Facultad de Ciencias Económicas y Empresariales (ICADE),
Universidad Pontificia Comillas

EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL SISTMEMA FINANCIERO

Clave: 201504730

MADRID | Abril 2020

Autor: Carlos Aldea

Director: José Luis Arroyo Barrigüete

Título: El impacto de la inteligencia artificial en el sistema financiero

Titulación: Doble Grado en Administración y Dirección de Empresas y Derecho

Resumen: El siguiente trabajo realiza un estudio sobre la literatura del impacto de la inteligencia artificial en los mercados. Debido a la gran variedad de variantes de la inteligencia artificial, se ha hecho énfasis en el estudio sobre el trading algorítmico, el trading de alta velocidad, la ciberseguridad y los "robo advisors"

En primer lugar, se realiza un recorrido histórico del desarrollo de esta tecnología desde 1943, empezando con el "*paper*" "*A Logical Calculus of the Ideas Inmanent in Nervous Activity" de* Warren McCulloch y Walter Pitts, hasta la actualidad. En segundo lugar, se hace un análisis del trading algorítmico y el trading de alta velocidad donde se exponen los efectos de la implementación de esta tecnología en los mercados financieros y los tipos de estrategias más utilizadas. En tercer lugar, se estudia la ciberseguridad, cuáles son las mayores ciberamenazas actuales y como puede utilizarse la inteligencia artificial en este campo. Para finalizar el estudio, se analizan los tipos de "*robo avisors*", sus ventajas y desventajas con respecto a los asesores humanos y su proyección de futuro.

Palabras clave: Inteligencia artificial, "*high frequency trading*", "*trading*" algorítmico, cibercrimen, ciberseguridad y "*robo advisors*".

Abstract: The following work conducts a study of the literature on the impact of artificial intelligence on markets. Due to the great number of variants of artificial intelligence, emphasis has been placed on the study of algorithmic trading, high frequency trading, cybersecurity and robo advisors.

First, a historical overview of the developments of this technology, starting from 1943 with Warren McCulloch and Walter Pitts´ paper "A Logical Calculus of the Ideas Immanent in Nervous Activity", is done. Secondly, the effects of high frequency trading and algorithmic trading in financial markets and the different strategies used with these technologies is analysed. Next, a study of what are currently the biggest cybersecurity threats and how artificial intelligence can be used in this field is accomplished. To concluded, the study analyses what different kinds of robo advisors are there, their advantages and disadvantages compared to human advisors and their future.

Key words: Artificial intelligence, high frequency trading, algorithmic trading, cybercrime, cybersecurity and robo advisors.

INDICE

1. Introducción

1.1. Objetivos y motivación

La inteligencia artificial es una de las tecnologías más disruptivas que ha creado el ser humano. Tradicionalmente era la mano de obra manual la que era sustituida o complementada por máquinas, sin embargo, debido a los avances en este campo, se está empezando a sustituir también los trabajos que requieren cierto análisis intelectual. El tema en cuestión no es baladí. Todo cambio en la estructura productiva de una sociedad provoca que ciertos trabajos se queden obsoletos. Es verdad que estos cambios también traen consigo una creación de nuevos empleos, no obstante, no toda la población consigue adaptarse para suplir estas demandas laborales. Si bien la inteligencia artificial incrementará la productividad y abrirá un abanico de oportunidades jamás visto, sino se prepara a la sociedad para los cambios que se avecinan se creará una grave inestabilidad social que podrá tener efectos devastadores en el mundo tal y como lo conocemos. Keynes (1930: 2) ya advirtió de este problema en su paper "*Economic Possibilities for our Grandchildren*":

> "We are being afflicted with a new disease of which some readers may not yet have heard the name, but of which they will hear a great deal in the years to come—namely, technological unemployment. This means unemployment due to our discovery of means of economising the use of labour outrunning the pace at which we can find new uses for labour."

Se ha decidido realizar el análisis con un claro foco en el sector financiero por su tendencia a incorporar la tecnología más vanguardista con el fin de obtener ventajas competitivas claras sobre sus competidores. A pesar de los defensores de las teorías del mercado eficiente, la realidad nos ha mostrado una clara asimetría en la cantidad y calidad de la información que reciben los diversos agentes del mercado. Esta tecnología, tiene el potencial de reducir los costes de esta industria y nivelar el campo de juego para todos los participantes. Los desarrollos en esta materia han empezado a producir grandes cambios en ámbitos como el bancario, la gestión de activos o la detección del fraude, no obstante, la verdadera revolución está todavía por llegar. Ante este paradigma, la

importancia del tema se justifica por los cambios de gran calado que está produciendo y va a seguir provocando.

El objetivo principal de este TFG es, a través de la revisión de la literatura correspondiente, analizar como los distintos avances en inteligencia artificial han afectado a los mercados financieros. El objeto de estudio es hacer un recorrido histórico de la evolución de la inteligencia artificial, analizar el impacto que el "*high frequency trading*" y el trading algorítmico han tenido en los mercados financieros; estudiar cómo la inteligencia artificial está afectando a la lucha contra el fraude; y evaluar los efectos que los robo-advisors han tenido en los mercados.

1.2. Metodología utilizada

Para la consecución de los objetivos descritos en el apartado anterior, se ha realizado una revisión de la literatura sobre el tema. Se han analizado artículos científicos, informes de entidades especializadas, libros de expertos y artículos de periódico para conocer la situación actual.

