas.

Coberturas:

- Gastos de expertos especializados para determinar qué tipo de datos han sido robados a cada persona.

- Gastos de notificación a los millones de personas cuyos datos han sido robados.

- Gastos de control de identidad para los individuos afectados para garantizar que no siguen sufriendo pérdidas después del robo de información.

- Gastos de consultoría de Relaciones Públicas para asesorar sobre cómo mitigar el daño reputacional a la empresa después de producirse el siniestro.

- Gastos de un experto en seguridad de la información para preparar a la empresa de cara a una probable investigación por parte de la Administración.

- Gastos de representación legal y defensa ante las demandas que se presenten a la empresa.

3.4. Necesidad en la contratación del seguro

¿Es necesario contratar este tipo de pólizas? Después de los diferentes estudios llevados a cabo y de las consecuencias que puede conllevar un ataque cibernético para las empresas, creemos que sí es necesario, indistintamente a la industria a la que se pertenezca.

Volviendo a los ejemplos de incidentes anteriores, observamos cómo las consecuencias han tenido impactos sustanciales sobre los resultados económicos y en la imagen reputacional de éstas.

Hay industrias más vulnerables que otras, sobre todo aquellas que utilizan los sistemas informáticos para almacenar datos privados, o aquellas como la industria farmacéutica, por ejemplo, que almacena información confidencial para los posibles desarrollos de medicamentos. No obstante, aquellos sectores más vulnerables se han descrito en los puntos anteriores.
La contratación de la póliza de ciber seguro en España es relativamente escasa hasta la fecha.

La percepción de recibir un ataque informático es muy reducida, por eso mismo, este ramo se está introduciendo en el mercado español/europeo con cierta lentitud.

La mayoría de empresarios, sobretodo en España, coinciden en algunos aspectos relacionados con este seguro.

Todos, o casi todos, muestran un especial interés sobre este nuevo fenómeno, pero, ¿son realmente conscientes de las consecuencias que puede tener un

ataque ciber para la empresa? La realidad nos dice que no, por eso mismo escuchamos siempre los mismos argumentos, como pueden ser:

- ‘’no lo necesitamos – ya estamos asegurados’’
- ‘’no lo necesitamos – contamos con un potente sistema de seguridad’’
- ‘’no pertenecemos a un sector de negocio ‘’objetivo’’’’
- ‘’la póliza de seguro resulta muy cara’’
- ‘’no lo necesitamos – contamos con una infraestructura muy sólida’’
  ‘’no lo necesitamos – no estamos sujetos a regulaciones similares a EE.UU.’’
- ‘’no lo necesitamos – subcontratamos a nuestra seguridad’’
- ‘’somos demasiado pequeños para preocuparnos’’
- ‘’los gastos derivados de una fuga de datos hacen insignificante el coste de la póliza’’
- ‘’nunca he tenido una fuga de datos por lo que no necesito esta cobertura’’

Por lo contrario, en EE.UU, que es dónde nació el seguro de ciber, sí podemos decir que el ramo está más desarrollado y empieza a contratarse a gran escala. Los empresarios son muy conscientes de las consecuencias que puede tener un ataque informático para la organización.

3.5. El mercado del seguro ciber

Sólo las principales compañías del mercado ofrecen este tipo de seguro. Compañías como Zurich, ACE Group, AIG, Hiscox, Chubb Insurance, Mapfre, Allianz Global han sabido adelantarse a las demás y se han convertido en las principales pioneras en este ramo.

Podemos considerar el seguro ciber, actualmente, como el seguro de D&O (Seguro de Directores y Administradores) en sus inicios. Es decir, en el momento en que se empezó a vender el seguro de D&O entre las organizaciones, tan solo eran un porcentaje muy reducido los que lo contrataban. Actualmente, el mismo seguro, se ha convertido en un ramo ‘tradicional’ de compra entre las empresas, es más, casi todas las compañías aseguradoras ya venden este producto con condicionados y limites muy similares.

