Cuadernos de Dirección Aseguradora

312

Impacto del IoT en el Sector Asegurador

Máster en Dirección de Entidades Aseguradoras y Financieras

UNIVERSITAT DE BARCELONA

UNIVERSITAT DE BARCELONA

312

Impacto del IoT en el Sector Asegurador

Estudio realizado por: Joaquín Chertó Sancho
Tutor: Casimiro Rey Viñuela

Tesis del Máster en Dirección de Entidades Aseguradoras y Financieras

Curso 2022/2023

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

Presentación y agradecimientos

Quisiera agradecer en primer lugar a mis padres por guiarme en los primeros pasos de la vida. A mi esposa por estar siempre a mi lado en cada paso del camio poyarme en todo lo que hago, a mis hijas por ser mi fuente de energía diaria, y a todos mis familiares y amigos que han estado a mi lado siempre que los he necesitado

En segundo lugar, quiero agradecer a Riccardo Scotto por darme la oportunidad de formar parte del Grupo Catalana Occidente. También quiero agradecer a todos aquellos compañeros que en algún momento de mi trayectoria profesional me han formado, apoyado y orientado, su compañerismo ha sido fundamental para mi crecimiento profesional.

En tercer lugar, agradecer al Grupo Catalana Occidente la oportunidad de cursar la 21ª edición del Máster en Dirección de Entidades Aseguradoras y Financieras.

En cuarto lugar, expresar mi agradecimiento a Mercedes, Ferran y a todos los profesores que han impartido el Máster en Dirección de Entidades Aseguradoras, sus experiencias personales compartidas y conocimientos transmitidos durante las clases, sin duda me serán de gran utilidad en el futuro.

Por último, pero no menos importante, agradecer a Casimiro Rey el tiempo dedicado en la tutoría de la tesis.

Resumen

Las mejoras en la conectividad junto con el IoT y la Inteligencia Artifical, tendrán un impacto disrruptibo en el sector asegurador. Los procesos de selección de riesgos y pago de prestaciones cambiaran por completo. En consequencia, las aseguradoras podrán ofrecer productos altamente personalizadosy servicios orientados a la prevención. No obstante, esta mejora tecnologica planterá un desafio al sector asegurador debido al incremento de riesgo ciber en un entorno de baja oferta.

Palabras claves: Seguros personalizados, Prevención, Inteligencia Artificial, Industria 4.0., Conectividad, 5G, Mitigación riesgos, Tecnología de frontera, Bonos catastróficos,

Resum

Les millores en la connectivitat, juntament amb l'IoT i la Intel·ligència Artificial, tindran un impacte disruptiu en el sector assegurador. Els processos de selecció de riscos i pagament de prestacions canviaran completament. En consequència, les asseguradores podran oferir productes altament personalitzats i serveis orientats a la prevenció. No obstant això, aquesta millora tecnològica plantejarà un desafiament al sector assegurador a causa de l'increment de risc ciber en un entorn de baixa oferta.

Paraules clau: Assegurances personalitzades, Prevenció, Intel·ligència Artificial, Indústria 4.0, Connectivitat, 5G, Mitigació de riscos, Tecnologia fronterera, Bons catastròfics.

Summary

Improvements in connectivity along with the Internet of Things (IoT) and artificial intelligence are set to have a disruptive impact on the insurance sector. Risk assessment and claims payment processes will undergo radical change. As a result, insurers will be able to offer highly personalized products and prevention-oriented services. However, this technological improvement will pose a challenge to the insurance sector due to the increase in cyber risk in a low-supply environment.

Keywords: Personalized insurance, prevention, artificial intelligence, Industry 4.0., connectivity, 5G, risk mitigation, frontier technology, catastrophic bonds.

Índice

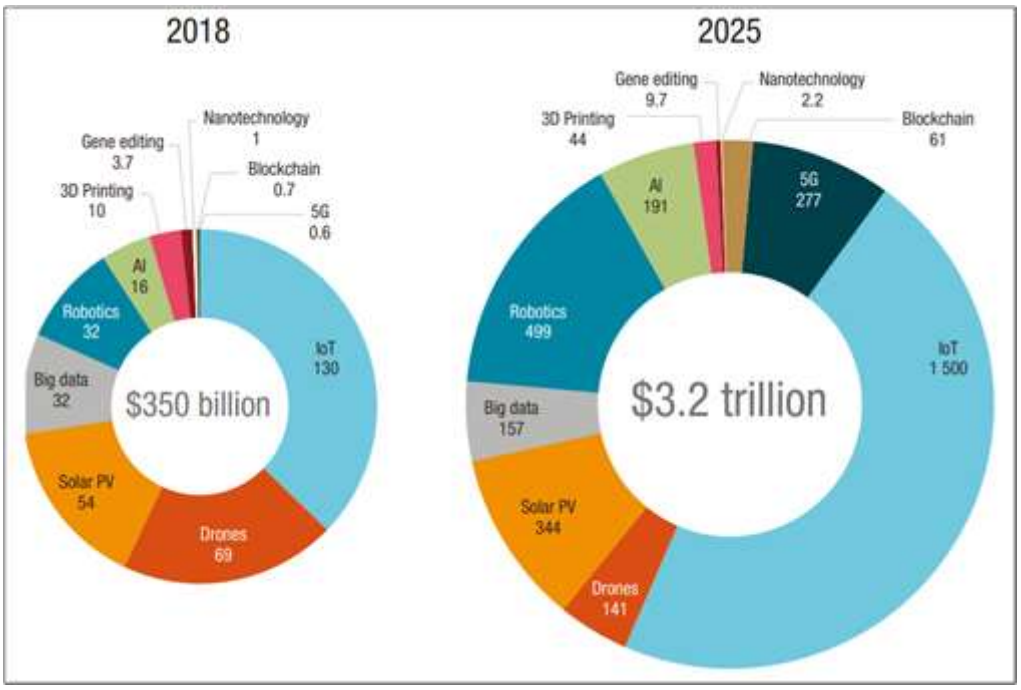
Impacto del IoT en el Sector Asegurador

1. Presentación del problema

El Internet de las cosas (IoT), es una tecnología que permite la interconexión y el intercambio de información en tiempo real entre dispositivos, máquinas y equipos. Este avance tecnológico está empezando a tener impacto en la industria y la vida cotidiana, y se espera que continúe haciendo en el futuro.

El IoT forma parte de las denominadas tecnologías de frontera, que son un grupo de tecnologías que aprovechan la digitalización y la conectividad para combinarse entre sí e incrementar su potencial. La siguiente gráfica presenta las estimaciones de volumen de negocio mundial de las tecnologías de frontera según el UNCTAD[1]

Gráfica 1: Estimación global del tamaño de mercado de las tecnologías de frontera.



Fuente: UNCTAD, Technology and Innovation Report 2021

[1] United Nations Conference on Trade and Development (UNCTAD), Technology and Innovation Report 2021

En los próximos años, se prevé que las tecnologías de frontera generen un gran número de oportunidades de negocio, se estima un volumen de negocio de hasta 3,2 trillones de dólares. Entre estas tecnologías, el IoT destaca como una de las que presenta un mayor potencial para aprovechar estas oportunidades.

El IoT ofrece innumerables oportunidades de mejora en la seguridad, en la atención médica, en la movilidad, en la eficiencia energética, en la optimización de los procesos productivos, en la domotización de las viviendas, y en un sinfín de disciplinas.

Hay que tener en cuenta que el IoT es una tecnología de reciente aparición que está evolucionando muy rápidamente, por consiguiente, hay que analizar en profundidad su potencial, aprovechar las ventajas que nos ofrece, analizar los riesgos que se puedan derivar de su implantación y proponer medidas para mitigarlos.

En mi opinión, este es uno de los grandes retos a los que se enfrenta la sociedad actual, todos los sectores productivos se verán impactados en menor o mayor mediada por este avance tecnológico, y el sector asegurador no será una excepción. Esto significa que los seguros tendrán que readaptarse para poder continuar satisfaciendo las necesidades de los clientes.

2. Antecedentes y evolución de la conectividad

Para comprender el contexto de conectividad actual y su potencial en el futuro es necesario realizar una mirada retrospectiva para ver cómo ha evolucionado esta tecnología.

Desde épocas inmemoriales los humanos hemos buscado sistemas para transmitir información de forma casi instantánea entre puntos distantes. Desde la antigüedad se han empleado las señales de humo y otros métodos para alertar de la presencia de peligros o transmitir información de relevancia, pero no se produjeron grandes avances en esta disciplina hasta el 1836 con la invención del telégrafo por parte de Samuel Morse, y el teléfono por parte de Antonio Meucci el 1854.

Paralelamente se estaban desarrollando sistemas de comunicación sin la necesidad de cables, en 1885 Heinrich Hertz descubrió la propagación de las ondas electromagnéticas, así como las propiedades de estas.

Las ondas electromagnéticas son una combinación de campos eléctricos y magnéticos que generan una onda oscilante capaz de trasladarse sin necesidad de ningún medio. En la atmosfera terrestre se desplazan a velocidades próximas a las de la luz, es decir, a casi 300.000km/s. Este descubrimiento sienta las bases de las comunicaciones inalámbricas. En 1900 Reginald Aubrey Fessenden efectúa lo que se considera la primea transmisión de radio con audio.

Los sistemas de comunicación basados en ondas electromagnéticos continúan evolucionando y el 1973 la empresa Motorola comercializa el Dyna TAC 8000X. Se trata del primer teléfono móvil, pesa 800 gramos, mide 33 centímetros de longitud y se comercializa un precio de 3.995 US$, más de 10.000€ al cambio actual, solo permite efectuar llamadas de voz y debido a su alto coste su uso muy limitado.

Fotografía 1. Martin Cooper efectúa primera llamada en público con el Motorola Dyna TAC 8000X.

Fuente: The Washington Post.

Las comunicaciones por cable también se continúan mejorando, en 1958 la compañía americana Bell consigue por primea vez en la historia transmitir datos entre dos ordenadores valiéndose de una línea telefónica de cobre, la transmisión es de solo unos pocos bits, (*dígitos binarios*). Sin embargo, el potencial de esta tecnología capta rápidamente la atención del Departamento de Defensa de los Estados Unidos y se crea el programa Arpanet. El objetivo de este programa era desarrollar una red de ordenadores capaz de soportar un ataque nuclear.

El programa tarda una década en desarrollarse, y consigue establecer una red de comunicación estable entre cuatro universidades a una velocidad de 50Kbits, 50.000 bits por segundo, posteriormente se continúa añadiendo ordenadores a la red y pasa a denominarse Internet.

Internet continúa centrándose en la comunicación entre universidades y centros gubernamentales, principalmente debido al alto coste de los ordenadores. No es hasta la década de los noventa, en la que las mejoras tecnológicas permiten el abaratamiento de costes fabricación de los ordenadores y estos se empiezan a implantar en las empresas y posteriormente en los hogares. Lo que significa la llegada de internet a miles de empresas y hogares.

Simultáneamente la telefonía móvil se continúa desarrollando, el 1991 aparece el estándar GSM, o también conocido como 2G, el estándar además de llamadas por de voz permite transmitir datos digitales, la velocidad de transmisión es de 9,6kBps (9,6 Kbits por segundo). Aparecen los SMS (Servicio de mensajes cortos) y MMS (mensajes multimedia).

El estándar GSM divide la zona geográfica en celdas, en cada celda se ubica una estación base, estas estaciones se conectan al centro de conmutación móvil (MSC) y a través de este se efectúa la conexión a la red cableada de telefonía e internet. Las bandas de frecuencia que se utilizan en Europa son la 900MHz y 1.800MHz.

Cada estación base puede soportar un determinado número de dispositivos, si se supera el límite, el ancho de banda se satura y se producen interferencias. El tamaño de las celdas se determina en función de los dispositivos a los que tiene que dar servicio la estación base, en consecuencia, en las zonas con alta densidad de dispositivos las celdas serán más pequeñas.

Al estándar 2G le sigue el 3G, o red de cuarta generación, las frecuencias que utiliza se corresponden con las bandas 900MHz y 2,1GHz (2.100MHz). Este estándar permite realizar simultáneamente llamadas se voz y transmisión de datos. La velocidad de transmisión de datos puede alcanzar velocidades de hasta 2Mbits por segundo, Esta mejora tecnología permite navegar por internet con fluidez con el teléfono móvil.

Paralelamente las conexiones mediante cableado también han evolucionado, las instalaciones de cable de cobre han quedado obsoletas y aparece la fibra óptica.

Los cables de fibra óptica están formados por un hilo muy fino de material transparente, normalmente vidrio, el cual se recubre con un material opaco. Por el interior del cable se transmiten pulsos de luz que representan los datos que se transmiten. En el 2023 es posible disponer de velocidades de carga y descarga de hasta 300Mbits por segundo en el ámbito empresarial y doméstico. Todavía es una tecnología que está en desarrollo, pero tiene un alto potencial, en 2020 un grupo de investigadores de la Universidad de Nonash (Australia) obtienen una velocidad de transmisión récord de 44Terabits por segundo.

Empieza a tener importancia la latencia de la red, o retraso en la comunicación de la red, es un indicador del tiempo que tardan los datos en transferirse a través de la red. Es decir, mientras que el ancho de banda hace referencia a la cantidad que datos que se pueden enviar por segundo, la latencia hace referencia al tiempo total que necesitan los datos para llegar desde un emisor a un receptor, normalmente se miden en milisegundos. En consecuencia, contra más baja sea la latencia más rápida, y de mayor calidad será la comunicación multidireccional entre los dispositivos conectados.

Para tener una referencia del orden de magnitud, latencias de 100 milisegundos permiten realizar video llamadas de poca calidad, con retrasos y con imágenes pixeladas. Cuando la latencia es inferior a los 40 milisegundos puede establecerse una video llamada de calidad, para jugar a juegos en línea con un entorno grafico complejo, se necesitan latencias de 20 milisegundos. En el 2023 es posible disponer de conexiones de fibra óptica con latencias de hasta 12 milisegundos tanto en el ámbito industrial como en viviendas.

El 4G, LTE o red de cuarta generación, supone el siguiente paso evolutivo tras la tecnología 3G. Utiliza las bandas de frecuencia 800MHz, 2.6GHz Las velocidades de descarga pueden llegar a los 100Mbps y las de subida a 50Mbps, la latencia media se situ en 100 milisegundos.

El 5G es la siguiente generación de estándares de comunicación y es una evolución del 4G/LTE. Se basa en tres bandas de frecuencia distintas: 700 MHz, 3,5 GHz y 24-100 GHz. La banda de 700 MHz o de baja frecuencia proporciona una amplia cobertura gracias a su capacidad para penetrar paredes, pero ofrece velocidades de transmisión de solo 100 Mbps. La banda de 1,8 GHz o de frecuencia media, brinda una cobertura moderada, pero es más susceptible a las interferencias debido a su limitada capacidad de penetración de paredes, puede ofrecer velocidades de 1 Gbps (1.000Mbps). La banda de 24-100 GHz o de alta frecuencia brinda una cobertura corta, no puede atravesar edificios, pero ofrece velocidades de hasta 10 Gbps (10.000Mbps)

La banda de alta frecuencia es la que ofrece las mayores velocidades de transmisión, pero también es la más susceptible a las interferencias. Pequeños obstáculos como árboles, personas o la lluvia pueden debilitar la señal, por lo que para lograr velocidades de 10 Gbps, es necesario tener una línea de visión directa entre el dispositivo y la antena transmisora. No obstante, en la práctica, se utiliza con mayor frecuencia la banda de 1.8 GHz o frecuencia media, que pese a tener un ancho de banda más limitado, es menos propensa a las interferencias.

Lo que distingue realmente el estándar de sus predecesores no es tanto su ancho de banda de transmisión, sino su baja latencia, el valor teórico se sitúa en aproximadamente 2 milisegundos.

En la práctica, esto significa que para visualizar una fotografía o un video almacenado en la nube se tardara el mismo tiempo que si estuviesen guardalados en la mejoría interna del móvil.

También permite la realización de cirugías teleasistidas, en las que el médico a distancia controla por 5G un brazo robótico que se encuentra en la sala de operaciones. La primera prueba con éxito se realiza el 8 de enero de 2019 en Fujan (China), un doctor situado a 50 kilómetros de distancia del quirófano realiza una lobectomía hepática completa a un perro.

Mientras en el 2023 la tecnología 5G está en pleno despliegue, la investigación sobro las tecnologías que el sucederán ya se ha iniciado. Para llevar a cabo la evolución del estándar de comunicación, se requiere desarrollar materiales más avanzados. Estos materiales deberían de ser capaces de trabajar a frecuencias mucho más elevadas, se requieren frecuencias de 95GHz a los 3THz, lo que permitiría alcanzar velocidades de transmisión teóricas hasta diez veces más rápidas que las del 5G, y con latencias de microsegundos.

Las mejoras en la conectividad implican que la cantidad y complejidad de los datos generados augmente año tras año. Para tener un orden de magnitud, según Statista, la estimación de datos generados en 2018 es de 33 Zettabytes (33.000 millones de Terabytes), para el año 2035 se prevé que esta esta cantidad alcance los 2.142 Zettabytes.

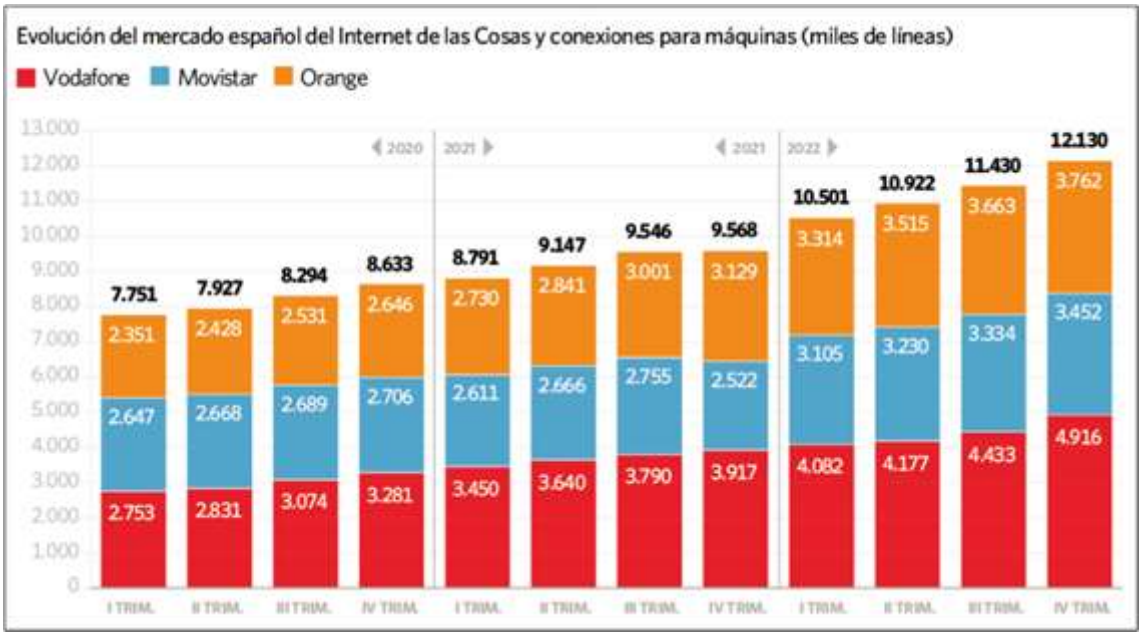
El 5G está orientado a aplicaciones que requieran un elevado ancho de vanada, pero no todos los dispositivos necesitan transmitir tanto volumen de información con latencias bajas. Para estos dispositivos se ha desarrollado el NarrowBand-Internet of Things (NB-IoT) o Low Power Wide Area (LPWA), las principales ventajas que ofrece esta tecnología es el bajo consumo energético y un amplio rango de cobertura, ya que utiliza bajas frecuencias, y estas se ven menos interferidas por los obstáculos. Los dispositivos podrían tener hasta autonomías de hasta 10 años.