Por el momento, tal y como hemos mencionado en el punto 3.2, este seguro sólo lo comercializa gente especialista ya que se trata de un ramo relativamente nuevo.

4. Entrevistas

4.1. Amparo Zabala: Zurich

- ¿Qué evolución prevés del Seguro de CyberRisk para los próximos 5 y 10 años?

Las previsiones para el mercado de seguros de ciber riesgos son de crecimiento. Se estima una cifra de USD 10 billones en 2020. El mercado más importante parece que seguirá siendo el de Estados Unidos, pero en Europa estamos viendo un creciente interés en el producto. En España nuestros grandes clientes están comprando la cobertura. Clientes medianos o pequeños lo están valorando y es probable que muchos de ellos la compren en los próximos años.

- ¿Porque el Seguro de CyberRisk se dio a conocer dentro del mercado europeo hace escasamente 2 años (fecha aproximada)?

El seguro de ciber riesgos nació en Estados Unidos, donde se enfocó en dar respuesta a incidentes de privacidad, de pérdida de datos de carácter personal. Desde 2002, en la mayoría de los estados existen leyes en las que se obliga a las empresas a notificar a los afectados de la ocurrencia de una brecha de seguridad. La Comisión Europea empezó a iniciar el mismo camino 10 años después, en 2012, cuando comenzaron los trabajos para reformar la legislación en materia de protección de datos en la UE. Esta reforma debería finalizarse durante 2015. Probablemente esto y también la continua escalada de ataques cibernéticos sufridos por las empresas, contribuirán al desarrollo del ciber seguro en Europa.

- ¿Cómo prevés que irán las primas en los próximos años? ¿se mantendrán? ¿irán al alza? ¿a la baja?

Uno de los principales problemas de las aseguradoras es la falta de datos actuariales sobre los riesgos a cubrir. La mayoría de los aseguradores europeos toman como referencia de tarificación la experiencia americana, pero ésta sólo es útil hasta un punto, ya que Estados Unidos es un mercado muy diferente al europeo en litigiosidad y, por tanto, en nivel de primas. Entiendo que, como ocurre en el lanzamiento de cualquier producto asegurador nuevo, el transcurso del tiempo proporcionará la experiencia siniestral necesaria para tarificar los riesgos con una base actuarial más fiable. Otro factor a tener en cuenta es la oferta. Si hay mucha capacidad, las primas tienden a bajar.

En definitiva, creo que es pronto para pronunciarse en relación a la posible evolución de las primas.

- ¿El mundo empresarial es consciente de los riesgos cibernéticos que pueden padecer? ¿En EE.UU son más conscientes?

Se percibe una mayor sensibilidad de nuestros clientes con estos temas, aunque hay diferencias significativas entre clientes corporativos y las pequeñas y medianas empresas.

Las pymes se están sensibilizando cada vez más con estos temas, ya que están siendo objeto de ciberataques seguidos de extorsiones en los que se les solicita una cantidad de bitcoins a cambio de que el hacker desbloquee sus sistemas. Esto les preocupa principalmente desde el punto de vista de su propio negocio, pero no respecto a la posibilidad de que puedan ser la puerta de entrada a empresas más grandes, de las que son proveedores. Las grandes corporaciones, sin embargo, están incluyendo en sus análisis de riesgos cibernéticos a todos sus proveedores, no sólo a los de seguridad y sistemas informáticos, conscientes de que, como hemos comentado, el internet de las cosas está cada vez más extendido.

- ¿El Seguro de CyberRisk, al cabo de los años, se acabará incorporando en las pólizas generalistas de Daños y RC como ha sucedido con otros ramos? ¿Qué piensas?

No lo creo, aunque sí veo factible que evolucione para cubrir los huecos de cobertura que estos ramos más tradicionales tienen en relación al mundo tecnológico. Igualmente, creo que se estudiará cómo interacciona el seguro de ciber riesgos con otros con otros de líneas financieras, como D&O o BBB, y se adecuará el producto a las necesidades detectadas.

4.2. Olivier Marcén: AIG

- ¿Qué evolución prevés del Seguro de CyberRisk para los próximos 5 y 10 años?