El NB-IoT, el 5G y las redes de telecomunicaciones satelitales ya se están empezando a interconectar, en julio de 2022, Telefónica Tech anuncia que en colaboración con Sateloit, operador de telecomunicaciones satelitales, desarrollará durante los próximos años un sistema de tecnología dual 5G – NB-IoT para ofrecer conectividad con estos nuevos estándares. Se prevé que esta tecnología permita implantar soluciones basadas en IoT en cualquier punto del territorio, podrá ser de especial interés en aplicaciones de agricultura, transporte marítimo y movilidad terrestre entre otros.

En Mobile World Congress del 2023 las principales compañías de telefonía del mundo anuncian la creación de la GSMA Open Gateway. Este nuevo estándar permitirá la integración de las redes de telecomunicaciones en la nube. Las API (interfaz de programación de aplicaciones) desarrolladas bajo este estándar serán estándares, interoperables y universales. En otras palabras, que los estándares de comunicación entre softwares de las aplicaciones serán estándares, de código abierto y las empresas de telecomunicaciones servirán como plataforma de alojamiento del servicio.

El número de líneas M2M (Machine to Machine) que son las líneas de telefonía móvil que principalmente se emplean para intercambiar datos entre dispositivos IoT continúa creciendo. En el 2022 se observa un incremento del 26% respecto al mismo periodo del año anterior, y se espera que estas tendencias se mantengan en los próximos años.

Gráfica 2: Evolución de las conexiones M2M, principales operadoras mercado español.



Fuente: elEconomista.es [2]

La administración también está contribuyendo activamente en la transición digital de la sociedad, especialmente después de la pandemia. Para muchos países es un objetivo estratégico.

En este sentido, la UE lanza el Plan Next Generation UE para impulsar la reactivación económica y social de los países de la unión. El plan supone una inyección de 750.000 millones de euros durante los próximos 6 años, una de las principales prioridades es apoyar la transición digital.

Para lograr este objetivo, la administración está trabajando en la creación de un marco regulatorio que propicie la innovación y el desarrollo tecnológico. También se están llevando a cabo políticas y programas orientados a fomentar la digitalización de las empresas, la mejora de la conectividad de la ciudadanía.

En este entorno de alta conectividad y con el soporte de la administración, se generan las condiciones necesarias para la disrupción del IoT o internet de las cosas, en los próximos años tendremos miles de millones de dispositivos conectados a internet. Esto significa que tanto objetos de uso diario como zapatillas, cafeteras, lavadoras, vehículos, o cualquier máquina que intervenga en cualquier proceso industrial podrá estar conectada a internet e intercambiar datos con otros objetos.

---

[2] elEconomista.es, Vodafone manda en el 'Internet de las Cosas' con cinco millones de líneas (eleconomista.es)

3. Gestión de los datos generados por IoT

3.1. Inteligencia Artificial y IoT

El IoT supone que millones de objetos dotados de sensores constantemente recopilen datos del entorno que los rodea para posteriormente reportarlos.

No hay ninguna duda de que la cantidad, complejidad y tamaño de los datos que se generarán continuará aumentado, la capacidad de los sistemas de tratamiento convencionales en este nuevo entorno cada vez estará más limitada.

El internet de las cosas sin una correcta gestión de los datos no supondrá una gran revolución, se necesita un motor o cerebro capaz de almacenar, ordena, gestionar e interpretar los datos. Para solventar el problema es preciso la utilización de lo que se conoce como Big Data y AI (Inteligencia Artificial).

El término Big Data se utiliza para referirse a la gestión de grandes cantidades de datos, de amplia variedad y alta velocidad de transferencia, que debido a su magnitud y diversidad no pueden ser recopilados y procesados mediante métodos convencionales

Los datos que se recopilan a través del IoT pueden ser muy variados, pero principalmente se clasifican en datos estructurados y no estructurados. Los datos estructurados son los que proceden de grandes bases de datos, mientas que los no estructurados provienen de la confluencia de pequeñas fuentes como correos electrónicos, videos, webs visitadas, IoT, redes sociales, hábitos de consumo etc…

Los millones de datos recopilados para ser útiles tienen que poder ser analizados adecuadamente. Hay que tener en cuenta que es posible que una parte significativa de los datos solo sean de interés si pueden ser tratados en tiempo real. Por lo tanto, es necesario que las latencias entre los puntos de recolección y los puntos de tratamiento o análisis sean muy bajas.

Otro aspecto que es necesario considerar en Big Data es lo que se conoce como calidad del dato, los principales criterios que definen la calidad del dato son la completitud, validez, integridad puntualidad, disponibilidad unicidad, exactitud y consistencia.

El concepto Big Data está necesariamente ligado a la Inteligencia Artificial. Los sistemas de AI están basados en algoritmos que tienen la capacidad de mejorar su rendimiento en base a la experiencia acumulada. El aprendizaje se realiza en base al método de prueba error.

Los algoritmos de la AI son esencialmente algoritmos predicativos que alimentados por un gran volumen de datos son capaces de analizar millones de combinaciones y ofrecer como solución la más probable entre las posibles.

Cuanto mayor es el volumen y la calidad de los datos que alimenta la AI más combinaciones puede evaluar el sistema y más fiables serán los resultados arrojados.

Las técnicas de aprendizaje de las AI se pueden categorizar en tres grandes grupos, Deep Learning, Aprendizaje por refuerzo y optimización, y Procesamiento del Lenguaje Natural.

Los algoritmos de Deep Learning realizan repetitivamente una tarea para mejorar gradualmente el resultado, lo que permite ofrecer en cada iteracion soluciones más optimas. El aprendizaje se realiza sin supervisión. Sus aplicaciones prácticas pueden ser análisis avanzado de imágenes y audios, predicción de patrones de comportamiento, soporte a los vehículos autónomos etc.

Los algoritmos de Aprendizaje por refuerzo y optimización son sistemas de aprendizaje supervisados. El objetivo es el desarrollo de un sistema que mejora su eficiencia en base a la interacción con su entorno, su comportamiento se adapta en base a un sistema de inputs que le indican como de bien o mal está realizando la acción.

Tienen aplicaciones en la conducción autónoma, por ejemplo, Tesla está utilizando esta tecnología para determinar la distancia de los obstáculos y el comportamiento probable de los otros vehículos y tomar decisiones en tiempo real.

Google también utiliza esta tecnología para reducir el consumo energético de los sistemas de refrigeración de sus centros de datos. Analizando cada cinco minutos la información que le reportan miles de sensores ubicado en los servidores puede predecir los consumos y ejecutar acciones que le permiten minimizar el consumo energético. En promedio se han obtenido reducciones del consumo energético del 30%.

Los algoritmos de procesamiento del lenguaje natural se ocupan de la interacción entre los ordenadores y los humanos usando el lenguaje natural, pretenden integrar los idiomas humanos en los sistemas de computación. No solo pretenden comprender el significado de las palabras o las frases, sino el significado global del texto o discurso. El lenguaje humano está lleno de ambigüedades y palabras con significados distintos según el contexto, esto implica que estos algoritmos sean de los más complejos.

Las aplicaciones de esta tipología de algoritmos se pueden aplicar a resúmenes de textos, ChatBots, generación de textos automática, clasificación de textos, traducción de textos a otros idiomas o a audio etc.…

La AI se podría asimilar al “cerebro” que analiza y ofrece soluciones coherentes y lógicas a partir de los datos recopilados por los sensores del IoT. El Big Data es la información que fluye bidireccionalmente entre estos y les permite interactuar en tiempo real.

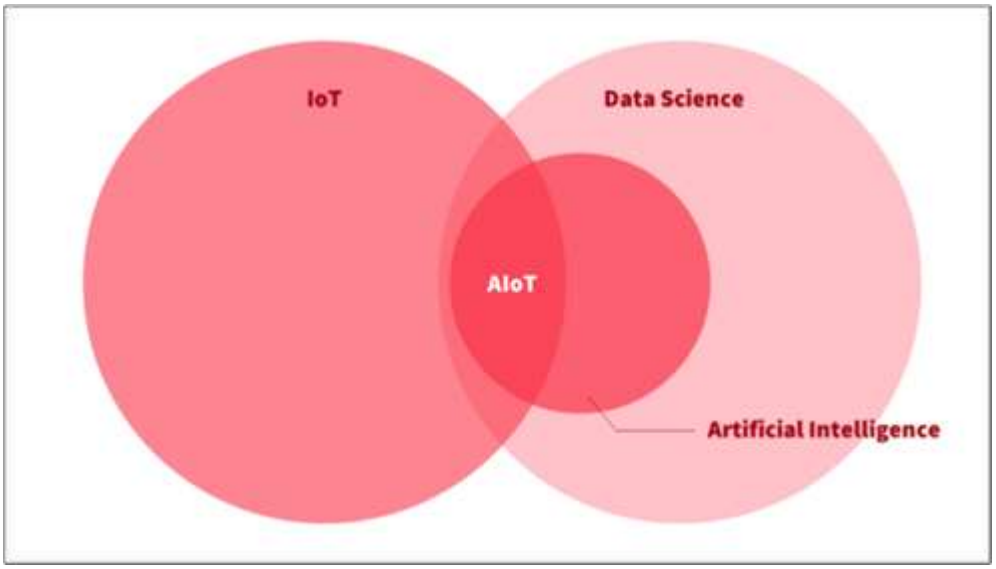
El potencial del Internet de las Cosas y las Inteligencias Artificiales solo se pueden aprovechar si actúan conjuntamente, por separado su potencial es muy limitado.

Ambas tecnologías necesitan unos niveles de desarrollo similares para funcionar como es de esperar. Actualmente el nivel de desarrollo de las AI va por detrás del IoT, se requieren ordenadores con mayores capacidades de procesamiento para tratar el alto volumen de datos que se generan. Las tecnologías basadas en la computación cuántica podrían ser una solución, pero actualmente todavía están en fase de desarrollo y se enfrentan a muchos retos.

3.2. AIoT – Inteligencia Artificial de las cosas

La combinación del potencial del AI (Artificial Inteligencie) y del IoT (Internet of Things) da lugar a un concepto que va mucho más allá, es el AIoT (Artificial Intelligence of Things). Esta tecnología pretende dotar a los dispositivos IoT la capacidad de analizar situaciones y tomar decisiones autónomas basadas en Inteligencia Artificial.

Gráfica 3: AIoT, la convergencia entre Inteligencia Artificial y IoT



Fuente: Barbaraiot.com, AIoT: la unión perfecta entre la Inteligencia Artificial y el IoT

En el AIoT, los datos se tratan en la fuente de origen, sin que sea necesaria la transferencia a servidores remotos. Esta tecnología presenta varias ventajas significativas.

En primer lugar, al analizar los datos en su lugar de generación, se resuelven los problemas de latencia, lo que se traduce en respuestas más rápidas. Esto resulta especialmente interesante en aplicaciones que requieren toma de decisiones en tiempo real, como la conducción autónoma.

Además, proporciona mayor fiabilidad, ya que no depende de una conexión constante con un servidor remoto. Los sistemas AIoT no se ven afectados por fallos de conectividad con la nube, lo que asegura que las aplicaciones sigan funcionando incluso en entornos con conectividad limitada o inestable.

Por otro lado, al mantener los datos en su fuente de origen, se mejoran aspectos relacionados con la privacidad y la seguridad. Al evitar la transferencia de datos a través de la red, se reduce el riesgo de exposición a posibles amenazas o brechas de seguridad.

3.3. AI y computación cuántica

Los sistemas de computación convencional utilizan como unidad básica de cálculo el bit, es un sistema binario que solo puede adoptar un valor al mismo tiempo, o cero o uno. En la computación cuántica la unidad básica de información es el qubit, la principal diferencia es que puede superponer simultáneamente ceros y unos, puede adoptar los dos estados al mismo tiempo, ya demás en distinta proporción. La multiplicidad de combinaciones que puede adoptar un solo qubit son muchísimas.

Para tener un orden de referencia, un ordenador cuántico de 30qubits puede realizar determinadas operaciones 5,8 billones más rápido que cualquier ordenador doméstico. El IBM Osprey de 433qubits es uno de los más potentes que actualmente existen.

La computación cuántica también plantea muchas dificultades, durante la fase de cálculo cuántico, la más mínima interferencia, como por ejemplo un fotón o una onda electromagnética provocan un error, lo que se conoce como descoherencia.

Se tienen que continuar mejorando el desarrollo de sistemas para detectar y aislar las descoherencias, dado que un único error puede invalidar la totalidad de la computación, además los datos calculados también pueden ser alterados cuando son observados.

Las condiciones de operación tienen que estar muy controladas, requieren entornos de vacío atmosférico, temperaturas ambientales próximas al cero absoluto (-273ºC) y ser aislados de las interferencias de cualquier radiación magnética o electromagnética, incluido el campo magnético terrestre.

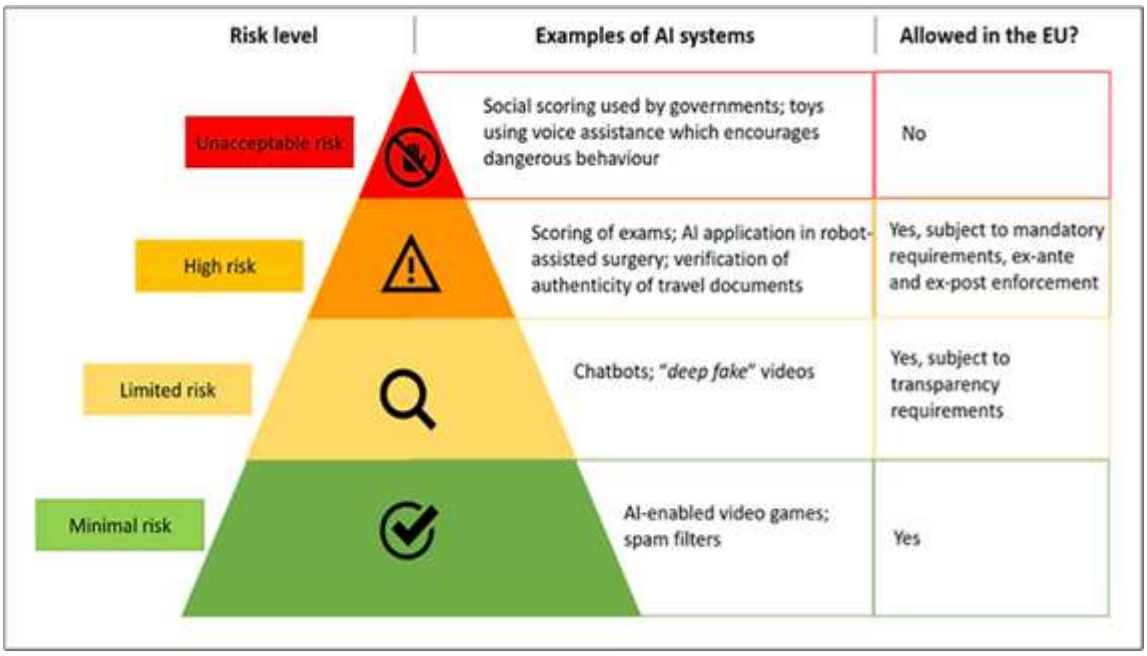
Superadas las dificultades planteadas, el poder computacional cuántico podrá ser utilizado para mejorar los procesos de optimización o aprendizaje de los algoritmos de la IA.

3.4. Regulación de la AI en la UE (AI Act.)

En abril de 2021, la Comisión Europea propone la regulación de la Inteligencia Artificial con el objetivo de garantizar que los sistemas utilizados en la Unión Europea sean seguros y respeten los derechos fundamentales y los valores de la UE. Esta propuesta, conocida como AIA (AI Act)

La Comisión Europea ha propuesto una clasificación de riesgos asociados a la inteligencia artificial en cuatro niveles: riesgo mínimo, riesgo limitado, riesgo elevado y riesgo inaceptable. Esta clasificación se utiliza como base para la regulación propuesta de la IA. La tabla siguiente muestra la clasificación de riesgos.

Cuadro 1: Esquema GRC



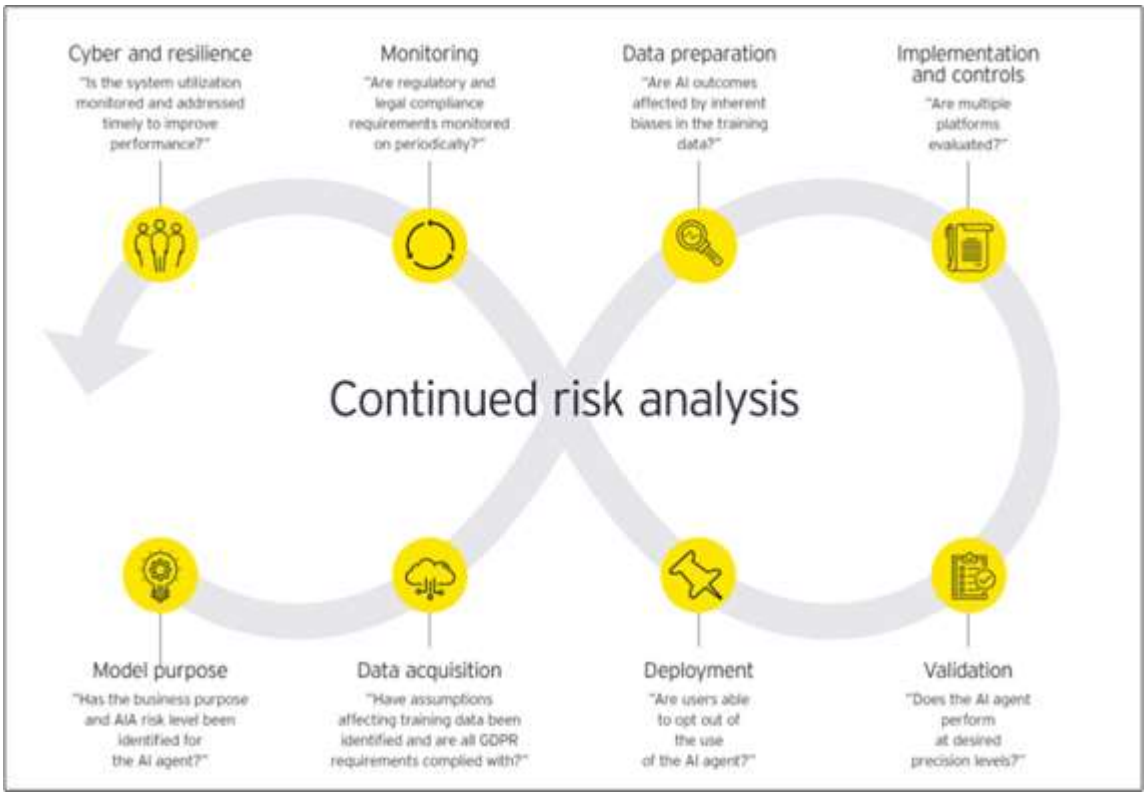
Fuente: The EU's New Rules on Artificial Intelligence: A Risky Endeavour, Dimitar Lilkov

Algunos sistemas de Inteligencia Artificial que son de interés para las compañías aseguradoras, como los chatbots, se ubican en la categoría de riesgo limitado. Si embargo, para la elaboración de modelos de siniestralidad se requiere de algoritmos catalogados como de alto riesgo.