Preveo una evolución creciente y de manera considerable, sobretodo en Europa. Según las estimaciones del mercado, se prevén unos ingresos de 10 billones de USD en primas para 2020, a día de hoy son de 2 billones. El ciberriesgo está a la orden del día, es un riesgo latente y está causando un interés importante en España y Europa. Creo que el seguro ira creciendo a lo largo de los años. A día de hoy ya existen más compañías del mercado que lo ofrecen porque es un riesgo real.

- ¿Porque el Seguro de CyberRisk se dio a conocer dentro del mercado europeo hace escasamente 2 años (fecha aproximada)?

La primera compañía que lanzó este producto fue AIG en EE.UU. Sí es cierto que en Europa ha tardado en llegar, pero se ha convertido en un seguro muy

demandado entre los clientes, es un tema de actualidad entre los Risk manager y las conferencias de Davos. Está en la agenda de los CEO y preocupan a las empresas. En el último mes hemos hecho 1.000.000 € en primas.

- ¿Cómo prevés que irán las primas en los próximos años? ¿se mantendrán? ¿irán al alza? ¿a la baja?

No hay muchos datos actuariales para hacer cálculos exactos, pero cada vez se va teniendo más información. ¿Cómo irán? Irán en función de la siniestralidad, como siempre. Puede haber una sobrecapacidad ya que muchas compañías ofrecen este ramo. Sí es cierto que es complicado establecer un guion ya que es muy pronto, pero en los últimos años las primas se han mantenido o han bajado entre un 2% y 3%, respectivamente.

- ¿El mundo empresarial es consciente de los riesgos cibernéticos que pueden padecer? ¿En EE.UU son más conscientes?

Es curioso cómo están respondiendo las empresas, creo que positivamente. No obstante, sigue existiendo aquella sensación de 'a mí no me va a pasar'. La visión en general está cambiando y se es consciente de la evolución de los ciberriesgos a medida que van avanzando los años. A los CEO les preocupa mucho este tema. En USA son más conscientes, en muchos estados es obligatorio hacer público que has recibido un ataque por lo que se convierte en un riesgo de actualidad. En Europa, por otro lado, se está trabajando para aplicar la misma ley y que las empresas también hagan públicos sus ataques.

- ¿El Seguro de CyberRisk, al cabo de los años, se acabará incorporando en las pólizas generalistas de Daños y RC como ha sucedido con otros ramos? ¿Qué piensas?

Las pólizas actuales de Cyber dan cobertura a los daños ocasionados a terceros, a la pérdida de beneficio, daños propios, etc. Por lo que no me sorprendería que acabaran incorporándose en ramos como el de Daños o RC, puede ser. Actualmente, en la póliza de daños, hay coberturas que dan cobertura al terrorismo. No obstante lo dicho anteriormente, creo que hay que esperar unos años para ver cómo evoluciona, tal como he indicado en preguntas anteriores, creo que aún es pronto para dar una respuesta contundente.

4.3. Isabel Ribas: Chubb Insurance

- ¿Qué evolución prevés del Seguro de CyberRisk para los próximos 5 y 10 años?

El seguro de ciber crecerá de forma abismal en los próximos 5 y 10 años. Isabel considera que es un riesgo emergente y la percepción del riesgo en España, en particular, está aumentando. Sí es cierto que la percepción está

aumentando, pero de manera lenta. No obstante, en USA, la percepción es superior que la de Europa y aumenta con rapidez. Isabel añade que el riesgo no se percibe hasta que sucede.

- ¿Porque el Seguro de CyberRisk se dio a conocer dentro del mercado europeo hace escasamente 2 años (fecha aproximada)?

Hace unos años la gente no era consciente de este tipo de riesgos. Según han ido avanzando los años, nos hemos ido introduciendo más en la era digital, por lo que hoy en día todo, o casi todo, se almacena en sistemas informáticos. Estos avances han propiciado que los ataques informáticos aumentaran exponencialmente, por lo que las noticias a través de la prensa también han ayudado a concienciar al empresario a ser consciente de este fenómeno.

- ¿Cómo prevés que irán las primas en los próximos años? ¿Se mantendrán? ¿Irán al alza? ¿A la baja?

En España hace 5 años las primas eran altísimas, algunas compañías aplicaban primas mínimas de 20.000 €. Con primas de 20.000 € nadie compraba el seguro. No obstante, las primas desde entonces han bajado mucho y lo continuaran haciendo, hoy en día puedes encontrar pólizas por 3.000 €. La poca percepción del riesgo cibernético también ha contribuido en la disminución de primas ya que la demanda era muy escasa y los empresarios no compraban la póliza, por lo que muchas compañías se vieron obligadas a disminuir hasta un 40% los precios respecto a los permitidos por su casa matriz en USA.

- ¿El mundo empresarial es consciente de los riesgos cibernéticos que pueden padecer? ¿En EE.UU son más conscientes?

No, y sí. Explico. Por un lado, como hemos comentado anteriormente, creo que el mundo empresarial aun no es del todo consciente de los riesgos cibernéticos, pero sí que esto está cambiando y el conocimiento va en aumento. ¿Si en EE.UU son más conscientes? Sí, lo son. El seguro de ciber nació en USA y allí las organizaciones son muy conscientes de los riesgos que pueden padecer.

- El Seguro de CyberRisk, al cabo de los años, se acabará incorporando en las pólizas generalistas de Daños y RC como ha sucedido con otros ramos? ¿Qué piensas?

Creo que sí pasará. Pienso que se acabará incorporando en la póliza de ‘’Crime’’ o BBB con algún sublimite.

4.4. Jose Luis Cort: Allianz Global

- ¿Qué evolución prevéis del Seguro de CyberRisk para los próximos 5 y 10 años?

Dada la baja contratación que existe actualmente (se estima que el volumen de primas de las pólizas de Cyber riesgos en el mercado europeo sea 150MM€) el potencial de crecimiento será muy elevado en los próximos años soportado por el incremento de incidentes en relación con cyber-ataques y a la elevada presión regulatoria.

Esta percepción se fundamenta además en que cada vez en mayor medida los gerentes de riesgos sitúan el cyber riesgo en las primeras posiciones de los riesgos que más les preocupan.

Según datos que manejamos en los próximos 3- 4 años el mercado de Cyber en Europa puede llegar a generar unos 700-900mm€ en primas.

- ¿Por qué el Seguro de CyberRisk se dio a conocer dentro del mercado europeo hace escasamente 2 años (aprox)?

La principal razón la podríamos encontrar en el anuncio sobre la modificación del marco normativo de la EU que se anunció en el 2012 y que está previsto entre en vigor en 2017.

Este nuevo marco viene a equiparar las responsabilidades que se establecen en la legislación americana por lo que de ella se deriva una agravación de la responsabilidad de las empresas por tratamiento de datos personales

- ¿Cómo prevéis que irán las primas en los próximos años? ¿se mantendrán? ¿irán al alza? ¿a la baja?

Las primas deberían de subir debido principalmente a:

- Incremento de cyberataques y sus ruinosas consecuencias para las empresas.

- Poca información actuarial sobre el riesgo cyber en el mercado europeo

- ¿El mundo empresarial es consciente de los riesgos cibernéticos que pueden padecer? ¿En EE.UU son más conscientes?

La percepción de las consecuencias económicas y legales derivadas de los riesgos cibernéticos en Europa es a día de hoy baja. En estadísticas que manejamos sólo un 24% de las personas encuestadas tiene una comprensión total de los riesgos cibernéticos a los que se expone su empresa.

Sin embargo, esta percepción del riesgo va sin ninguna duda en aumento. Los riesgos cibernéticos han pasado en el Risk Barometer de Alianz del puesto 12

al 3 en tan sólo un año y en una encuesta de Ponemon Institute el 40% de los encuestados sitúan a las consecuencias económicas derivadas de los ciber riesgos.