La AIA todavía no ha sido aprobada por el Parlamento Europeo, pero dada la rápida evolución de las tecnologías de frontera, la aparición de nuevos riesgos asociados a las mismas no se puede subestimar, ya que puede tener grabes consecuencias para las compañías aseguradoras. Por ejemplo, si los datos no se utilizan de manera adecuada o los modelos presentan sesgos discriminatorios, el riesgo reputacional puede ser muy elevado.

Dado que el cumplimiento del AIA puede requerir un esfuerzo significativo por parte de las compañías aseguradoras, es recomendable que en la medida en que implanten tecnologías de Inteligencia Artificial se anticipen y tomen medidas preventivas, como por ejemplo implantando sistemáticas de evaluación de riesgo como los que se proponen en la siguiente figura.

Cuadro 2: Esquema GRC



Fuente: EY Consulting[3]

[3] EY Consulting, How AI is transforming governance and risk management in insurance

4. Aplicaciones del IoT

4.1. Campos de aplicación del IoT

Las soluciones basadas en IoT están teniendo aplicaciones prácticas en múltiples campos de interés para la sociedad actual. En los siguientes puntos se presenta algunas de las posibles aplicaciones.

Mantenimiento predictivo

Para los responsables de producción las paradas no programadas son una de las principales preocupaciones, debido a que implican perdida de horas productivas y materias primas, fabricación de productos deficientes y en ocasiones hasta la ruptura de la cadena de producción y suministro. Además, las reparaciones de los equipos afectados suelen ser costosas, generalmente el fallo de una pieza ocasiona daños en otras partes de la máquina.

Recogiendo datos del funcionamiento de los equipos con sensores IoT y tratándolos mediante AI es posible determinar cuál es la probabilidad de que una pieza de un equipo en concreto falle en un momento determinado, esto permite planificar paradas y efectuar los correspondientes trabajos de mantenimiento.

Un correcto sistema de mantenimiento preventivo puede permitir reducir los costes de mantenimiento hasta un 25% e incrementar la disponibilidad de los equipos entorno al 15%.

El volver a reiniciar una línea de producción tras una avería puede consumir grandes cantidades de energía y generar tiempos improductivos, con un correcto mantenimiento predictivo el número y frecuencia de las pardas se reducen.

Gestión energética

La eficiencia energética también se puede mejorar, además de la optimización de la temperatura de los edificios para minimizar el consumo energético asociado a la climatización, si se conoce el consumo energético de cada equipo se pueden ajustar las líneas de producción para que determinados procesos se realicen en aquellas franjas horarias en la energía es más económica.

Detección precoz de los defectos de producción

La monitorización de manera continua de múltiples indicadores mediante sensores IoT permite saber cuándo se va han producir los errores en la línea de producción y anticipar medias preventivas, se evita el fabricar productos que no serán aptos, se reducen los costes de fabricación y se incrementa la fiabilidad de los productos.

Optimización del stock

Evitar la detención de una línea de producción por no disponer de un determinado componente o no saturar un almacén de producto terminado es uno de los objetivos que tiene que cumplir un sistema de gestión de stock. Mediante sensores IoT es posible controlar todos los elementos del inventario y asegurar que en cada momento se conoce la cantidad de productos que existen en la planta de producción.

Seguridad en los entornos laborales

La prevención de los accidentes laborales también se puede mejorar con sistemas IoT. Por ejemplo, analizando la calidad del aire y la presencia de partículas contaminantes se pueden implantar soluciones para mejorar el confort de los operarios e incrementar su productividad. También es posible determinar la fatiga o la falta de atención en determinadas tareas y reducir los accidentes, lo también supone un incremento de productividad al haber menos bajas laborales.

Robótica Autónoma

La combinación de la robótica y el IoT permite el desarrollo de robots que pueden realizar determinadas tareas con un alto grado de autonomía o incluso sin la intervención humana. Actualmente están diferentes sectores industriales como la logística, seguridad, defensa, medicina y exploración espacial.

Simulaciones y Gemelos Digitales

Las simulaciones y los gemelos digitales son herramientas que se utilizan para crear modelos virtuales de procesos productivos, productos máquinas etc. Las simulaciones permiten a los ingenieros de diseño probar y ajustar sus prototipos en un entorno virtual antes de implementarlos en el mundo real. Son modelos virtuales que con la ayuda de miles de sensores IoT replican en tiempo real sistemas del mundo real.

Detección precoz de incendios forestales

Instalando en las redes de distribución de alta tensión sensores IoT que mediante el análisis de las radiaciones alertan de forma temprana de la presencia de un incendio facilitando la actuación temprana y reduciendo la duración del siniestro y sus constes sociales y medioambientales.

Smart Retail

Mediante cámaras con sistemas de reconocimiento facial se puede identificar a las personas que acceden a una tienda, analizar su edad, genero, preferencias de productos y recorridos. Una vez los datos se han analizado se puede predecir el comportamiento de los clientes y ubicar los productos en función de sus preferencias.

Incluso es posible permitir que los clientes eviten la cola de pago mediante sistemas como el implementado por Amazon Go o Carrefour Flash. En estos sistemas, el cliente accede al establecimiento, toma los productos que necesita y al salir por la pueta, se le carga automáticamente el importe de la compra en su cuenta bancaria.

Movilidad Urbana

La movilidad Urbana también puede beneficiarse del IoT, mediante el uso de drones, cámaras estratégicamente instaladas o con los datos que puedan reportar los vehículos se puede monitorizar el tráfico en tiempo real.

Con datos precisos sobre los flujos de vehículos, se pueden tomar medidas para mejorar la fluidez del tráfico, como ajustar los límites de velocidad, los tiempos de los semáforos y hasta incluso modificar los sentidos de circulación de los carriles. La plataforma desarrollada por Alibaba Cloud

Vehículos autónomos

Actualmente para la gestión de flotas de vehículos se están empleado sistemas IoT de posicionamiento GPS, por ejemplo, para optimizar rutas de reparto y reducir los costes de combustible.

Los sistemas de Autopiloto de Tesla utilizan sensores de proximidad, radares y cámaras para recopilar datos del entorno. Estos datos son analizados por un sistema de inteligencia artificial que predice el comportamiento de otros vehículos y peatones, y efectúa las maniobras de circulación pertinentes. El vehículo en su conjunto funciona como un sistema de IoT.

Entrega autónoma de paquetería

Con la creciente demanda de servicios logísticos cada vez más empresas tecnológicas como Amazon, Google FedEx, Robomart, Kiwi, Cartken por nombrar algunas, están utilizando robots autónomos para la entrega de pequeños paquetes. El principio de funcionamiento es similar al de los vehículos autónomos.

4.2. IoT en la Industrias 4.0 (4IR)

El concepto de Industria 4.0 se refiere a la integración de tecnologías digitales como el Internet de las Cosas (IoT), la robótica, el Big Data, la Inteligencia Artificial y los gemelos digitales en los procesos industriales. Su objetivo es crear fábricas y sistemas logísticos inteligentes y altamente eficientes.

Algunas empresas ya han entendido el potencial disruptivo de estas tecnologías y las están adoptando para mejorar sus sistemas productivos. A continuación, se presentan algunas de las empresas que están liderando su implantación

Campofrío Nueva Bureba

En 2014, un devastador incendio arrasó por completo la planta cárnica de Campofrío en Burgos, sin embargo, la empresa supo aprovechar el siniestro para transformar por completo su centro productivo en una industria 4.0.

Mediante el uso de microchips, se realiza un seguimiento en tiempo real de todo el flujo de producto, desde su entrada en la planta productiva hasta su expedición. Todo el proceso de producción está completamente robotizado, incluyendo el encajado y paletizado. La implementación de la Inteligencia Artificial ha supuesto una mejora del 10% en la productividad

Usando tecnologías de *machine learning* se logra una previsión más precisa de la demanda y se puede anticipar el volumen de producción y reducir los pedidos urgentes, lo que se traduce en un mayor nivel de satisfacción de los clientes. Además, la empresa cuenta con un gemelo digital que les permite simular todos los flujos de operaciones y analizar opciones de mejora de los procesos.

Se utiliza la tecnología *blockchain* para garantizar la trazabilidad de los productos, lo que se traduce en una mejora significativa de los estándares de transparencia.

Shanghai International Port Group (SIPG)

El puerto de Shanghái es el puerto más importante del mundo en términos de volumen de contenedores, anualmente mueve 47 millones de TEUs (Twenty-foot Equivalent Units). Para comprender la magnitud de esta cifra, podemos compararla con el puerto de Barcelona, cuyo volumen anual alcanza aproximadamente los 3,5 millones de TEUs (Twenty-foot Equivalent Units).

En la Terminal Yangshan, una de las principales terminales del puerto de Shanghái, la presencia humana prácticamente ha desaparecido, se ha implementado un sistema de automatización que elimina por completo la necesidad de intervención humana directa. Las grúas de contenedores son dirigidas de manera remota sin la necesidad de operarios en el campo a través de un avanzado sistema de gestión basado en el back-end.

Los camiones portacontenedores también han dejado de ser necesarios, han sido sustituidos por una flota de Vehículos Guiados Automatizados (AGVs). Estos AGVs pueden moverse libremente a través del puerto, realizan tareas de carga, descarga y transporte de contenedores de manera autónoma, además, tienen funcionalidades de auto diagnóstico y monitorización de energía para minimizar su tiempo de inactividad.

La comunicación de todo el sistema con la Inteligencia Artificial que lo administra se realiza de manera inalámbrica a través de redes 4.5G LTE de Huawei.

Centros logísticos de Amazon

Los centros logísticos de Amazon son otro ejemplo de cómo la combinación de la robótica, la Inteligencia Artificial, el Internet de las Cosas y conectividad inalámbrica se puede aplicar para mejor la eficiencia en el sector logístico.

Amazon en sus almacenes emplea robots para el almacenamiento y transporte de las mercancías. Estos robots se desplazan de forma autonoma mejorando la eficiencia del flujo de productos y reduciendo los tiempos de entrega. Además, mediante sistemas de inteligencia artificial, anticipan la demanda y optimizan la distribución de productos en las estanterías

En los sistemas de clasificación y embalaje también se utiliza la robótica y la Inteligencia Artificial. Mediante el uso de algoritmos de autoaprendizaje se mejora la clasificación y se optimiza el proceso de embalaje. Esto permite una reducción en los costes de estocaje y de transporte.

La comunicación entre los robots, las balizas de posicionamiento y la inteligencia artificial que los coordina se realiza mediante sistemas inalámbricos.

Aviones tripulados remotamente

Reliable Robotics, una empresa fundada por ex ingenieros de Space X y Tesla ha logrado que la FAA (Administración Federal de Aviación en Estados Unidos), la agencia encargada de supervisar las actividades relacionadas con la aviación civil de Estados Unidos. acepte las bases de certificación para los sistemas de vuelo sin piloto supervisados por personal de tierra. Está previsto que las primeras pruebas comiencen con un Cessna 208 Caravan antes de 2024.

Aunque los vuelos de pasajeros en aviones comerciales sin piloto se encuentran en una fase incipiente, es muy probable que en los próximos años se conviertan en una realidad una vez que se cumplan los estándares de seguridad necesarios.

5. Aplicaciones del IoT en el Sector Asegurador

5.1. Mejora en modelos matemáticos

El principio de funcionamiento del Sector Asegurador se basa en determinar mediante complejas técnicas de matemática actuarial la probabilidad y severidad de ocurrencia de un determinado evento económicamente cuantificable, en otras palabras, intenta predecir o simular la probabilidad de ocurrencia de un siniestro y el coste que podría suponer.

Calculadas la frecuencia siniestral esperada y cuantía económica esperada es posible calcular primas puras, tarificar, hacer reservas técnicas, ofertar productos a los clientes, cumplir con los requerimientos de solvencia etc.

Los datos que se utilizan para realizar los cálculos actuariales se obtienen de la experiencia acumulada de años anteriores. Para aquellos productos en los que la aseguradora tiene una larga trayectoria de comercialización, los resultados de los cálculos efectuados son mucho más fiables que para aquellos productos de nueva creación en los que apenas se dispone de un historial de datos.

Es necesario destacar que disponer de datos en cantidad y calidad suficiente es fundamental para realizar previsiones matemáticas fiables. Cuanto mayor sea la calidad de los datos y más variables representativas se puedan analizar, más precisas serán las previsiones.

Se pone de manifiesto la relevancia que tienen los datos para el sector asegurador. El dato es como la materia prima, el correcto funcionamiento de la actividad se basa en disponer de datos en cantidad y de calidad suficiente para realizar simulaciones fiables.

El IoT es una inmensa fuente de datos que puede ayudar al sector asegurador a mejorar la precisión de los modelos matemáticos de todas las líneas de negocio, desde automoción y hogar, hasta seguros de salud y de riesgos industriales

Tomando como ejemplo el caso del seguro del automóvil, tradicionalmente los modelos actuariales se han nutrido de variables como el kilometraje, la edad del conductor, la potencia y antigüedad del vehículo, entre otros. Sin embargo, gracias al IoT, es posible analizar variables más precisas y de mayor calidad, como la cantidad de horas que se conduce diariamente, el número de frenadas y aceleraciones realizadas durante un trayecto y la intensidad de estas, la velocidad de circulación y las características de las vías por las que normalmente se circulan.

Con toda esta información, los modelos tradicionales se pueden complementar con datos que permiten conocer con más precisión el comportamiento real del conductor y, por lo tanto, obtener modelos matemáticos más precisos para evaluar el riesgo asociado a un potencial cliente.

El seguro del hogar también podría beneficiarse del uso del IoT. Tradicionalmente, los datos que principalmente se han empleado en la modelización de esta tipología de riesgos han sido la ubicación geográfica de la vivienda, las características constructivas del inmueble, la superficie útil y número de personas que se declara que habitan en ella.

El uso que se le da a la vivienda es un factor muy relevante en la ecuación del seguro del hogar. Sin embargo, este dato es proporcionado por el cliente y no siempre se corresponde con la realidad o puede cambiar durante la vigencia de la póliza sin que la compañía aseguradora tenga conocimiento de ello generando distorsiones en las modelizaciones.

El riesgo de robo en una vivienda puede variar dependiendo de si está permanentemente ocupada por personas que teletrabajan los cinco días de la semana o si está ocupada por personas que constantemente están viajando y pernoctando en hoteles por motivos laborales durante la semana y el fin de semana prefieren descansar en su segunda residencia. En este último caso el riesgo de robo será mayor.

De manera similar, el riesgo de sufrir daños por agua puede variar según el uso que se dé a la vivienda. Por ejemplo, una vivienda cuyos moradores se duchan en el gimnasio y prefieren comer en un restaurante a medio día y encargar la cena, estará sujeta a un menor desgaste y será menos susceptible de sufrir siniestros de rotura de tuberías que una vivienda cuyos moradores se duchan tres veces al día y están constantemente cocinando.

Mediante sensores IoT instalados en las acometidas de luz y agua o aprovechando el potencial de otros dispositivos IoT como robots de limpieza y asistentes de voz, sería posible determinar los patrones de comportamiento de los asegurados y ajustar la modelización actuarial al uso real que el asegurado hace de la vivienda.

En los seguros de salud el IoT tiene aplicaciones. Con el uso de relojes inteligentes es posible monitorizar información relevante en el ámbito de la salud, como el número de pasos que una persona realiza, su frecuencia cardiaca, las horas que permanece sentado, y el tiempo que dedica a hacer ejercicio o a dormir. Presumiblemente una persona con una baja actividad física tenga más riesgos de sufrir ciertas enfermedades que una persona con una actividad física moderada, pero si la actividad es muy elevada se corre el riesgo de incrementar el número de lesiones.

Las aplicaciones del IoT también son extrapolables al ámbito industrial. Una planta productiva en la que las líneas estén operando veinticuatro horas al día tiene más riesgo de sufrir averías de maquinaría que una planta que su actividad es de solo ocho horas diarias. Por el contrario, si la activad es estacional, el riesgo de avería se incrementa en el momento que se retoma la actividad debido a que ciertos equipos pueden sufrir un deterioro acelerado si permanecen inactivos durante largos periodos de tiempo. Con la instalación de

sensores IoT en las máquinas y en las acometidas de suministro, se puede determinar con mayor precisión el modelo productivo de la empresa y conocer si realiza paradas programadas de mantenimiento y con qué frecuencia las realiza. De esta forma, se puede ajustar el modelo de previsión de siniestralidad.

5.2. Productos personalizados

Los clientes esperamos un trato personalizado, nos queremos sentir especiales, las aseguradoras también tendrán que ofrecer productos personalizados para continuar satisfaciendo las expectativas de los clientes.

Actualmente ya existen aseguradoras que están ofreciendo estos productos en seguros de automóvil. Los clientes y potenciales clientes, se instalan una aplicación móvil que monitorea el comportamiento de la conducción del vehículo, la prima se calcula en función del comportamiento del conductor. Los conductores que muestren una conducción más prudente pueden obtener primas mucho más bajas. Pueden no contratar aquellas garantías que les penalizan en la prima o incluso solamente contratar las garantías cuando las necesiten.