En US la percepción del riesgo es mucho mayor como demuestra el comportamiento del mercado de seguros que en actualidad cuenta con 1.3 billion USD y la contratación de este tipo de pólizas ha registrado un crecimiento del 80% en sólo 4 años.

- ¿El Seguro de CyberRisk, al cabo de los años, se acabará incorporando en las pólizas generalistas de Daños y RC como ha sucedido con otros ramos?

Yo diría que no debido a la naturaleza del propio producto que ha sido el motivo principal de su aparición en el mercado.

Los productos tradicionales no estaban diseñados para cubrir a los clientes ante riesgos cibernéticos en conceptos tan importantes para el aseguramiento como la pérdida de beneficios o la responsabilidad civil.

4.5. Alan Abreu: ACE Group

- ¿Qué evolución prevéis del Seguro de CyberRisk para los próximos 5 y 10 años?

Creo que en los próximos 5 años veremos la consolidación del producto como solución aseguradora, tomando en cuenta que hay cada vez una mayor conciencia de los riesgos que implica la economía y la vida digital. El factor clave para la evolución de este producto será la obligación de notificar los incidentes, y tal vez la posible obligación de indemnizar por los mismos. Hay escenarios que ven a Cyber, no como stand-alone póliza, sino como solución en los distintos productos existentes y futuros, siempre relacionado con la evolución que tenga IoT (“Internet de las cosas”) y otros factores. Los servicios adicionales, pre y post incidentes, tendrán una evolución importante.

- ¿Por qué el Seguro de CyberRisk se dio a conocer dentro del mercado europeo hace escasamente 2 años (aprox)?

Las condiciones de otros mercados, por ejemplo el de EE.UU, no se han dado en el mercado Europeo (aunque hay muchas diferencias entre países europeos). La obligación a notificar incidentes, como desde hace años lo se establece en EE.UU, y recientemente en Australia, además de la cultura de demandar, nos aleja del nivel de maduración de este seguro con respecto a otros mercados, aunque la evolución el último año ha sido importante.

- ¿Cómo prevéis que irán las primas en los próximos años? ¿se mantendrán? ¿irán al alza? ¿a la baja?

Si la siniestralidad se mantiene en niveles aceptables, muy probablemente como ha pasado tal vez con la D&O (una de las ultimas soluciones

aseguradoras creadas), la primas tenderán a bajar. Aunque no lo sé si tendremos la misma suerte.

- ¿El mundo empresarial es consciente de los riesgos cibernéticos que pueden padecer? ¿En EE.UU son más conscientes?

Hay cada vez más conciencia al respecto, los medios de comunicación y diversos estudios así lo confirman. El mercado de EE.UU, como antes indicaba tiene un mayor nivel de maduración. El 2016 y 2017 serán años claves para el mercado europeo.

- ¿El Seguro de CyberRisk, al cabo de los años, se acabará incorporando en las pólizas generalistas de Daños y RC como ha sucedido con otros ramos?

Es un escenario muy factible, que como decía anteriormente dependerá de la evolución, básicamente del IoT (“Internet de las cosas”).

5. Conclusiones

El importante auge de internet y el rápido progreso tecnológico ha permitido que empresas, instituciones, administraciones y usuarios almacenen toda su información en servidores de archivos gestionados por sistemas conectados a la red.

En los últimos años la ciber delincuencia ha pasado a tener cierta importancia en el mundo actual. Un ataque informático puede poner en peligro uno de los activos más importantes que atesora una empresa, ‘’la información’’. El mercado asegurador, por otro lado, cuenta con capacidad suficiente para cubrir los ciber riesgos o ciber ataques.

Disponer de un adecuado seguro para dar cobertura a los diferentes ciber riesgos o ciber ataques no es tarea fácil.

Solo especialistas del mercado asegurador suscriben este ramo; aquellos considerados profesionales altamente cualificados y con un dominio absoluto de la materia.

Al tratarse de un nuevo ramo, la información del mismo es escasa aunque el seguro está en proceso de expansión.