En seguros de salud también se está aplicando, algunas compañías de EE.UU. utilizan aplicaciones móviles y relojes inteligentes para monitorizar el comportamiento del asegurado, se registra los lugares que frecuenta y las actividades diarias que realiza, aplicando AI se hacen sugerencias para mejorar el estilo de vida o la conducción. Con los datos obtenidos se pueden discriminar los asegurados que tienen un estilo de vida con menos predisposición a sufrir siniestros y ofrecerles descuentos en las primas. La normativa en materia de privacidad de datos de la UE limita considerablemente el desarrollo de esta tipología de productos.

5.3. Vigilancia de cartera

Las compañías aseguradoras utilizan técnicas de vigilancia de cartera para fidelizar y retener aquellos clientes que tienen un buen comportamiento siniestral y penalizar o incluso no renovar aquellas pólizas con elevada siniestralidad.

Una compañía aseguradora con una cartera de clientes que presenta un buen comportamiento siniestral puede ofrecer tarifas más competitivas. Al ofertar productos con tarifas competitivas es posible centrarse en aquellos segmentos de clientes que se espera que tengan un buen comportamiento según los modelos de previsión actuarial.

Esto permite atraer a los clientes que son de interés para la aseguradora y rechazar los que no interesan, que son los que se prevé que tengan un mal comportamiento siniestral. Se genera circulo que se retroalimenta, permitiendo a la aseguradora tener tarifas más competitivas, clientes mejor seleccionados y menos siniestros.

Cuadro 3: Círculo virtuoso de la siniestralidad

Fuente: Elaboración propia

En base a lo anteriormente expuesto, se deduce que para que una compañía pueda continuar siendo competitiva es necesario que aplique una correcta política de vigilancia de cartera.

Actualmente, la vigilancia de cartera se efectúa en base al comportamiento de la póliza. En la toma de decisiones se tienen en cuenta otros factores como la vinculación del cliente. Por ejemplo, un cliente que tenga varias pólizas contratadas puede tener un mal comportamiento siniestral en uno de los productos y un excelente comportamiento en el resto, existe la posibilidad de que teniendo en cuenta el conjunto de los productos que tiene contratados el cliente sea rentable y a la compañía le interese retenerlo. En cualquier caso, la toma de decisiones se efectúa una vez los siniestros ha han ocurrido.

Pongamos como ejemplo el caso del seguro del automóvil, supongamos que una persona acude a una compañía aseguradora para suscribir una póliza de automóvil, en base a los modelos actuariales de previsión de siniestros se determina que es un perfil de baja siniestralidad, se le suscribe la póliza y como era de esperar durante los tres primeros años no declara ningún siniestro.

Al cuarto año, su situación personal cambia, cede ocasionalmente su vehículo a su nueva pareja, estas variaciones normalmente no son notificadas a la compañía aseguradora. La persona que también puede conducir el vehículo se corresponde con un perfil de riesgo elevado que de promedio declara un siniestro cada dos años. Si la aseguradora fuese capaz de detectar este cambio en los patrones de la conducción podría determinar que el riesgo de siniestralidad se ha incrementado considerablemente y por consiguiente aplicar la correspondiente política de vigilancia de cartera.

Este ejemplo es escalable a todos los niveles, ya que puede aplicarse a diferentes tipos de seguros. Por ejemplo, en el caso de un seguro de familia hogar, si el comportamiento de los habitantes de la casa cambia durante la vida de la póliza, se producirá una variación en el riesgo suscrito. Del mismo modo, en el caso de una fábrica, si las políticas de producción y mantenimiento cambian durante la vida de la póliza, también puede haber una variación en el nivel de riesgo asociado. En ambos casos, si la aseguradora puede detectar cualquier cambio en los patrones que afectan el riesgo de siniestralidad, puede aplicar las oportunas medidas de vigilancia de cartera.

Con los datos recopilados por los sensores IoT y con el correspondiente análisis de los datos con IA será posible detectar cambios en los patrones de comportamiento de los riesgos y aplicar políticas de vigilancia de cartera preventiva. Es decir, la compañía podrá penalizar o aplicar políticas de fidelización en función de la variación del comportamiento del cliente, y en aquellos casos en los que el comportamiento no se ajuste a las políticas de suscripción, no renovar el contrato si el regulador lo permite.

5.4. Prevención de siniestros

Con la implementación del IoT y la Inteligencia Artificial, las aseguradoras dispondrán de modelos cada vez más fiables, lo que les permitirá prever con mayor precisión la ocurrencia de siniestros. Esto podría implicar un cambio en relación con algunos productos que se comercializan actualmente, pasando de centrarse en la valoración de las perdidas como consecuencia de los siniestros ocurridos a enfocarse en la prevención de pérdidas.

Este nuevo enfoque podría transformar la concepción tradicional del seguro, evolucionando de un modelo basado en la aceptación o transferencia de riesgos a un modelo de negocio más orientado a la prevención y mitigación de riesgos.

Por ejemplo, en las líneas de producción en las que intervienen personas, se podría aprovechar la tecnología de Inteligencia Artificial para analizar los datos recopilados por los sensores IoT y las imágenes capturadas las cámaras de videovigilancia. Esto permitiría identificar comportamientos que aumentan el riesgo de sufrir accidentes laborales, como la disminución de la atención debido

a la fatiga. De detectarse un nivel de riesgo superior a un umbral predeterminado, se podrían implementar medidas adecuadas para permitir que el trabajador se recupere, evitando así posibles accidentes laborales.

También, instalando sensores IoT en la ropa o las herramientas de los operarios que trabajan en tareas de mantenimiento o en el sector de construcción sería posible monitorizar su ubicación en tiempo real, i de acceder a zonas catalogadas como peligrosas o ubicarse cerca de máquinas que les pueda ocasionar daños personales, se podría generar alertas o incluso detener las máquinas, y evitar posibles accidentes y las posteriores reclamaciones de daños personales.

En el ámbito de los seguros de salud, el IoT también podría ser de interés. Por ejemplo, mediante la monitorización del ritmo cardiaco, los niveles de azúcar en sangre y otras constantes vitales, se podrían detectar cambios que alerten de manera temprana sobre la posibilidad de sufrir determinadas patologías, como paros cardiacos. Esto permitiría activar los correspondientes protocolos sanitarios para actuar en una fase temprana o incluso prevenir la aparición de la patología. Los costes de hospitalización y rehabilitación se podrían reducir considerablemente.

Informando al asegurado en relación con ciertos comportamiento o situaciones que le representan un riesgo elevado de sufrir determinados siniestros, este podría tomar medidas para reducir su exposición, además de disminuirse la frecuencia de los siniestros y cuantía de las indemnizaciones al actuar de forma más precoz, se fomentaría la cultura de la prevención.

Las compañías aseguradoras también pueden aprovechar los servicios de prevención como una oportunidad de negocio para fidelizar a los clientes y reducir las tasas de anulación de pólizas. Incrementando la frecuencia de interacción con los clientes se refuerza el vínculo emocional con la compañía aseguradora y se incrementa la fidelidad del cliente.

El IoT ofrece nuevas oportunidades de negocio para las aseguradoras. Es posible que esta tecnología permita para determinadas coberturas cambiar el actual modelo en el que la compañía por norma general solo interactúa con el asegurado tras la ocurrencia de un siniestro, a un modelo más orientado a la interacción constante a través de servicios de prevención.

5.5. Automatización de la tramitación de siniestros

La automatización de la tramitación de los siniestros permite mejorar tanto la eficiencia como la rapidez de los procesos. Además de reducir los costes de personal, ofrece la posibilidad de reportar al cliente en tiempo real los hitos más relevantes de la vida del siniestro, lo que se traduce en un proceso mucho más transparente para el cliente.

En algunos segmentos de los denominados siniestros de frecuencia, siniestros de baja cuantía y escasa dificultad, es posible que en los próximos años desaparezca por completo la necesidad de intervención humana.

Pongamos como ejemplo un siniestro en el que al asegurado le aparece una mancha de humedad en el techo del baño de su vivienda. Ante esta situación, el asegurado envía un video a la compañía aseguradora en el que se detalla la ubicación y magnitud de los daños. Los algoritmos de inteligencia artificial implementados por compañía aseguradora analizan el contenido del video y determinan que el origen del siniestro es una avería en las instalaciones del piso superior, además, efectúan una medición de la superficie de pintura afectada y tasan el coste que supone la reparación.

En el supuesto de que el asegurado perjudicado pudiese proporcionar a su aseguradora los datos de la compañía que asegura el piso causante, se podría automatizar la comunicación entre ambas aseguradoras, de tal manera que la compañía que asegura el piso causante del siniestro podría enviar un técnico especializado para reparar el origen de los daños.

En el caso de que técnico enviado por la compañía aseguradora del piso causante también se encargase de reparar los daños del piso perjudicado, la compañía del piso perjudicado podría llevar a cabo todo el proceso de tramitación del siniestro sin necesidad de intervención humana en ninguna de las etapas del proceso.

Conforme las capacidades de la inteligencia artificial mejoren, la tipología de siniestros susceptibles de ser gestionados sin intervención humana se incrementará. En el caso particular de los siniestros de frecuencia, es posible que la única intervención humana necesaria sea la del técnico encargado de realizar la reparación de los daños, y que solo en los siniestros singulares o de alta complejidad se requerirá de la participación de peritos y tramitadores.

No obstante, las aseguradoras no tienen que perder de vista que a pesar de que las mejoras tecnológicas permitirán que en los próximos años sea posible la gestión de un elevado número siniestros sin la intervención humana, para algunos clientes la interacción con personas seguirá siendo un elemento clave diferenciador de la calidad del servicio percibido.

En consecuencia, las compañías en función del perfil de su cliente objetivo deberán de buscar el equilibrio entre la automatización de los procesos y el valor añadido que aporta para algunos clientes la intervención humana.

5.6. Reducción del coste de los siniestros

Mediante el uso de dispositivos IoT será posible detectar los siniestros en su etapa inicial, esto permitirá tomar medidas para minimizar los daños que se pueden ocasionar.

Del mismo modo que con el empleo de sensores de detección de humo es posible detectar la existencia de un conato de incendio y tomar medidas para evitar su propagación, empleando sensores IoT es posible detectar siniestros en su fase incipiente y tomas las correspondientes medias para minimizar los daños que se puedan derivar.

Por ejemplo, en el ámbito del seguro del hogar, donde aproximadamente el 50% del coste de los siniestros de frecuencia es consecuencia de fugas de agua, instalando dispositivos IoT en la acomedida de la vivienda es posible detectar pequeñas fugas antes de que estas generen daños.

Detectando las averías en la fase incipiente es posible generar un aviso a un técnico de la compañía para que verifique el estado de la instalación y efectúe las correspondientes reparaciones antes de que el daño se manifieste de una forma evidente en paredes, suelos de parquet, puertas y otros elementos. De esta manera se pueden reducir considerablemente el importe de las reclamaciones. Este concepto es extrapolable para muchas otras tipologías de siniestros.

5.7. Transformación sectorial

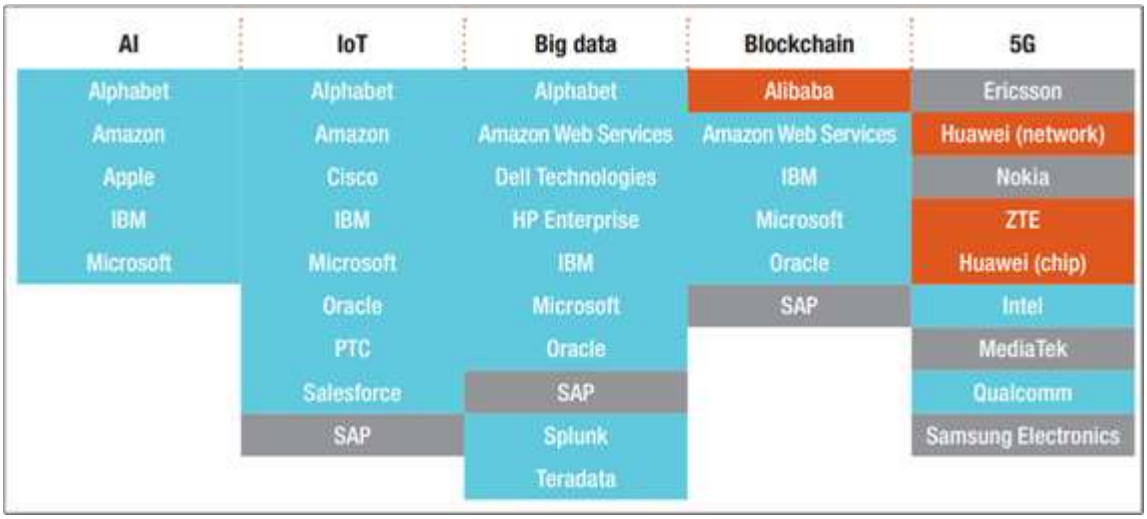
Una de las claves del éxito de una compañía aseguradora es su capacidad para disponer de datos de datos suficientes, tanto en calidad como en cantidad, para conocer el comportamiento siniestral de sus clientes. Estos datos son esenciales para poder crear modelos matemáticos precisos que permitan hacer previsiones de riesgo de siniestralidad.

Cuantos más datos dispone una compañía, más segmentados estarán los perfiles de los clientes y, por lo tanto, más precisos son los modelos matemáticos. De esta manera, es posible identificar con mayor exactitud los perfiles de mayor riesgo y establecer políticas de suscripción y tarificación adecuadas, lo que se traduce en una siniestralidad mejor y mayores beneficios empresariales para la compañía aseguradora.

Como se ha mencionado en los capítulos anteriores, el Internet de las cosas (IoT) es la tecnología responsable de recopilar los datos que alimentan el Big Data. Para manejar adecuadamente el volumen masivo de información que representa el Big Data, es necesaria una Inteligencia Artificial capaz de analizarlo de forma efectiva. De lo contrario, los métodos convencionales no serán suficientes para aprovechar todas las posibilidades que brindan los datos obtenidos a través del IoT.

Las tres tecnologías que pueden tienen influencia decisiva en el sector asegurador, el IoT, el AI y el Big Data se corresponden a las denominadas tecnologías de frontera, además, los principales proveedores de servicios de estas tecnologías están presentes en las tres.

Gráfica 4: Principales proveedores de tecnología de frontera.



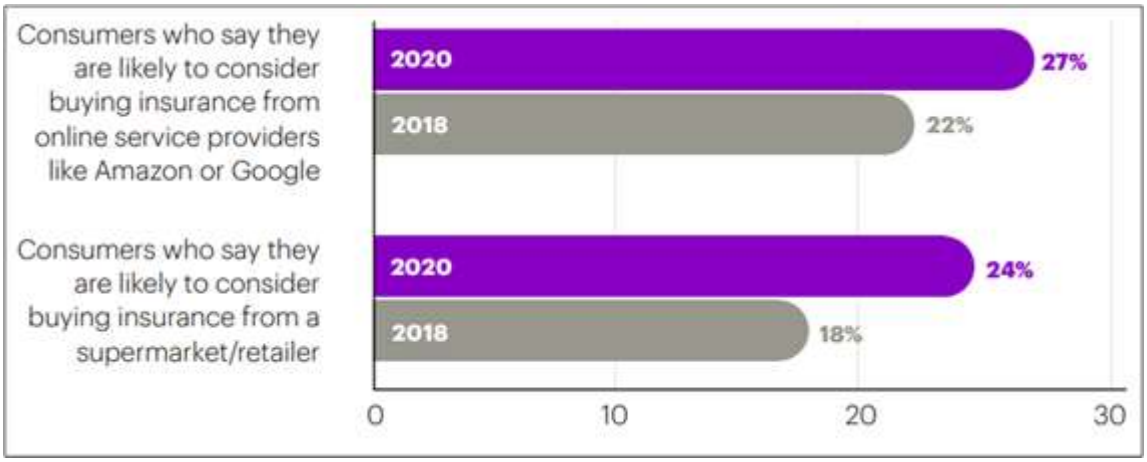
Fuente: United Nations Conference on Trade and Development (UNCTAD), Technology and Innovation Report 2021

El gráfico presentado anteriormente muestra que Alphabet, Amazon, IBM y Microsoft son líderes en los campos del IoT, la AI y el Big Data. Estas empresas, ya sea directamente o a través de sus filiales, como Google y Android en el caso de Alphabet, han desplegado millones de dispositivos de IoT en hogares, están realizando pruebas en vehículos autónomos y son proveedores de sistemas de control industrial

Además, estas empresas han implementado una estrategia de fidelización altamente efectiva. Al mantener una interacción constante con sus clientes, han logrado establecer un vínculo confianza, como resultado, sus clientes están muy predispuestos a adquirir cualquier producto que se les ofrezcan.

En la siguiente gráfica se puede apreciar cómo la intención de compra de productos relacionados con el seguro a través de las mencionadas empresas presenta una tendencia alcista.

Gráfica 5: Intención de compra de seguros



Fuente: Accenture's Global Insurance Consumer Study 2021

Las empresas punteras en tecnología de frontera, como Alphabet, Amazon, IBM y Microsoft, tienen una ventana de oportunidad para introducirse en el sector asegurador debido a su capacidad financiera, experiencia en el manejo de datos, gran número de clientes y reputación en los mercados.

Estas empresas pueden seguir diversas estrategias para introducirse en el mercado, como crear filiales aseguradoras, comercializar productos de aseguradoras tradicionales, valerse de las aseguradoras tradicionales como proveedores de servicios o transferir su capacidad de tratamiento de datos.

Cualquiera que sea la estrategia que elijan, tendrá un impacto significativo en la cadena de valor de la industria. La tecnología incrementará la precisión en la evaluación de riesgos, y tal y como ha ocurrido en otros sectores, mejorará la experiencia del cliente.

Sin embargo, dependiendo de la estrategia que elijan, deberán de superar la barrera de entrada cumpliendo con las regulaciones y requisitos legales del sector y enfrentarse los desafíos que plantea un mercado altamente competitivo y maduro como el de los seguros.

5.8. Aprovechamiento de las sinergias de los ecosistemas

La constante digitalización de la sociedad no solo está cambiando las expectativas de los clientes, sino que también está difuminando los límites entre las industrias. Las compañías aseguradoras no pueden evitar este fenómeno que afecta a todos los sectores industriales, y que es previsible que se acelere con la disrupción de las tecnologías de frontera como el IoT i la AI.

A medida que los límites sectoriales se difuminan, otras industrias pueden captar parte del negocio asegurador, pero las compañías aseguradoras también tienen la oportunidad de captar negocio de otras industrias.

En el mundo natural, los organismos que habitan un mismo espacio interactúan entre sí compitiendo por los recursos disponibles, pero también establecen relaciones de colaboración simbiótica que les ofrecen beneficios mutuos. En el mundo empresarial actual, en el que cada vez los límites entre sectores están más difuminados y existe una mayor interdependencia entre sectores, se pueden aprovechar los ecosistemas empresariales.