Debemos tener en cuenta que es imprescindible contar con un especialista en la materia al suscribir el seguro, considerando que los términos, condiciones, coberturas y límites de la póliza no son iguales en todas las compañías.

Debido al crecimiento de internet y de la digitalización, el cual se espera que siga creciendo de forma exponencial, las empresas, incluyendo todos los sectores, van siendo más conscientes de los riesgos y pérdidas que suponen los ciber ataques, por eso mismo se espera que el seguro de ciber siga creciendo en los próximos años.

6. Bibliografía

Artículos:

ASEGURANZA. Revista de los profesionales del Seguro y la Seguridad. ‘’El creciente fenómeno de las ciber amenazas en España’’. 01 Julio 2015

‘’Cyber Security & Risk Management’’ Annual Review, July 2015.

‘’Cyber Defense Strategy’’ March 2015.

‘’Thyber Ciber_Elcano_Num5’’ July 2015.

Informes:

WILLIS. ‘’BROCHURE_Cyber_Email_’’ Willis Limited. London.

INSURANCE INFORMATION INSTITUTE. ‘’Cyber Risks: The Growing Threat’’. June 2014.

AIG. ‘’Guía CyberEdge para mediadores de Seguros’’.

ZURICH. ‘’Cyber-Risk Report 2014. Zurich and Atlantic Council’’

AON ‘’La gestión de riesgos en la era digital’’

MARSH ‘’UK Cyber Security – The Role of Insurance In Managing And Mitigating The Risk’’

JLT ‘’Cyber & Technology Risks’’

Fuentes de internet:

Cyber Security Standards.
https://en.wikipedia.org/wiki/Cyber_security_standards#ISO_15408
(Fecha de consulta: 19 Febrero 2015)

Protecting Against Cyber Risk - A Primer on Cyber Insurance.
http://www.hklaw.com/PrivacyBlog/Protecting-Against-Cyber-Risk-A-Primer-on-Cyber-Insurance-01-15-2015/
(Fecha de consulta: 20 Marzo 2015)

Ciber riesgos: prevención y soluciones aseguradoras,
http://blogmapfre.com/mc-events/ciber-riesgos-prevencion-y-soluciones-aseguradoras/
(Fecha de consulta: 05 Julio 2015)

Ciber riesgos, nuevos retos a los que se enfrenta la industria aseguradora. https://www.redcumes.com/blog/2014/10/24/ciberriesgos-webinar/
(Fecha de consulta: 08 Junio 2015)

ACE Data Protect.
http://www.acegroup.com/es-es/empresas/cyber-risk-dataguard-comercio.aspx
(Fecha de consulta: 23 Marzo 2015)

Ciber seguros. El reto de transferir la inevitabilidad de la falla en un mundo digital y globalizado.
http://insecurityit.blogspot.com.es/2015/02/ciber-seguros-el-reto-de-transferir-la.html
(Fecha de consulta: 23 Agosto 2015)

Ciber Riesgos: el enfoque de Aon.
http://www.aon.com/spain/productos_servicios/consultoria-gestion-riesgos/ciber_riesgos.jsp
(Fecha de consulta: 16 Mayo 2015)

Revolución Tecnológica.
https://es.wikipedia.org/wiki/Revoluci%C3%B3n_tecnol%C3%B3gica
(Fecha de consulta: 16 Mayo 2015)

Treasury Troubled by Smaller Firms Not Buying Cyber Insurance.
http://www.insurancejournal.com/news/national/2015/02/18/357713.htm
(Fecha de consulta: 21 Mayo 2015)

Travelers Knows Cyber Insurance.
https://www.travelers.com/business-insurance/cyber-security/index.aspx
(Fecha de consulta: 28 Mayo 2015)

Companies Worried About Hackers Turn To Cyber Insurance.
http://www.npr.org/2015/03/19/393865187/companies-worried-about-hackers-turn-to-cyber-insurance
(Fecha de consulta: 02 Junio 2015)

Cyber security insurance: new steps to make UK world centre.
https://www.gov.uk/government/news/cyber-security-insurance-new-steps-to-make-uk-world-centre
(Fecha de consulta: 18 Marzo 2015)

Cyber Insurance 101: The Basics of Cyber Coverage.
http://www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-basics
(Fecha de consulta: 19 Marzo 2015)

CYBER & TECHNOLOGY INSURANCE.
http://www.lockton.com/cyber-and-technology
(Fecha de consulta: 29 Abril 2015)

Why cyber-insurance will be the next big thing.
http://www.cnbc.com/2014/07/01/why-cyber-insurance-will-be-the-next-big-thing.html
(Fecha de consulta: 22 Julio 2015)

cyber and privacy insurance.
http://www.irmi.com/online/insurance-glossary/terms/c/cyber-and-privacy-insurance.aspx
(Fecha de consulta: 11 Mayo 2015)

CyberEde.
http://www.aig.com/CyberEdge_3171_417963.html
(Fecha de consulta: 29 Junio 2015)

CyberSecurity by Chubb.
http://www.chubb.com/cybersecurity/
(Fecha de consulta: 12 Junio 2015)

CYBERSECURITY INSURANCE.
http://www.dhs.gov/publication/cybersecurity-insurance-reports
(Fecha de consulta: 14 Marzo 2015)

Cyber insurance.
https://www.abi.org.uk/Insurance-and-savings/Products/Business-insurance/Cyber-risk-insurance
(Fecha de consulta: 19 Marzo 2015)

Cinco errores comunes en ciberseguridad.
http://www.kpmgciberseguridad.es/cinco-errores-comunes-en-ciberseguridad/
(Fecha de consulta: 22 Mayo 2015)

SegurosTv.
http://blog.segurostv.es/tag/ciber-riesgos/
(Fecha de consulta: 28 Mayo 2015)

March JLT crea una nueva solución integral para empresas que cubre los riesgos de un ciber-ataque.
http://www.pymeseguros.com/march-jlt-crea-una-nueva-soluci%C3%B3n-integral-para-empresas-que-cubre-los-riesgos-de-un-ciber-ataque
(Fecha de consulta: 27 Marzo 2015)

Confirman ataque de hackers a cuentas de JPMorgan Chase.
http://www.laopinion.com/tecnologia-hackers-atacan-banco-jpmorgan-chase
(Fecha de consulta: 03 Marzo 2015)

Ataque cibernético a Home Depot afectaría a millones de clientes.
http://www.elnuevoherald.com/noticias/estados-unidos/article1992565.html
(Fecha de consulta: 03 Marzo 2015)

eBay es víctima de ataque cibernético.
http://www.cnnexpansion.com/tecnologia/2014/05/21/ebay-es-victima-de-un-ciberataque
(Fecha de consulta: 03 Marzo 2015)

Ashley Madison. Piratas informáticos publican los datos de usuarios de una web para infidelidades.
http://www.lavanguardia.com/tecnologia/internet/20150819/54435892537/piratas-informaticos-publican-datos-usuarios-web-infidelidades.html
(Fecha de consulta: 08 Agosto 2015)

Cyber Insurance: An Efficient Way to Manage Security and Privacy Risk in the Cloud?
http://www.infolawgroup.com/2012/02/articles/cloud-computing-1/cyber-insurance-an-efficient-way-to-manage-security-and-privacy-risk-in-the-cloud/
(Fecha de consulta: 05 Junio 2015)

The Top 5 Most Brutal Cyber Attacks Of 2014 So Far.
http://www.forbes.com/sites/jaymcgregor/2014/07/28/the-top-5-most-brutal-cyber-attacks-of-2014-so-far/
(Fecha de consulta: 26 Febrero 2015)

Ciber riesgo, una de las principales preocupaciones.
http://www.iberoamerica.net/colombia/prensa-generalista/elespectador.com/20150519/noticia.html?id=80qxJ21
(Fecha de consulta: 03 Julio 2015)