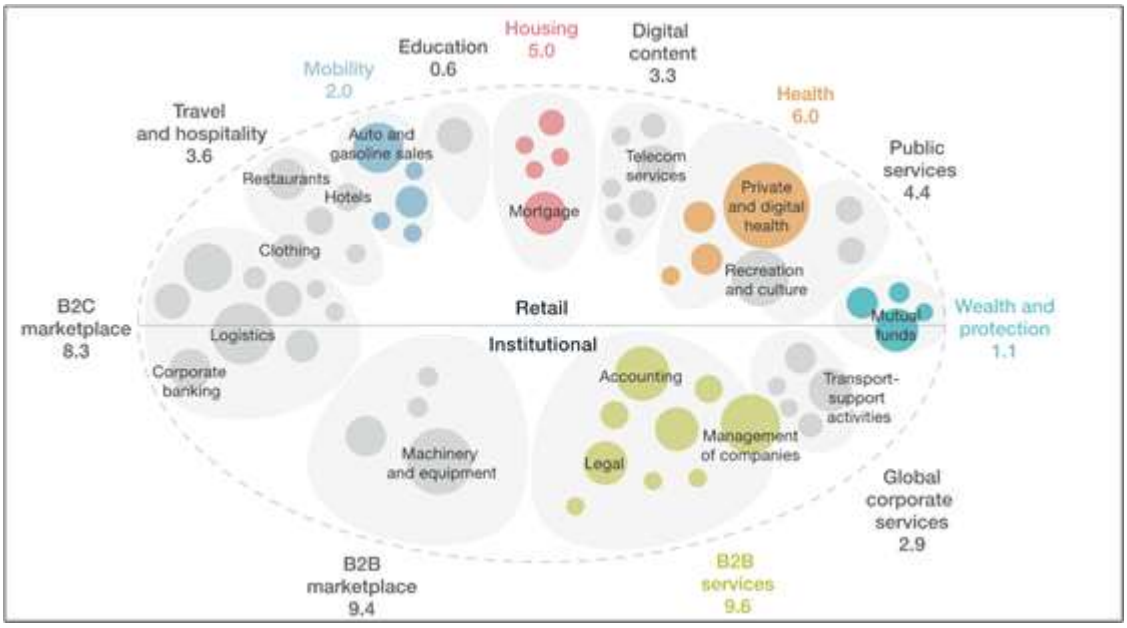
Las empresas que operan en modo ecosistema forman una red colaborativa con otras empresas, lo que les permite aprovechar sinergias, compartir tecnología e incluso integrarlas en partes de su cadena de valor. Este enfoque les ofrece una gran agilidad y capacidad de evolución, permitiéndoles adaptarse rápidamente a los cambios de los mercados.

Según la consultora McKinsey[4], para el año 2025 estima que alrededor del 30% de los ingresos mundiales serán generados por ecosistemas empresariales. Los ecosistemas empresariales se centrarán dar respuesta a las necesidades básicas de los individuos.

En la siguiente gráfica se muestra los principales ecosistemas y su volumen de negocio esperado en billones de dólares según McKinsey.

[4] McKinsey & Company, Insurance beyond digital: The rise of ecosystems and platforms

Gráfica 6: Principales ecosistemas y volumen de negocio esperado para el 2025



Fuente: McKinsey & Company, Insurance beyond digital: The rise of ecosystems and platforms

Por poner algunos ejemplos de oportunidades de negocio, en el ecosistema de la movilidad personal, las aseguradoras tienen la oportunidad de expandirse en áreas como la gestión de vehículos compartidos, la compra de vehículos y la gestión de su mantenimiento.

También en el ecosistema de los viajes y el alojamiento pueden expandirse en áreas como el alojamiento compartido, por ejemplo, colaborando con empresas de alojamiento compartido para ofrecer productos que cubran las necesidades del perfil de clientes de demandan estos servicios.

Además, en los ecosistemas B2C, las aseguradoras pueden beneficiarse de la utilización de nuevos canales de distribución y llegar a un público objetivo que busca una experiencia de interacción completamente digital.

Adoptar una política de ecosistema en un negocio conservador como el asegurador puede suponer un reto, pero es probable que aquellas aseguradoras que entiendan el cambio de paradigma en la evolución del mercado y den los primeros pasos, además de acceder a nuevos nichos de mercado, se sitúen en una posición ventajosa respecto a sus competidores.

Posiblemente algunas compañías opten por una estrategia más centrada en ofrecer una amplia variedad de productos y servicios a sus clientes, mientras que otras intenten integrarse en la cadena de valor del customer journey. Sin embargo, ambas estrategias requieren mejoras en la capacitación tecnológica y organizativa.

En cuanto a la mejora de la capacidad tecnología, las inversiones se tendrían que orientar en el desarrollo arquitecturas TI (Tecnología de la información) flexibles que les permita integrar de manera rápida y económica sus servicios y productos a los ecosistemas a través de Interfaces de Programación de Aplicaciones (API)

En el ámbito organizativo, las inversiones se tendrían que orientar en mejor la capacidad para asociarse de manera ágil con otros socios comerciales, y especialmente con aquellos que se mueven en otros contextos diferentes al del sector asegurador.

6. Riesgos asociados al IoT

6.1. Riesgos Cyber

6.1.1. Impacto del Cyber risk en la sociedad

Para que un ataque informático sea efectivo en un dispositivo IoT se tienen que dar alguna de las siguientes condiciones. Es necesario que los dispositivos sean visibles para el atacante, que el software que tienen instalado presente algún tipo de vulnerabilidad que pueda ser explotada, o que los dispositivos se conecten a través de protocolos o canales de comunicación no seguros, si no se dan están circunstancias difícilmente un atacante podrá establecer comunicación con ellos, enviar comandos o capturar paquetes de datos.

Es común que en el ámbito de IoT se cumplan alguna o todas las condiciones mencionadas anteriormente con relativa frecuencia. Muchos dispositivos son puestos en funcionamiento utilizando las configuraciones preestablecidas de fábrica sin que se tomen medidas básicas de seguridad como cambiar las contraseñas o realizar una auditoría para verificar la robustez de los protocolos de cifrado de las conexiones

La seguridad en una red informática frente a los ataques cibernéticos se puede comparar con la protección de una vivienda. Por más que se tenga una puerta blindada con cerraduras de alta seguridad, si se deja una pequeña puerta trasera abierta, atacantes malintencionados podrían aprovechar esa debilidad para acceder al interior de la vivienda. De manera similar, los dispositivos IoT pueden convertirse en el eslabón más débil de la cadena, lo que permite que los atacantes se infiltren en la red a través de ellos y comprometan la seguridad de todos los elementos que la conforma

Por lo tanto, es fundamental prestar atención a la seguridad de los dispositivos IoT y tomar medidas para reducir el riesgo de ataques cibernéticos en la red. A continuación, se mencionan algunos de los ataques informáticos más frecuentes que pueden estar relacionados con los dispositivos IoT.

Botnets

Una botnet o también denominado red zombi es una red de ordenadores o dispositivos IoT que han sido infectados por un programa maligno y son controlados remotamente por un atacante. A los dispositivos individuales de les llama bots o zombis, y un grupo de bots de le llama botnet.

Los dueños legítimos de los dispositivos infectados generalmente no se dan cuenta de que su equipo forma parte de una botnet, el malware actúa en segundo plano de manera casi imperceptible. Los botnets no son un fin en sí mismo, son un instrumento para realizar otro tipo de ataques.

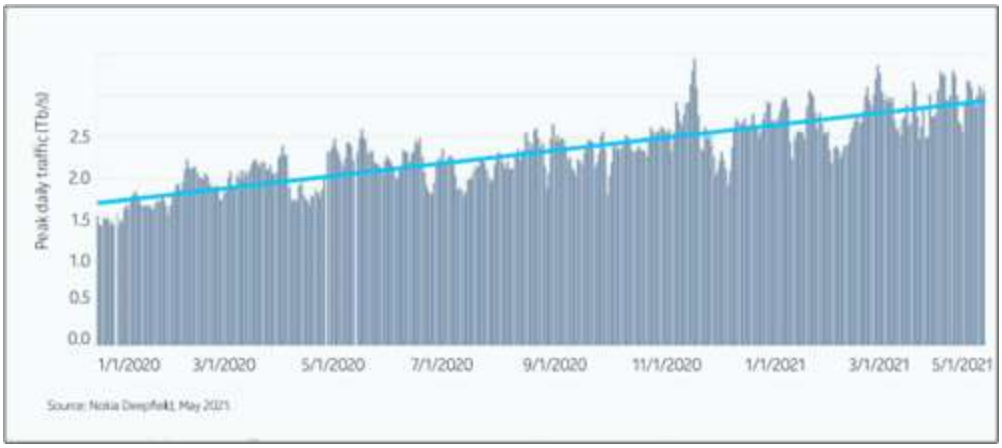
Los botnets pueden ser utilizados de manera coordinada para realizar ataques de denegación de servicio (DoS). A medida que el número de dispositivos conectados aumenta el potencial de esta tipología de ataques se incrementa. Además, como cada bot es un dispositivo legítimo de internet, filtrar el tráfico de datos de ataque del tráfico normal es muy complejo.

Denegación de servicio (DDoS)

Los ataques de denegación de servicio o DDoS (Distributed Denial of Service) son un tipo de ataque que tiene como objetivo interrumpir el funcionamiento de un servicio informático o dispositivo conectado a la red. Estos ataques consisten en incrementar el tráfico de la red o las peticiones de acceso del dispositivo objetivo hasta que lo saturan, lo que impide que pueda responder a las solicitudes legítimas. Los cibercriminales para perpetrar esta tipología de ataques generalmente utilizan lo que se conoce como redes zombi o botnets.

En los últimos años, el tráfico de datos asociados a DDoS se ha duplicado anualmente según Nokia[5], y se espera que esta tendencia se mantenga en los próximos años. A continuación se presenta una gráfica en la que se estima los picos diarios del trafico mundial de datos asociados a ataques DDoS.

Gráfica 7:Estimación de picos de tráfico diario asociad a DDoS



Fuente: Nokia Deepfield, May 2021.

Los ataques volumétricos son los más comunes dentro de los ataques DDoS y se caracterizan por transmitir grandes cantidades de datos con el objetivo de saturar el ancho de banda de la conexión. Al saturar el ancho de banda, la conexión se vuelve lenta o incluso se interrumpe por completo, lo que impide a los usuarios legítimos acceder al servicio.

[5] Nokia, Deepfield Network Intelligence Report DDoS in 2022

También existen ataques que se basan en enviar una gran cantidad de solicitudes de conexiones TCP (Transmission Control Protocol), UDP(User Datagram Protocol) o ICMP(Internet Control Message Protocol) al servidor o equipo objetivo con el fin de saturar su capacidad de procesamiento.

Los ataques también pueden producirse a nivel de aplicación, el procedimiento es similar al utilizado en otros tipos de ataque DDoS, se aumenta el tráfico de datos hasta que se provoca la saturación de la aplicación y se impide su normal funcionamiento.

Los atacantes pueden exigir a las víctimas un rescate, generalmente en forma de criptomonedas, a cambio de poner fin a los ataques.

Manipulación de datos

Los ataques de manipulación de datos consisten en alterar o falsear los datos recopilados por los sensores IoT. El objetivo de que el servidor o Inteligencia Artificial que los analiza ejecute ordenes incorrectas y ocasione averías a las instalaciones.

Por ejemplo, supongamos el caso de una vivienda en la que una alteración en las lecturas del termostato de la nevera hace que permanezca funcionando de forma ininterrumpida a muy baja temperatura, como consecuencia del ataque el compresor sufre sobrecalentamiento y se avería.

En una línea de producción el problema podría ser mucho más grave, supongamos un robot que tiene que apretar tornillos con un determinado par de apriete, una alteración en los datos reportados por los sensores dinamométricos resulta en piezas con un montaje deficiente. Además del sobrecoste de repetir la operación de montaje, también está la responsabilidad que se podría derivar de producto defectuoso.

Divulgación de datos

La cadena hotelera Marriott en 2018 sufrió un ataque de divulgación de datos en el que quedaron expuestos los datos de más de 500 millones de clientes. Los datos incluían información sensible como direcciones, números de teléfono, correos electrónicos, números de pasaporte, horas de entrada y salida número de tarjeta de crédito. Un ataque de estas características puede tener graves consecuencias reputacionales para la empresa.

Ransomware

En los últimos años, se ha observado un aumento en la amenaza de ransomware, es un software malicioso diseñado para bloquear el acceso a los equipos infectados mediante el cifrado de su contenido, y luego exigir un rescate para restablecer el acceso. Normalmente los cibercriminales exigen el rescate en criptomonedas para evitar que las autoridades les puedan rastrear.

En 2005 se reportan los primeros casos concretos de ransomware en Rusia, desde entonces, este tipo de software malicioso ha alcanzado una escala global y su efectividad ha aumentado con cada nueva variante desarrollada. En 2011 se produce un incremento exponencial del número de ataques registrados, y esta cifra ha seguido aumentando año tras año.

Entre el 12 y el 16 de mayo de 2017 se registra el primer ataque de alcance global, el malware empleado es conocido como WannaCry o WannaCrypt. La propagación se efectúa a través de equipos con Microsoft Windows aprovechando una vulnerabilidad del sistema.

Casi dos meses antes de que se registrase el ataque, Microsoft había lanzado una actualización del sistema, por lo que solo eran susceptibles de ser infectados aquellos equipos que no habían actualizado el sistema.

Deloite estima que unos 360 mil ordenadores en más de 180 países se ven afectados por el incidente. Sin embargo, otras fuentes sugieren que la cantidad podría llegar hasta los 15 millones, dado que en grandes empresas hay muchos equipos que comparten una única dirección IP de salida a internet, y detrás de ella hay muchos otros equipos que también pueden ser infectados. El impacto económico del incidente se estima superior a los 200 millones de dólares.

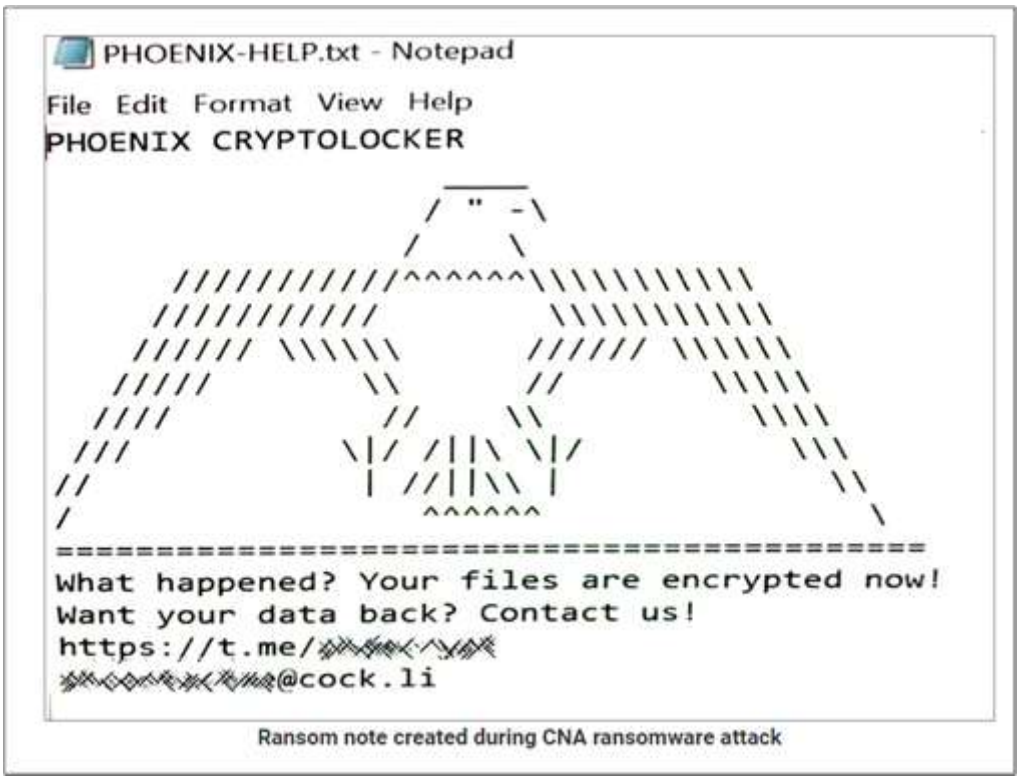
Lo que llama la atención del caso WannaCry es que es un incidente evitable si las empresas y usuarios en general siguen una correcta política de prevención manteniendo los equipos actualizados.

El sector asegurador también ha sufrido ataques de ransomware, en marzo de 2021, CNA, la séptima compañía en volumen de facturación en seguros de daños patrimoniales y reclamación de Estados Unidos sufrió un ataque con el ransomware llamado Phoenix CryptoLocker.

Alrededor de 15.000 dispositivos fueron encriptados, incluyendo los equipos de los empleados que en el momento del ataque estaban trabajando en remoto a través de protocolos VPN.

Todos Los archivos almacenados en los discos duros de los dispositivos afectados fueron cifrados en su totalidad, lo que impidió el acceso a sus propietarios legítimos. El único archivo que se mantuvo accesible fue uno llamado PHOENIX-HELP.txt, el cual contenía el siguiente mensaje.

Fotografía 2. Nota de rescate durante el ataque con ransomware en CNA



Fuente: Bleepingcomputer [6]

Los atacantes exigieron un rescate en criptomonedas de 1.099 Bitcoins (aproximadamente 55 millones de dólares) para restaurar el acceso a los archivos cifrados. CNA cedió a las demandas y pagó el rescate dos semanas después del incidente.

Esta tipología de ataques se prevé que continúe incrementándose, Cybercrime Magazine[7], estima que las pérdidas ocasionadas a nivel mundial por esta tipología de ataques se sitúen en los 265 Billones de dólares en el año 2031.

[6] Bleepingcomputer, Insurance giant CNA hit by new Phoenix CryptoLocker ransomware, Marzo 2023

[7] Cybersecurity Ventures, Boardroom Cybersecurity 2022 Report

Cuadro 4: Estimación del coste mundial de los daños cibernéticos

Fuente: CYBERCRIME (secureworks.com)

6.1.2. Identificación de las vulnerabilidades Cyber en IoT

En los siguientes puntos se identifican las principales vulnerabilidades del IoT asociadas a la ciberseguridad.

Incremento de la superficie de ataque

Cada dispositivo que se añade a una red puede suponer una oportunidad de ataque para un ciberatacante. Contra más dispositivos están conectados a una red más puntos pueden ser atacados, lo que se conoce como superficie de ataque.

Parches de seguridad obsoletos

El software de algunos dispositivos IoT puede estar obsoleto en términos de ciberseguridad incluso antes de que el producto sea comercializado. Los productos que a los pocos meses de su lanzamiento son reemplazados por productos de mejores prestaciones, los denominados productos de ciclo de vida corto, con frecuencia no disponen de parches de actualización de software para corregir las vulnerabilidades de seguridad. Para los fabricantes no es rentable destinar recursos en el desarrollo de soluciones para productos que ya no se comercializan.