Ciber riesgo, una de las principales preocupaciones para empresarios.
http://www.elespectador.com/tecnologia/ciber-riesgo-una-de-principales-preocupaciones-empresar-articulo-560513
(Fecha de consulta: 24 Mayo 2015)

9 Recent Cyberattacks Against Big Businesses.
http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0
(Fecha de consulta: 30 Junio 2015)

Cyber Attacks on U.S. Companies in 2014.
http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014
(Fecha de consulta: 20 Abril 2015)

Ataques cibernéticos, un enemigo silencioso del que nadie está exento.
http://colombia-inn.com.co/ataques-ciberneticos-un-enemigo-silencioso-del-que-nadie-esta-exento/
(Fecha de consulta: 13 Junio 2015)

ATAQUES INFORMÁTICOS.
http://elpais.com/tag/ataques_informaticos/a/
(Fecha de consulta: 07 Junio 2015)

Microsoft y el FBI desactivan una red mundial de cibercrimen.
http://www.abc.es/tecnologia/noticias/20130606/abci-microsoft-cibercrimen-201306060945.html
(Fecha de consulta: 03 Marzo 2015)

Roban a Yahoo! datos de 22 millones de usuarios.
http://tecnologia.elpais.com/tecnologia/2013/05/20/actualidad/1369054770_786876.html
(Fecha de consulta: 03 Marzo 2015)

Los ciberataques sustituyen al terrorismo como primera amenaza para EE UU.
http://internacional.elpais.com/internacional/2013/03/13/actualidad/1363187707199021.html
(Fecha de consulta: 01 Abril 2015)

Atención al virus informático de moda: «Policía Nacional, páguenos 100 euros»
http://www.abc.es/espana/20130501/abci-atencion-virus-informatico-moda-201305011100.html
(Fecha de consulta: 18 Abril 2015)

Un ataque informático bloquea durante unos minutos la nueva web del Senado.
http://www.elmundo.es/elmundo/2012/11/12/navegante/1352742760.html
(Fecha de consulta: 06 Junio 2015)

LOS CIBER RIESGOS SUPONEN PÉRDIDAS MILLONARIAS CADA AÑO A LAS EMPRESAS.
http://www.abascalcomunicacion.com/los-ciber-riesgos-suponen-perdidas-millonarias-cada-ano-a-las-empresas/
(Fecha de consulta: 02 Junio 2015)

THE INSTITUTE OF RISK MANAGEMENT.
http://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/
(Fecha de consulta: 25 Mayo 2015)

RSA Conference 2015.
https://www.rsaconference.com/writable/presentations/file_upload/cxo-w03-can-cyber-insurance-be-linked-to-assurance.pdf
(Fecha de consulta: 22 Junio 2015)

An introduction to cyber liability insurance cover.
http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover
(Fecha de consulta: 27 Abril 2015)

INFOSEC INSTITUTE.
http://resources.infosecinstitute.com/cyber-insurance/
(Fecha de consulta: 23 Mayo 2015)

Marc Esteve Grau

Nacido en Barcelona, el 17 de febrero de 1989.

Licenciado en Administración y Dirección de Empresas (ADE) por la Universidad de Barcelona (UB) en 2012.

Inició, en 2010, su carrera profesional en Ambler Correduría de Seguros desarrollando tareas administrativas, comerciales y contables durante un periodo de 2 años.

En 2012 se incorporó a la entidad Willis S&Cc hasta la fecha de hoy, desarrollando y participando en diferentes proyectos en el departamento de Grandes Cuentas e Internacional.

COLECCIÓN "CUADERNOS DE DIRECCIÓN ASEGURADORA"

Master 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" 2009/20010

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 Caldés 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 Mª 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.- Mª 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 Guarner: “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.- Lluis 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 Muguerza 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.- Mª 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 Viciana 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 Texidó: “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 Rifá: "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 publico” 2009/2010

143.- José Angel Ansón Tortosa: “Gerencia de Riesgos en la Empresa española” 2011/2012

144.- María Mecedes 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 Costumer Experience as a Sorce 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.- Lluis 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 Siniestros 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.