Parches de seguridad de fuentes no fiables

Para solventar las deficiencias de seguridad es necesario instalar regularmente parches a los dispositivos, en ocasiones se pueden instalar parches de seguridad que contengas nuevas vulnerabilidades o incluso si las fuentes no son fiables, pueden contener malware.

Vulnerabilidades en Firmware

El firmware o también conocido como soporte lógico inalterable, es el programa básico que controla las funciones de cada uno de los componentes de un dispositivo, determina el funcionamiento lógico de los componentes electrónicos y sirve como base para la instalación de los sistemas operativos e interfaces de usuario. Información sensible como determinadas claves de encriptación también se almacenan en el firmware. Cada circuito electrónico integrado tiene su propio firmware, por lo tanto, los dispositivos complejos que están formados por más de un cirquito integrado tienen varios firmwares.

A diferencia de lo que ocurre con los sistemas operativos y el software en general, el firmware no se actualiza de forma automatizada, por lo general se requiere de conocimientos avanzados para su actualización. Las vulnerabilidades del firmware pueden ser aprovechadas por los ciberdelincuentes como puerta de entrada para atacar dispositivos IoT.

Comunicaciones no cifradas

Los dispositivos IoT intercambian constantemente información con otros dispositivos IoT, para evitar que los datos puedan ser interceptados con facilidad por terceros se utilizan sistemas de cifrado, lo que se conoce como cifrado de extremo a extremo. Solo los usuarios o aquellos dispositivos que conocen las claves de cifrado pueden desencriptar el contenido de la información. Sin embargo, algunos dispositivos IoT no tienen suficiente potencia computacional para utilizar los algoritmos de cifrado y se comunican sin ningún tipo de encriptado.

Esta vulnerabilidad puede ser aprovechada por los ciberdelincuentes para recopilar datos sin el consentimiento del dueño legitimo o como puerta de entrada para atacar otros dispositivos IoT de la red.

Sistemas de autentificación y verificación deficientes

Muchos dispositivos salen de fábrica con una contraseña predefinida, pero en muchos casos, estas contraseñas son extremadamente simples y fáciles de adivinar para cualquier posible atacante. Algunas de las contraseñas más comunes incluyen combinaciones como "Admin", "User", "0000" o "1234".

Algunos fabricantes están más comprometidos con la seguridad y optan por asignar una contraseña única a cada dispositivo utilizando algoritmos que generan una combinación alfanumérica a partir del MAC (Media Access Control). Aunque estas contraseñas parecen más robustas inicialmente, una vez que un atacante descifra el algoritmo de generación de contraseñas, puede reproducirlo y descifrar en cuestión de segundos la contraseña de todos los dispositivos cuyas contraseñas fueron generadas utilizando el mismo algoritmo.

Interfaz web poco segura

La gestión de muchos dispositivos IoT se realiza a través de una interfaz web alojada en un servidor remoto. Sin embargo, si esta interfaz web no se diseña y codifica adecuadamente con las debidas protecciones contra ciberataques, podría convertirse en una puerta de entrada para los ciberdelincuentes, permitiéndoles acceder a otros dispositivos de la red local.

Interfaz Cloud poco segura.

Muchos dispositivos IoT pueden acceder a servicios Cloud, de manera similar a lo que sucede con las interfaces web, si existen vulnerabilidades en los sistemas de protección del Cloud, un ciberatacante podría aprovecharlas para infiltrarse en la red local y atacar el resto de los dispositivos conectados a ella.

Interfaz móvil poco segura.

Los teléfonos móviles también se utilizan para gestionar dispositivos IoT, normalmente la interfaz utilizada es en forma de App. Sin embargo, si la App no está diseñada adecuadamente y presenta brechas de seguridad, podría permitir que un atacante acceda a la red local y comprometa la seguridad de otros dispositivos conectados.

Mecanismos de detección de amenazas insuficientes o inexistentes.

Los dispositivos IoT de baja potencia computacional no son capaces de ejecutar software especializado en la detección de amenazas, como los antivirus. Por lo tanto, es posible que un dispositivo esté infectado sin que haya una forma de detectarlo.

6.1.3. Formas de impacto de los ataques informáticos

Los ataques informáticos están afectando a todos los sectores productivos y a la sociedad en general, pueden tener distintas formas de impacto. En general, se pueden distinguir tres tipos de impactos: directo, indirecto y diferido.

Impacto directo

El impacto directo se refiere a la pérdida del hardware o equipo afectado, los costes asociados a la recuperación de datos y las pérdidas económicas generadas por la paralización de la actividad.

También se tiene que considerar como impacto directo el coste salarial que supone la imposibilidad de que el personal de la empresa pueda realizar sus tareas durante el periodo que los equipos están inoperativos, bien sea porque han sido directamente dañados o desconectados de forma preventiva como media de contención para evitar la propagación del ataque a otros equipos.

Impacto directo

El impacto indirecto se refiere a la pérdida de clientes por el incumplimiento de los compromisos de suministro de productos a servicios como consecuencia de la paralización de la actividad productiva. También se refiere a los costes de revisión, auditoría e implementación de mejores en la seguridad de las instalaciones existentes para evitar ataques futuros.

Impacto diferido

El impacto diferido es el menos evidente, pero puede ser el de mayor repercusión a largo plazo, ya que se refiere al daño reputacional. Los clientes pueden percibir la empresa como poco fiable después de un ataque informático, la pérdida de confianza de los clientes puede generar una progresiva pérdida de cuota de mercado en favor de empresas que les inspiran mayor confianza.

Las inversiones también pueden verse afectadas, ya que los inversos son conocedores del riesgo reputacional y sus consecuencias y pueden optar por invertir en empresas que les ofrezcan menos incertidumbre.

6.1.4. Impacto del Cyber Risk en el sector asegurador

El incremento de la frecuencia en la que se dan los siniestros de carácter ciber, y el potencial coste que se puede derivar de los mismos, como en el caso expuesto de Colonial Pipeline, está empujando al sector asegurador a seguir políticas de suscripción cada vez más restrictivas en esta tipología de riesgos y a centrar las líneas de negocio en productos de ramos tradicionales.

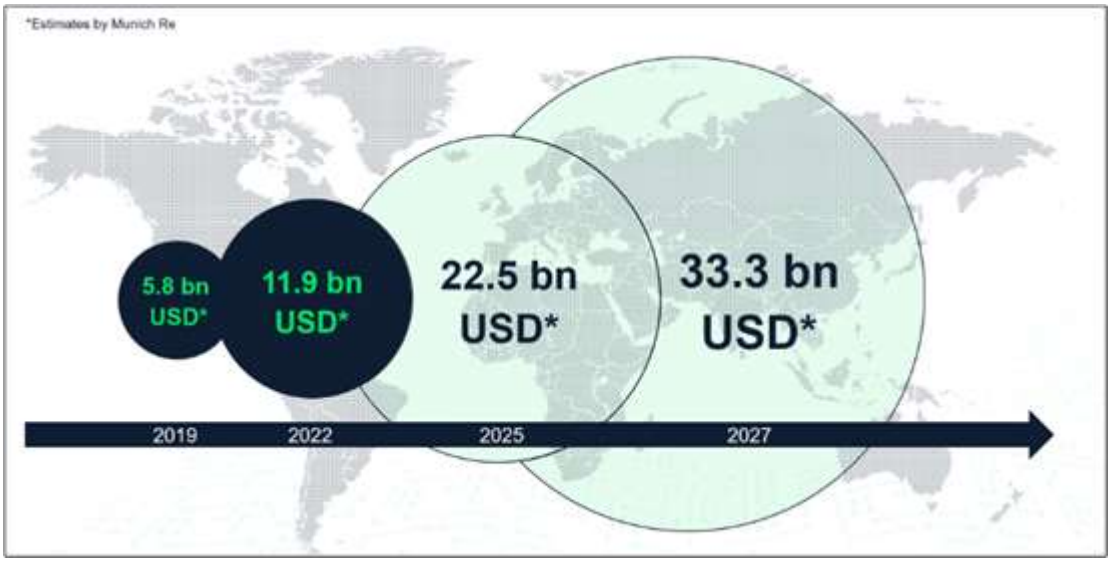
En un futuro altamente conectado, con millones de sensores IoT monitoreando el entorno y reportando datos a sistemas basados en Inteligencia Artificial capaces de detectar patrones de riesgo y alertar para que se tomen las correspondientes medidas preventivas, la frecuencia de ocurrencia de los llamados siniestros tradicionales como incendios, robos, impactos de vehículos y averías de maquinaria se verá significativamente reducida.

En este entorno, la demanda de protección de la sociedad frente a las pérdidas ocasionadas por siniestros se desplazará hacia riesgos carácter cibernético.

Según Munich RE[8] la demanda de protección frente a esta tipología de riesgos se triplicará durante los próximos años.

[8] Munich RE, Cyber insurance: Risks and trends 2023

Gráfica 8: Estimación de la demanda ciber seguro según Munich RE



Fuente: Munich RE, Cyber insurance: Risks and trends 2023

Conforme se incremente la conectividad de la sociedad, más aumentará la necesidad de protección frente a riesgos carácter cibernético, y esto es una oportunidad de negocio para el sector.

El sector asegurador podría aprovechar la oportunidad para buscar socios en otros sectores industriales para unir sinergias. Esta colaboración facilitaría la transferencia de talento y permitiría a las aseguradoras abordar el desafío de la ciberseguridad de manera más proactiva. Se podría reorientar el actual modelo de negocio basado en el pago de siniestros a uno más enfocado a la identificación y mitigación de los riesgos cibernéticos través de programas de gestión de riesgos (risk management).

6.2. Riegos de Interrupción de conectividad

En un entorno de alta conectividad como el que se espera en los próximos años, además de las amenazas relacionadas con ataques cibernéticos, hay que tener en cuenta las consecuencias que se pueden derivar de las interrupciones de conectividad entre los sensores IoT que monitorean el entorno, la Inteligencia Artificial y operadores que analizan los datos recopilados y toman las decisiones y los máquinas y robots que las implementan.

Las máquinas que dependen del feedback permanente de una Inteligencia Artificial ubicada en la nueve o de un operador remoto para funcionar correctamente pueden actuar de forma errónea si se producen cortes en la conectividad.

Tomemos como ejemplo el caso del puerto de Shanghái mencionado en el apartado "*4.2IoT en la Industrias 4.0 (4IR)*" en el que las grúas de contenedores son controladas remotamente. En el supuesto de producirse un corte en el cable de fibra óptica que comunica el puerto con el centro de control, la terminal quedaría paralizaría por completo durante horas.

El impacto de una interrupción de estas características dependería de la duración de esta, pero sin duda su repercusión podría ser significativa tanto a nivel local como global. Además de las perdidas por paralización y los costes de reparación, que probablemente serían los menos significativos, habría que considerar las reclamaciones por los perjuicios ocasionados a terceros, y que en algunos casos podrían ser de elevadas cuantías.

Entre las reclamaciones se podría destacar:

- Reclamaciones por incumplimiento de los compromisos de servicio del puerto con las navieras.
- Reclamaciones derivadas de retrasos en los envíos, así como las consiguientes afectaciones en la cadena de suministro.
- Reclamaciones relacionadas con gastos adicionales de fondeo y consumo de combustible necesario para mantener la posición de los buques.
- Reclamaciones derivadas al aumento de los costos de almacenamiento de contenedores, especialmente en productos perecederos.
- Reclamaciones por el aumento de gastos de tripulación, incluyendo sueldos y manutención.
- Reclamaciones por del incumplimiento de los compromisos de servicio de la naviera, que también serían repercutido al puerto.

Además de las interrupciones de conexión de larga duración, también hay que tener en cuenta las interrupciones breves y los microcortes. Incluso interrupciones de microsegundos de duración pueden provocar que las instrucciones transmitidas a las máquinas sean imprecisas desencadenando actuaciones incorrectas que ocasionen daños, especialmente en aplicaciones que requieren de bajas latencias.

Por ejemplo, en entornos de cirugía teleasistida, donde los movimientos de los brazos robóticos tienen que extremadamente precisos y coordinados, un microcorte en la comunicación podría alterar la secuencia de instrucciones y provocar errores graves en la intervención quirúrgica, con consecuencias potencialmente mortales para el paciente.

Las interrupciones pueden tener múltiples orígenes, como una avería en el sistema de telecomunicaciones del proveedor del servicio, el paso de un vehículo gubernamental dotado de inhibidoras de frecuencia, un sabotaje

malintencionado mediante el uso de equipos generadores de interferencias o inhibidores de frecuencia, daños en el cableado de fibra óptica debido a unas obras cercanas, por mencionar algunos ejemplos.

6.3. Riesgos internos del sistema

El riesgo interno se refiere a posibles fallas o mal funcionamiento del hardware que controla un dispositivo, ya sea debido al uso y desgaste, o a la incompatibilidad entre las versiones del software después de un proceso de actualización.

También hay que tener en cuenta que los sesgos o errores de programación en los algoritmos de Inteligencia Artificial pueden llevar a que los equipos operen de manera incorrecta en ciertas circunstancias

6.4. Riesgos en el tratamiento de datos personales

Los dispositivos IoT recopilan, almacenan y transmiten datos constantemente, es importante destacar que estos datos pueden ser en algún momento utilizados por terceros, tales como proveedores de servicios, desarrolladores de hardware y software, servicios en la nube, Inteligencias Artificiales etc.

Se tiende a pensar que los dispositivos IoT solo recopilan datos personales en el ámbito doméstico y de salud, sin embargo, en el sector industrial también es posible que se maneje un importante volumen de datos personales, los cuales también están sujetos al Reglamento General de Protección de Datos (RGPD).

El constante incremento en el uso de dispositivos IoT implica un aumento en el volumen de datos que se manejan, lo que representa un importante desafío para la protección de datos, especialmente en un sector tan regulado como el asegurador.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales adapta el RGPD a la normativa española y exige a los responsables y encargados del tratamiento que tomen medidas para garantizar la protección de los datos personales recopilados a través de medios como el IoT.

La regulación es muy clara en lo relativo a tratamiento de los datos personales, sin embargo, dado que puede haber varios actores involucrados en el proceso, como el fabricante del dispositivo, el fabricante del hardware, el desarrollador del software, la inteligencia artificial que analiza los datos, un intermediario como por ejemplo una aseguradora que utiliza los datos para ofrecer un producto específico a un cliente, resulta difícil determinar quién es responsable en caso de una brecha de seguridad.

Además, hay que tener en cuenta que en muchos casos en los que interviene una Inteligencia Artificial ni los propios desarrolladores del algoritmo de aprendizaje pueden determinar con exactitud que usos se da a los datos recopilados.

Teniendo en cuenta que el destino final de los datos en muchos casos no es completamente transparente, una brecha de seguridad o un uso indebido en uno de los eslabones de la cadena podría afectar la imagen reputacional del resto.

Las restricciones regulatorias relacionadas con la protección de datos personales pueden representar un obstáculo para el desarrollo del potencial del IoT en una economía altamente regulada como la europea.

7. Mitigación de los riesgos asociados al IoT

7.1. Mitigación riesgos Cyber

7.1.1. Mecanismos de detección de ataques Cyber

Los IDS (Intrusion detection systems) o sistemas de detección de intrusos son sistemas que monitorean constantemente el tráfico de la red de una organización en búsqueda de actividad maliciosa o potencialmente dañina para los sistemas que protegen.

Existen sistemas de detección de intrusos (IDS) basados en firmas y en comportamientos. Si bien los sistemas basados en firma tienen una alta capacidad de detección cuando se trata de ataques ya conocidos, su capacidad se ve muy limitada cuando se trata de ataques que todavía no han sido descubiertos

IDS Basados en firma IDS (Signature-based IDS)

El sistema de detección de intrusiones basado en firmas funciona mediante la comparación de paquetes o secuencias de datos con una base de datos de firmas de ataques previamente conocidos. Si se encuentra una coincidencia, se genera una alerta de posible intrusión en el sistema.

Este método es efectivo para detectar ataques ya conocidos y patrones de tráfico que se han identificado previamente como maliciosos. Sin embargo, esta solución no es eficaz para detectar ataques nuevos o desconocidos, ya que no hay ninguna firma de ataque existente para comparar con los paquetes de datos entrantes. Además, los atacantes pueden utilizar técnicas de evasión para evitar la detección de los sistemas basados en firmas.

IDS Basados en comportamiento (Behaviour-based IDS)

Los sistemas de detección de intrusiones basados en comportamientos utilizan algoritmos de aprendizaje automático y análisis estadístico para construir un modelo de comportamiento normal de la red y detectar patrones que se desvían de lo normal. A diferencia de los sistemas basados en firmas, no buscan patrones específicos de ataque, sino que identifican cualquier comportamiento que se salga de lo normal. Estos sistemas son especialmente útiles para detectar ataques nuevos que todavía no han sido reportados.

No obstante, es importante tener en cuenta que estos sistemas pueden generar falsos positivos. Esto puede suceder cuando se detecta un comportamiento inusual de la red que no se debe a tráfico malicioso, sino a eventos externos que no han sido contemplados por los algoritmos de comportamiento.

Parece que, una combinación de los dos sistemas podría ser la solución más adecuada. No obstante, la potencia computacional de los dispositivos IoT suele ser limitada, lo que no solo impide su ejecución simultánea, sino que en muchas ocasiones no es posible ejecutar ninguno de los dos sistemas.

7.1.2. Recomendaciones de prevención

Los sistemas de IDS pueden contribuir a reducir la severidad de los ataques informáticos al permitir detectarlos en la fase temprana, pero para garantizar una mayor seguridad es imprescindible un sistema de prevención robusto y correctamente planificado.

A continuación, se detallan algunos de los mecanismos de prevención que pueden resultar de interés para fortalecer la seguridad de los dispositivos IoT.

Minimizar superficie de ataque

Los dispositivos IoT pueden tener puertos abiertos con servicios activos que no son necesarios para la función que cumplen. Mantener activos servicios no necesarios expone el dispositivo a posibles ataques innecesarios. Por lo tanto, es recomendable solo mantener activos los servicios necesarios para minimizar la superficie de ataque.

Política de actualización de software

Es necesario mantener actualizado el software de los dispositivos IoT para dar respuesta a las nuevas amenazas de seguridad que constantemente aparecen. Por este motivo, es recomendable utilizar dispositivos cuyos fabricantes se comprometen a proporcionar actualizaciones durante toda la vida útil del producto.

Además, es importante asegurarse de que los parches de seguridad que se instalan son legítimos y no están infectados por malware o introducen nuevas vulnerabilidades, se recomienda solo instalar parches que procedan del fabricante del dispositivo o de fuentes de fiabilidad contrastada.

Uso de blockchain

El Blockchain es una tecnología que se utiliza para almacenar y compartir información de manera segura y transparente sin la necesidad de un intermediario centralizado. La información en lugar de almacenarse en una base datos centralizada, se divide en bloques que están enlazados de forma segura mediante criptografía.

Esta tecnología se ha popularizado gracias a su uso en criptomonedas como el Bitcoin, pero tiene un elevado potencial en lo relativo a verificación de identidad digital y gestión de datos.

En las redes de comunicación de IoT, el uso del Blockchain es una solución potencialmente más fiable que las soluciones de criptografía de clave pública como TLS (Transport Layer Security). La principal ventaja del Blockchain reside en que proporciona un control más fiable sobre el acceso, inalterabilidad y uso de los datos.

Además, al ser una tecnología descentralizada, permite realizar copias descentralizadas de los datos, lo que representa un gran plus de seguridad ante ataques tipo ransomware, ya que si un dispositivo se ve comprometido, la información almacenada en él puede ser recuperada desde cualquier otro dispositivo en la red.

Autentificación adecuada

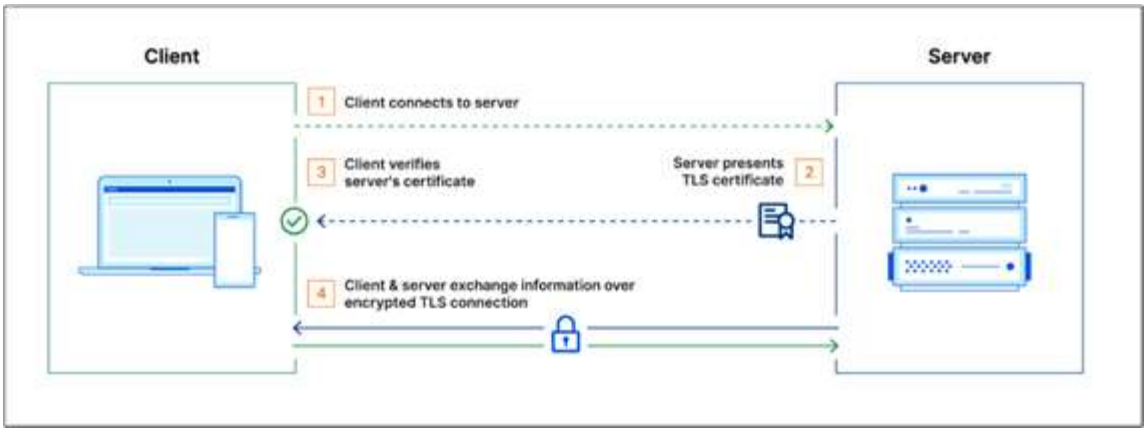
Para crear sistemas de comunicaciones seguros y fiables es imprescindible utilizar protocolos de autentificación adecuados.

Es recomendable que cada dispositivo IoT sea autenticado mediante protocolos estándar de la industria como 802.1x (EAP), RADIUS o OTP/CHAP etc... Una vez autenticados, los dispositivos deberían utilizar protocolos criptográficos que garanticen que las comunicaciones se efectúan de forma cifrada, y solo pueden ser descifradas por las partes autorizadas. Esto dificulta los ataques de espionaje por parte de los hackers con fines maliciosos y protege la integridad y confidencialidad de los datos transmitidos.

Entre los sistemas de autentificación destacar el TLS (Transport Layer Security) y el mTLS (mutual Transport Layer Security)

En los sistemas de autentificación TLS (Transport Layer Security), el servidor tiene un certificado TLS y un par de claves público – privadas , mientras que el cliente no. El proceso de TLS funciona tal y como se resume en el siguiente esquema:

Cuadro 5: Esquema autentificación TLS



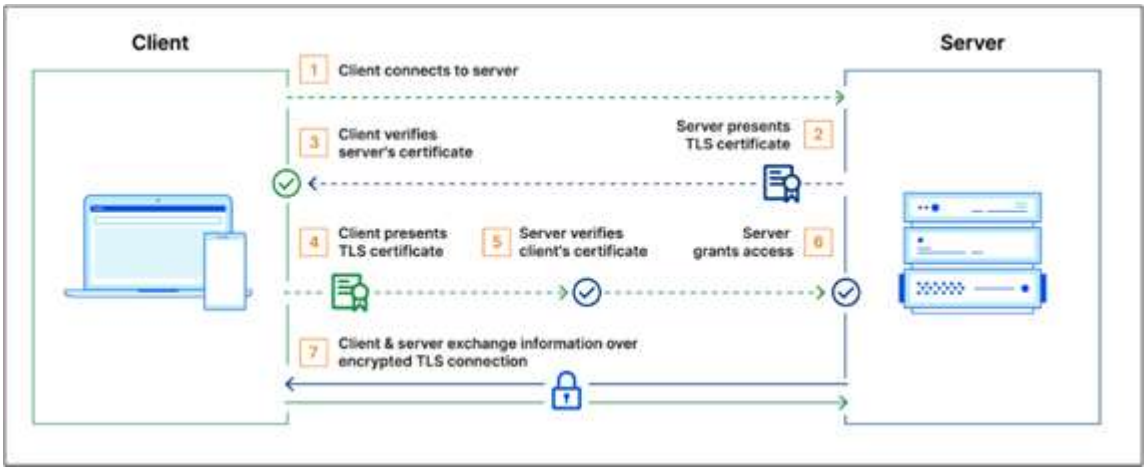
Fuente: Cloudflare.com

1. El cliente se conecta al servidor.
2. El servidor responde enviando su certificado TLS al cliente. El certificado incluye la clave pública del servidor, junto con otra información como el nombre de dominio del servidor.
3. El cliente recibe el certificado del servidor y realiza varias verificaciones para verificar su autenticidad, comprueba también que el nombre de dominio en el certificado coincida con el servidor al que pretendía conectarse
4. Si el certificado del servidor pasa todas las verificaciones, el cliente y el servidor acuerdan un conjunto de algoritmos de cifrado y generan claves compartidas para establecer una conexión cifrada.

Una vez que se ha establecido la conexión segura, tanto el cliente como el servidor pueden intercambiar información a través de la conexión TLS, que está encriptada y protegida contra escuchas no autorizadas.

Los sistemas mTLS (mutual Transport Layer Security) son una evolución del TLS (Transport Layer Security) en el que servidor y cliente se autentican utilizando su par de claves público - privadas. El esquema de funcionamiento del protocolo se esquematiza en el cuadro siguiente.

Cuadro 6: Esquema autentificación mTLS



Fuente: Cloudflare.com

1. El cliente se conecta al servidor.
2. El servidor responde enviando su certificado TLS al cliente. El certificado incluye la clave pública del servidor, junto con otra información como el nombre de dominio del servidor.

3. El cliente recibe el certificado del servidor y realiza varias verificaciones para verificar su autenticidad, comprueba también que el nombre de dominio en el certificado coincida con el servidor al que pretendía conectarse

4. El cliente presenta su certificado TLS.

5. El servidor verifica el certificado del cliente.

6. El servidor concede el acceso.

7. El cliente y el servidor intercambian información a través de una conexión TLS cifrada.

Fog computing

A diferencia del cloud computing, en el que los datos recopilados por los dispositivos IoT son transferidos a centros de tratamiento remoto, el fog computing utiliza la potencia computacional de dispositivos intermedios, como routers o gateways, para procesar y almacenar los datos. Solo se envían a la nube los datos relevantes para su almacenamiento y procesamiento a largo plazo.

El fog computing se podría definir como un modelo de computación distribuida que procesa los datos cerca de los dispositivos que los generan y solo transfiere a la nube los datos de interés.

Este enfoque reduce significativamente el tráfico de datos hacia la nube y permite que los datos sensibles se procesen localmente en un entorno más controlado.

Filtros DNS

Los dominios de internet son nombres que identifican de manera inequívoca los sitios web. Por ejemplo, el dominio “https://web.ub.edu” se corresponde con la página principal de web de la Universitat de Barcelona y no puede ser utilizado por ningún otro sitio.

Los sistemas de filtrado DNS (Domain Name System) funcionan como un filtro de seguridad que permite a los dispositivos IoT conectarse únicamente a dominios que han sido previamente evaluados y catalogados como sitios de confianza. De esta manera, se evita que los dispositivos establezcan conexiones con sitios web de dudosa confianza o potencialmente peligrosos, como podría ser el dominio de un atacante.

Uso de firewalls

Los firewalls son soluciones informáticas para proteger una red informática de accesos no autorizados o actividades potencialmente dañinas. Funcionan como una barrera o filtro que controla el tráfico de datos entre internet y la red interna.

El firewall examina los paquetes que entran y salen de la red interna y en función de unas reglas de seguridad predefinidas permiten o bloquean el tráfico. Las reglas pueden basarse en IP, puertos, protocolos de conexión o cualquier otro criterio de seguridad.

Auditorías regulares

Para garantizar un correcto funcionamiento de los sistemas es imprescindible realizar regularmente auditorias que permitan detectar vulnerabilidades y aplicar las mejoras pertinentes. Para llevar a cabo este proceso, se utilizan herramientas de auditoría de seguridad, las cuales son programas informáticos diseñados específicamente para simular ataques y evaluar la robustez de los sistemas en términos de seguridad.

Conexiones seguras

Para mantener la seguridad de la red hay que asegurar que todos los dispositivos se conectan a la red local, y que no se enlazan a través de redes de terceros. De esta manera se garantiza que todas las conexiones pasan a través del firewall y se reduce el riesgo de que sean hackeados remotamente.

7.2. Mitigación de los riesgos internos

Los riesgos internos tal y como ocurre con otros riesgos, no pueden ser eliminados por completo, pero si mitigados. Una forma de mitigarlos es primar el uso de equipos que dispongan de sistemas redundantes en los procesos críticos.

Por ejemplo, en el caso de un vehículo autónomo, la detección de obstáculos es un proceso crítico. Un enfoque para reducir el riesgo interno en este sistema es emplear redundancia en los sensores de detección de obstáculos. Un vehículo que utiliza un sensor de ultrasonidos para contrastar el campo de visión de una cámara tiene una tasa de fiabilidad superior en comparación con aquellos que dependen únicamente de una cámara de visión.

7.3. Mitigación de riesgos de interrupción conectividad

Las interrupciones de conectividad pueden deberse tanto a fallos en los componentes de la red, hardware y software, como a interferencias externos.

Con independencia de la tecnología utilizada, disponer de un correcto plan de mantenimiento es indispensable para prevenir que fallo inesperado de cualquiera de los elementos que componen una red ocasione una interrupción en la conectividad.

En relación con los riesgos de interrupción de conectividad relacionados con interferencias externas una alternativa para minimizarlos es el empleado de sistemas cableados. Estos sistemas son poco susceptibles a interferencias externas lo que les convierte en una alternativa fiable, especialmente en aplicaciones críticas.

Sin embargo, hay que tener en cuenta que los sistemas cableados son muy estáticos, esto supone una limitación, especialmente en entornos en los que se efectúan constantemente cambios y se requiere flexibilidad, como por ejemplo en las líneas de producción. Los trabajos de recableado de los sensores IoT y los equipos robotizados además de ser lentos son costosos en términos económicos.

En numerosas aplicaciones las soluciones cableadas no son prácticas, en los casos en los que se requiera el empleo de soluciones inalámbricas se recomienda priorizar el uso de aquellas menos susceptibles a interferencias externas, como, por ejemplo:

- Wi-Fi 6 (802.11ax), es el último estándar wi-fi, además de tener un mejor rendimiento en zonas con alta densidad de dispositivos y ofrecer mejor cobertura, es menos susceptible a interferencias.
- 5G, la capacidad de cambiar de banda de frecuencia, así como la posibilidad para transmitir por canales no saturados, le ofrece mayor robustez frente a las interferencias en comparación con las tecnologías que le preceden.
- LoRaWAN, permite comunicaciones de largo alcance con un bajo consumo, por lo que es de interés para sistemas redundantes de seguridad o que tengan que ser alimentados por baterías en caso de corte de suministro eléctrico.
- Bluetooth 5.0, la última versión de Bluetooth mejora la velocidad y el rango de la conexión, y también introduce una nueva característica llamada "LE Coded" que aumenta la fiabilidad de la conexión en entornos con mucha interferencia.

- NFC, empleada principalmente en entornos de corto alcance, debido a su corto alcance es de interés en entornos en los que el espectro de radiofrecuencias está saturado.

8. Impacto del IoT en el enfoque GRC

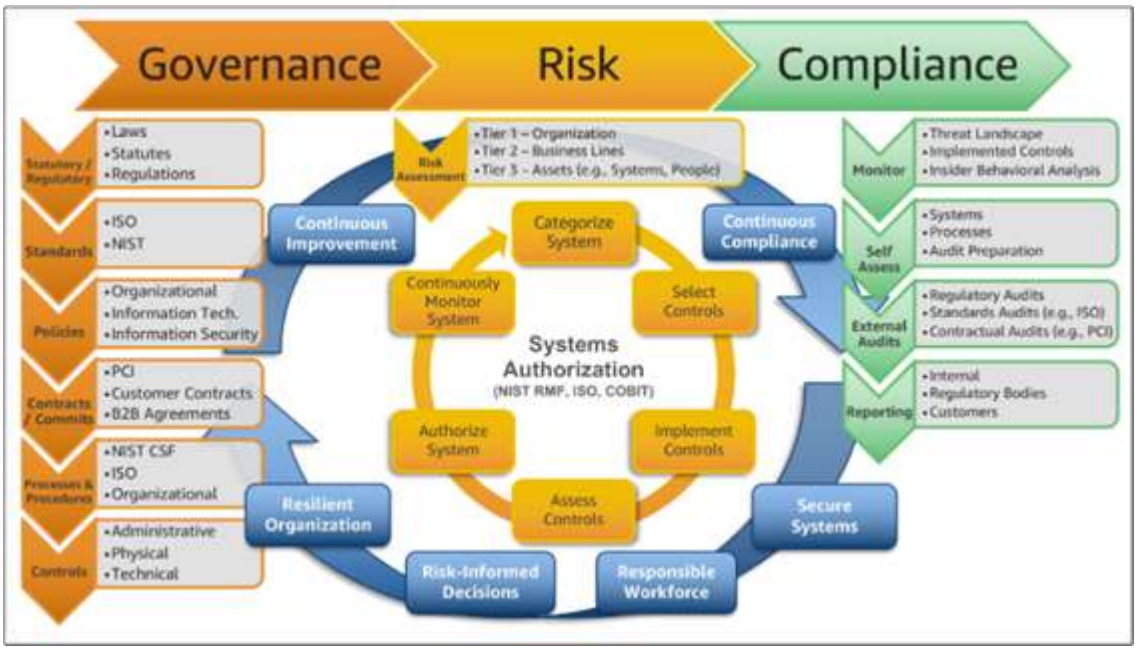
La gobernanza de una empresa es el conjunto de políticas y reglas que se usan para lograr los objetivos empresariales. Determina las responsabilidades de la junta directiva, la alta dirección y todas las partes que intervienen. Una buena gobernanza implica ética, transparencia, administración responsable de recursos, compromiso social y medioambiental entre otros.

Las empresas para garantizar su estabilidad y continuidad a largo plazo tienen que anticiparse y protegerse frente a cualquier riesgo que les puede afectar significativamente, que pueden ser; financieros, legales, estratégicos, de seguridad, reputacionales entre otros.

Además, las empresas tienen que cumplir con los requisitos legales establecidos por las autoridades regulatorias, así como con las políticas corporativas internas.

Un correcto enfoque GRC (gobernanza, riesgo y cumplimiento) tiene que lograr que las tecnologías se alineen con los objetivos de la empresa, a la vez que se gestionan los riesgos de manera eficiente para dar cumplimiento a las obligaciones establecidas por el legislador.

Cuadro 7: Esquema GRC (Governance Risk Compliance)



Fuente: Amazon AWS

La irrupción del Internet de las cosas (IoT) y otras tecnologías de frontera en el sector asegurador cambiará la manera en que se gestiona y procesa la información, lo que implica que las GRC deberán de reenfocarse

Tradicionalmente, las aseguradoras han utilizado la matemática actuarial para definir los modelos de previsión de siniestralidad y evaluación de riesgos. Estas metodologías de cálculo son transparentes y arrojan resultados que pueden ser explicados y comprendidos con relativa facilidad. Sin embargo, para aprovechar el potencial del volumen de datos generado por el IoT es necesario el uso de sistemas de inteligencia artificial.

El empleo de Inteligencia Artificial ofrece una mejora significativa en la fiabilidad, rapidez, y sencillez de creación de nuevos modelos de previsión siniestral. Sin embargo, su uso plantea inconvenientes en términos de transparencia.

Tanto si los modelos de inteligencia artificial utilizan algoritmos de autoaprendizaje como de aprendizaje por refuerzo, su funcionamiento por lo general es de caja negra, lo que significa que los resultados que arrojan son poco transparentes y muy difíciles de explicar. Esto supone un problema para las aseguradoras, porque además de tener que justificar sus decisiones de aceptación de riesgos y previsión de siniestros ante el regulador, también tienen que cumplir con la normativa en materia de tratamiento de datos personales.

Debido a la mayor complejidad de los modelos basados en Inteligencia Artificial se presentan nuevos riesgos en comparación con los modelos estadísticos tradicionalmente utilizados en el sector asegurador. Los principales riesgos son los siguientes:

Riesgo de efecto caja negra

En los modelos creados por Inteligencia Artificial resulta complicado conocer la metodología de cálculo empleada, los resultados son difíciles de contrastar e interpretar, ya que son modelos muy poco transparentes.

Esto puede ocasionar muchos problemas a las aseguradoras, como, por ejemplo, que se rechace la aceptación de un determinado riesgo sin que el suscriptor pueda entender el razonamiento detrás de la no aceptación.

Riesgo en el tratamiento de información sensible

Para proteger la privacidad de las personas los datos se pueden anonimizar. Sin embargo, si se reagrupan grandes cantidades de datos anonimizados, existe el riesgo de revelar información que permita identificar a individuos concretos.

Riesgo de uso de modelos de AI sesgados

Los datos utilizados para entrenar los modelos de Inteligencia Artificial son la base del modelo, lo que significa que cualquier sesgo que presenten puede ser amplificado en las predicciones del modelo. Además, en los algoritmos de aprendizaje por refuerzo, donde se requiere la validación humana de los resultados, la subjetividad de los validadores puede inducir sesgos en el algoritmo. Los sesgos de los algoritmos pueden ser muy sutiles y difíciles de detectar.

Riesgo de inestabilidad de los modelos de AI

Los modelos de IA son muy complejos y funcionan como una caja negra. Si la información que se introduce difiere de la utilizada en el entrenamiento, existe el riesgo de que se generen inestabilidades en el modelo y que las predicciones pierdan precisión. Esta anomalía puede pasar desapercibida durante mucho tiempo si no se emplean las herramientas adecuadas para monitorear posibles desviaciones en el modelo.

Riesgo de incumplir el RGPD

Los sistemas basados en inteligencia artificial necesitan grandes cantidades de datos para funcionar correctamente, y estos datos pueden proceder de diversas fuentes. En consecuencia, puede ser difícil asegurar que el propietario legítimo de los datos haya otorgado su consentimiento para que se utilicen en un modelo específico.

Riesgo ciber

La implementación de sistemas de inteligencia artificial llevará a una mayor dependencia tecnológica de las empresas aseguradoras y, como resultado, aumentará el riesgo de ataques cibernéticos. La superficie de ataque se incrementará y surgirán más puntos vulnerables que los atacantes pueden aprovechar. Además, en caso de que los sistemas de inteligencia artificial sean atacados, el impacto podría ser más profundo y perjudicial para la organización.

9. Desafíos en el Mercado de Seguros

9.1. Limitaciones en la capacidad de absorción de riesgo

El conflicto bélico ente Rusia y Ucrania y los posibles ataques cibernéticos relacionados ha puesto en el punto de mira las clausulas de exclusión por ataques cibernéticos.

En agosto de 2022 Lloyd's de Londres, uno de los principales mercados de seguro a nivel mundial, publica un boletín de mercado[9] indicando que a partir del 31 de marzo de 2023 las aseguradoras de Lloyd's excluirán en las pólizas independientes las pérdidas ocasionadas por ataques cibernéticos efectuados o respaldados por un estado soberano que perjudiquen seriamente el funcionamiento de otro estado, tanto en contexto de guerra declarada como fuera de este contexto.

Lloyd's pone de manifiesto la facilidad en la que un estado puede orquestar un ataque cibernético a escala global, y advierte que, si esta tipología de riesgo no es correctamente gestionada, el mercado de los seguros cibernéticos podría quedar expuesto a un riesgo sistémico que los sindicados de Lloyd's tendrían dificultades para afrontar.

En la práctica, esta modificación no implica grandes cambios. Los daños ocasionados como consecuencia de ataques en contexto de guerra ya están excluidos en la mayoría de las pólizas cibernéticas. En cuanto a los daños ocasionados fuera del contexto de guerra, su exclusión solo será de aplicación si dichos ataques causan un perjuicio grave a las capacidades operativas de otro estado, afortunadamente, esta tipología de ataques es poco frecuentes.

Sin embargo, Lloyd's evidencia la existencia de un riesgo sistémico en el sector asegurador, dado que las pérdidas resultantes de un ataque global, perpetrado ya sea por un estado o por cualquier otra organización, como un grupo terrorista, podrían superar la capacidad de cobertura de las compañías aseguradoras.

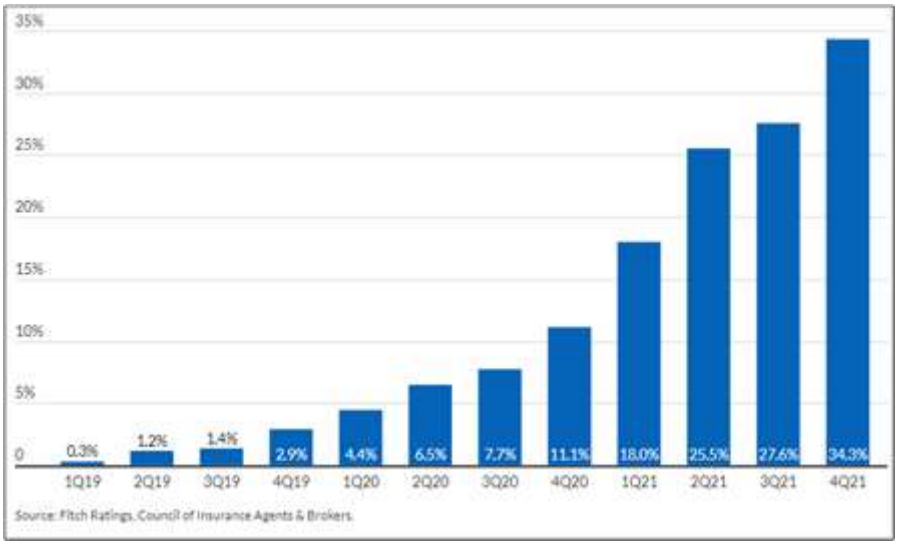
[9] LLOYD'S Market Bulletin Ref: Y5381

9.2. Alternativas de transferencia de riesgo

En una sociedad cada vez más tecnológica la demanda de seguro para riesgos ciber está en constante aumento además la frecuencia y severidad de los ataques se está incrementado.

Como consecuencia, las aseguradoras están transfiriendo el incremento de riesgo a las reaseguradoras, lo que implica un incremento en las primas de reaseguro. Teniendo en cuenta que las aseguradoras quieren mantener sus márgenes de rentabilidad, el incremento de costes en las prestaciones es directamente repercutido en las primas que las empresas tienen que pagar al contratar un seguro cibernético en el mercado primario.

Gráfica 9: Evolución de las primas para riesgo ciber en U.S.



Fuente: Fitch Ratings, Council of Insurance Agents & Brokers

Además, las aseguradoras están tomando conciencia de la posibilidad de ocurrencia de un evento cibernético de alcance global que supere la capacidad de aseguramiento sectorial, en consecuencia, están limitando su exposición, lo que implica que algunos riesgos se quedarán sin cobertura.

En un contexto en el que la demanda de seguros para riesgos cibernéticos está en aumento y la oferta es limitada, se hace necesario explorar alternativas que permitan ampliar la capacidad de aseguramiento para satisfacer las necesidades de protección de la sociedad.

Una alternativa que se podría explorar son los bonos de catástrofe. Los bonos catástrofe son un instrumento financiero emitido por las aseguradoras. El emisor del bono obtiene dinero de los inversores y a cambio paga un interés durante la duración del bono.

En el supuesto de ocurrir un evento catastrófico, como un huracán, un terremoto u otro tipo de desastre, el emisor de los bonos de catástrofe utiliza el dinero captado para cubrir los daños ocasionados por dicho siniestro, una vez los gastos han sido sufragados, cualquier excedente de dinero que quede disponible se devuelve al inversor.

Los bonos de catástrofe son instrumentos financieros atractivos para los inversores debido a la alta rentabilidad que ofrecen. Sin embargo, hay que tener en cuenta que estos bonos son productos de riesgo, en caso de que ocurra un evento catastrófico, los inversores pueden llegar a perder parte de su inversión.

Del mismo modo que algunas aseguradoras limitan su exposición a eventos climatológicos adversos o pandemias transfiriendo parte del riesgo a inversores mediante bonos catastróficos, se podría limitar la exposición de las aseguradoras a un evento de carácter cibernético de gran alcance valiéndose del mismo instrumento financiero.

.

10. Conclusiones

En los últimos años, especialmente a partir del despliegue del 5G, se han logrado niveles de conectividad que permiten aprovechar los beneficios del IoT. Sin embargo, en el sector asegurador su impacto todavía sigue siendo limitado, el momento disruptivo llegará cuando se logre combinar de manera efectiva el IoT con la Inteligencia Artificial.

La capacidad de los sistemas de IA para analizar millones de datos, fotos y videos recopilados por los sensores IoT, tendrá un impacto disruptivo en los procedimientos actuales de suscripción de riesgos, modelos matemáticos e incluso en los protocolos de valoración de daños en caso de siniestro. Es muy probable que las actuales sistemáticas de cálculo queden obsoletas, tal como ocurrió con las calculadoras cuando aparecieron las hojas de cálculo de ordenador.

La combinación del IoT y la IA permitirá ofrecer productos altamente personalizados y adaptados a las necesidades del cliente y mejorará la precisión de los modelos actuariales de comportamiento siniestral, lo que se traducirá en tarifas más atractivas para el cliente objetivo.

La implementación de modelos de comportamiento siniestral de alta precisión permitirá anticipar con un elevado porcentaje de fiabilidad la ocurrencia de determinados siniestros, esto permitirá a las aseguradoras alertar a sus asegurados para que tomen medidas preventivas orientadas a reducir su exposición al riesgo.

Este nuevo enfoque puede transformar la concepción tradicional del seguro, evolucionando de un modelo muy centrado en la aceptación y transferencia de riesgos a un modelo más orientado a la prevención y mitigación de riesgos.

Además de ser una oportunidad de negocio en un nicho de mercado actualmente no cubierto, los servicios de prevención pueden permitir a las compañías aseguradoras incrementar la frecuencia de interacción con sus clientes, esto también puede ser una oportunidad para reforzar los vínculos emocionales con los clientes, incrementar su fidelidad y reducir las tasas de anulaciones de pólizas.

En los próximos años el IoT y los avances en Inteligencia Artificial permitirán la automatización de los procesos de tramitación y valoración de daños en determinadas tipologías de siniestros. La automatización será especialmente de aplicación en los siniestros de frecuencia, en los que en un elevado porcentaje de casos el único humano interviniente será el técnico que efectúa la reparación, los peritos y tramitadores solo actuarán en aquellos siniestros singulares y de mayor complejidad. A pesar de que las mejoras tecnologías permitan reducir la intervención humana, es importante tener en cuenta que

para determinados segmentos del público objetivo la interacción con personas seguirá aportando valor añadido a la experiencia.

En este contexto, las aseguradoras deberán de velar por disponer de redes de reparadores altamente profesionalizados y buscar el equilibrio entre la reducción de costes mediante la automatización de procesos y el valor añadido que aporta para los clientes la interacción con personas.

La digitalización de la sociedad está difuminando los límites entre los diferentes sectores industriales, lo que puede permitir a empresas de otros sectores incursionar en el negocio asegurador.

Es probable que las grandes empresas tecnológicas como Alphabet, Amazon, IBM, que han desplegado millones de dispositivos IoT en el ámbito doméstico e industrial y están desarrollando sistemas avanzados de inteligencia artificial, busquen aprovechar su ventaja competitiva frente a las aseguradoras tradicionales y exploren vías para introducirse en el sector asegurador. No obstante, la regulación en materia de tratamiento de datos personales puede suponerles una barrera de entrada en algunos mercados altamente regulados como el europeo.

La difuminación de los límites sectores también representa una oportunidad para las aseguradoras para expandirse y captar una parte del negocio de otros sectores. Para aprovechar estas oportunidades, es necesario redefinir el modelo de negocio actual y adoptar un enfoque de ecosistema, en el que se colabore con socios comerciales de contextos diferentes al sector asegurador.

La implementación de tecnologías relacionadas con el IoT puede mejorar la siniestralidad de ciertos riesgos y generar oportunidades de negocio en nuevos nichos de mercado. Sin embargo, es importante tener en cuenta que esta transformación digital también implica un aumento significativo de los riesgos cibernéticos.

El incremento de los riesgos de ciberseguridad y la creciente adopción de tecnologías de Inteligencia Artificial clasificadas como de alto riesgo según la AIA (AI Act), exigirá a las compañías aseguradoras un reenfoque de las estrategias GRC (Gobierno, Riesgo y Cumplimiento).

La actual oferta de protección frente a riesgos de carácter cibernético es inferior a la demandada por la sociedad, especialmente para eventos de gran magnitud. Para evitar que determinados riesgos se queden desprotegidos, es necesario incrementar la capacidad de aseguramiento sectorial explorando alternativas como los bonos catástrofe. De este modo, se podría transferir parcialmente el riesgo cibernético a inversores a la vez que se incrementar la capacidad sectorial.

En base al análisis efectuado en los párrafos anteriores, concluir que la combinación del IoT y la Inteligencia Artificial tiene un potencial disruptivo en el sector asegurador. Su entrada será inevitable, y actuará como catalizador para la transformación sectorial ocasionados cambios profundos en el modelo de negocio de las aseguradoras tradicionales

Además, ante la posibilidad de que el desarrollo de estas tecnologías sea más rápido de lo previsto, es necesario que las compañías aseguradoras se anticipen y tomen medidas proactivas para no perder ventaja competitiva en un mundo cada vez más digital y tecnológico.

11. Bibliografía

Artículos:

Bill Corcoran, Mengxi Tan2, Xingyuan Xu 2, Andreas Boes, Jiayang Wu2, Thach G. Nguyen3,Sai T. Chu, Brent E. Little, Roberto Morandotti, Arnan Mitchell, David J. Moss. “Ultra-dense optical data transmission over standard fibre with a single chip source”, Nature Communications, vol.11, págs.1-7

Muhammad Shafiq, Zhaoquan Gu ,Omar Cheikhrouhou ,Wajdi Alhakami, Habib Hamam. "The Rise of “Internet of Things”: Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks”

Fuentes de internet:

¿Qué es, Para qué Sirve y Cómo Funciona el Arpanet? - Historia del Internet <https://miracomosehace.com/que-es-para-que-sirve-como-funciona-arpanet-historia-internet/>
(Fecha de consulta: 23 de enero de 2023).

The History of the Mobile Phone - The Washington Post <https://www.washingtonpost.com/news/the-switch/wp/2014/09/09/the-history-of-the-mobile-phone>
(Fecha de consulta 28 de enero de 2023)

¿Qué es la red GSM y cómo funciona? - CCM <https://es.ccm.net/contents/681-estandar-gsm-sistema-global-de-comunicaciones-moviles>
(Fecha de consulta 29 de enero de 2023)

Xataka móvil, Del 1G al 5G <https://www.xatakamovil.com/conectividad/1g-al-5g-asi-funcionan-redes-moviles-todo-que-cambia-cada-salto-generacion>
(Fecha de consulta 30 de enero de 2023)

Ministerio de Asuntos Económicos y Transformación Digital <https://avancedigital.mineco.gob.es/banda-ancha/tecnologias/movil/Paginas/UMTS.aspx>
(Fecha de consulta 30 de enero de 2023)

Nature communications - Ultra-dense optical data transmission <https://www.nature.com/articles/s41467-020-16265-x>
(Fecha de consulta 31 de enero de 2023)

5G: qué es y qué diferencias tiene con el 4G | xataka.com <https://www.xataka.com/basics/que-5g-que-diferencias-tiene-4g>
(Fecha de consulta 02 de febrero de 2023)

El 5G ya permite realizar cirugía teleasistida
<https://www.xataka.com/medicina-y-salud/5g-permite-realizar-cirugia-teleasistida-china-completa-exito-primera-operacion-animales>
(Fecha de consulta 02 de febrero de 2023)

¿No te basta el 5G? Pues ya los hay pensando en 6G y 7G (nobbot.com)
<https://www.nobbot.com/futuro/5g-6g-7g/>
(Fecha de consulta 09 de febrero de 2023)

Narrowband – Internet of Things (NB-IoT)
<https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/>
(Fecha de consulta 09 de febrero de 2023)

Big Data - Expertos en IIC (uam.es)
<https://www.iic.uam.es/big-data/>
(Fecha de consulta 19 de febrero de 2023

IOT , INSURTECH6 Ways IoT will Change the Insurance Sector in 2023
<https://research.aimultiple.com/insurance-iot/>
(Fecha de consulta 22 de febrero de 2023)

Insurance Europe, Annual Report 2021-2022
<https://www.insuranceeurope.eu/publications/2620/annual-report-2021-2022/ >
(Fecha de consulta 25 de febrero de 2023)

Kaspersky. Ransomware WannaCry: todo lo que necesita saber
<https://latam.kaspersky.com/resource-center/threats/ransomware-wannacry>
(Fecha de consulta 25 de febrero de 2023)

Infosec. The Top Ten IoT Vulnerabilities
<https://resources.infosecinstitute.com/topic/the-top-ten-iot-vulnerabilities>
(Fecha de consulta 10 de marzo 2023)

Barbaraiot.com, AIoT: la unión perfecta entre la Inteligencia Artificial y el IoT - Barbara (barbaraiot.com)
<https://barbaraiot.com/es/blog/aiot-internet-de-las-cosas-inteligencia-artificial>
(Fecha de consulta 23 de abril 2023)

EY Consulting, How AI is transforming governance and risk management in insurance
<https://www.ey.com/en_dk/financial-services/how-ai-is-transforming-governance-and-risk-management-in-insurance>
(Fecha de consulta 23 de abril de 2023)

What is mTLS? | Mutual TLS | Cloudflare
<https://www.cloudflare.com/learning/access-management/what-is-mutual-tls/>
(Fecha de consulta 15 de mayo de 2023)

Shanghai Port Group Goes Smart | Huawei Enterprise
<https://e.huawei.com/eu/news/ebg/2021/intelligent-command-control-center>
(Fecha de consulta 21 de mayo de 2023)

The World's Largest Automated Container Port Operates Using First-of-Its-Kind 5.8 GHz LTE | Huawei Topic
<https://e.huawei.com/topic/leading-new-ict-ua/yangshan-port-case.html>
(Fecha de consulta 21 de mayo de 2023)

FAA Clears Certification Path For Pilotless Aircraft | FutureFlight
<https://www.futureflight.aero/news-article/2022-08-23/faa-accepts-reliable-robotics-certification-basis-pilotless-technology>
(Fecha de consulta 22 de mayo de 2023)

Is cyber insurance becoming an 'unviable product'? | Tech Monitor
<https://techmonitor.ai/technology/cybersecurity/cyber-insurance-unviable-product-lloyds-of-london-ferma>
(Fecha de consulta 1 de junio de 2023)

Lloyd's Market Bulletins
<https://www.lloyds.com/news-and-insights/market-communications>
(Fecha de consulta 10 de junio de 2023)

Russia, Ukraine, cyber insurance & the war exclusion | Lockton
<https://global.lockton.com/news-insights/russia-ukraine-cyber-insurance-and-the-war-exclusion>
(Fechade consulta 11 de junio de 2023)

Fuentes Oficiales:

ENISA (European Union Agency for Cybersecurity), Good Practices for Security of IoT, November 2020.

REAL DECRETO 303/2004 por el que se aprueba el Reglamento de los Comisionados para la Defensa del Cliente de Servicios Financieros (BOE de 3 de marzo de 2004).

Joaquín Chertó

Soy Ingeniero Técnico Industrial Mecánico, Ingeniero Industrial especializado en edificación y Comisario de Averías del Colegio de Oficiales de Marina Mercante.

Cuento con una experiencia de catorce años en el sector asegurador, toda mi trayectoria profesional se ha desarrollado en Prepersa AIE, filial de Grupo Catalana Occidente.

Las funciones que he desempañado durante mi trayectoria profesional han sido la gestión de redes de colaboradores externos, como peritos, talleres de reparación de automóviles y servicios técnicos de reparaciones.

Otras funciones que he desempañado han sido la peritación de siniestros relevantes, la reconstrucción de accidentes de circulación y elaboración de informes de evaluación de riesgo para la suscripción de riesgos industriales.