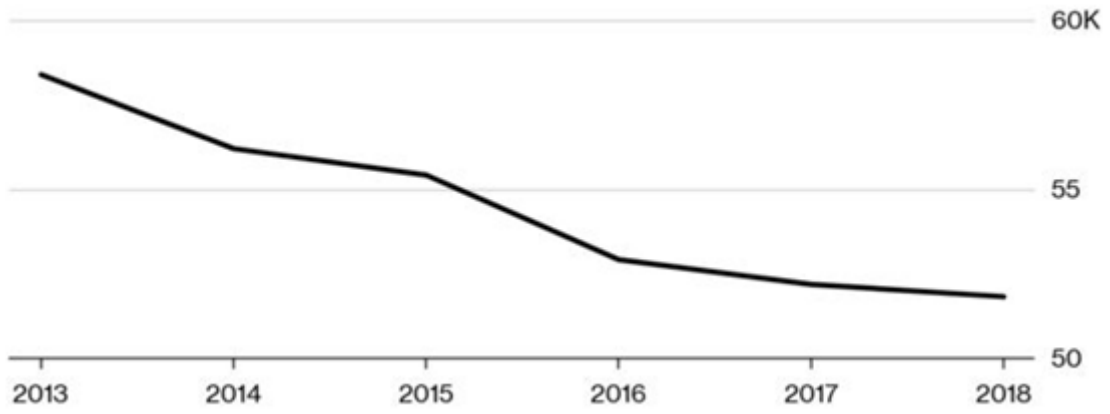
1.3 Estado de la cuestión

La inteligencia artificial es uno de los temas candentes hoy en día en nuestra sociedad. Ciertos políticos como el candidato demócrata Andrew Yang, ya están advirtiendo de las consecuencias de la incorporación de esta tecnología en nuestra estructura productiva y proponiendo medidas para suavizar la difícil transición que millones de estadounidenses tendrán que realizar para adaptarse a la nueva realidad del mercado laboral (principalmente su "*freedom dividend*", una renta básica universal de 1000 dólares para cualquier ciudadano estadounidense mayor de 18 años), (Gang, 2020).

La inteligencia artificial está lentamente penetrando en el sistema económico, sin embargo, podemos apreciar una adopción más que notable en la industria financiera. La gestión de activos y el análisis de valores se han automatizado, los "*brokers*" en los grandes bancos han sido prácticamente sustituidos por algoritmos, los banqueros de las sucursales están siendo rápidamente desplazados por la banca online y los "*chatbots*". Prueba de esta disrupción son los despidos masivos que se están acometiendo en el sector bancario. A modo de ejemplo son destacables los siguientes hechos: en 2018 Bankia

aprobó un ERE con los sindicatos de 2000 personas, (Skrycky, 2018). En 2019 el Banco Santander acordó con los sindicatos un despido colectivo de 3223 personas y la eliminación de 1128 sucursales, alrededor del 25% su red total en España (De Barrón, 2019); CaixaBank un ERE de 1890 personas (Ramón, 2019); Deutsche Bank un despido colectivo de 18 000 empleados globalmente en 3 años (Valero, 2019); y Commerbank 4300 empleados en 3 años (Reinicke, 2019), entre otros bancos. Si se observa el gráfico 1 de Bloomberg, se puede apreciar que la tendencia es generalizada y lleva años produciéndose

Gráfico 1: Evolución del número de empleos en los 12 bancos de inversión más grandes del mundo entre 2013 y 2018.



Fuente: Bloomberg, 2018 (Citado en Dickson, 2019)

El siguiente trabajo comenzará con un recorrido histórico de la evolución de la inteligencia artificial y se enfocará en como distintas aplicaciones de la inteligencia artificial, entre ellas el trading algorítmico, el "*high frequency trading*" o los "*robo-advisors*", está impactando los mercados financieros.

2. Recorrido histórico de la inteligencia artificial

2.1. ¿Qué es la inteligencia artificial?

No existe una respuesta fácil para responder que es la inteligencia artificial. Cada disciplina enfoca su definición desde una perspectiva particular, lo que evidentemente dificulta la posibilidad de obtener una definición unitaria.

Copping (2004: 4) la define de forma simplista como "métodos basados en comportamientos inteligentes de humanos y animales para la resolución de problemas complejos"

Russel y Norvig (2009) en su libro "*Artificial Intelligence: A Modern Approach*" recogen 8 definiciones distintas sobre inteligencia artificial agrupadas en 4 categorías.

> "Las definiciones en la parte superior hacen referencia al comportamiento. Las definiciones en la izquierda miden el grado de éxito en términos de fidelidad con el desempeño humano , mientras que las definiciones de la derecha lo miden contra el desempeño ideal, llamado "rationality". Un sistema es racional (*rational*) si hace lo correcto con la información que posee en ese momento." (p 1-2)

Tabla 1: Definiciones de inteligencia artificial

Pensar de forma humana	**Pensar de forma racional**
El esfuerzo de hacer a las máquinas pensar como si tuvieran mente en el sentido pleno y literal. La automatización de actividades que se asocian con el pensar humano como por ejemplo la toma de decisiones, el aprendizaje o la resolución de problemas.	El estudio de las facultades mentales a través de modelos computacionales. El estudio de las actividades computacionales que pueden hacer posible percibir, pensar y actuar.
Actuar de forma humana	**Actuar de forma racional**
El arte de crear máquinas que realizan funciones que requieren inteligencia cuando son realizadas por seres humanos. El estudio de cómo hacer que las máquinas han cosas que tradicionalmente han hecho los humanos mejor.	La inteligencia computacional es el estudio del diseño de agentes inteligentes La Inteligencia Artificial se preocupa del comportamiento inteligente en artefactos.

Fuente: Adaptado de Russel y Norvig (2009:2)

2.2. Historia de la inteligencia artificial

2.2.1. Los orígenes de la inteligencia artificial

Pospíchal y Kvasnička (2015) consideran como una de las semillas de la inteligencia artificial, por no decir la más importante, el trabajo de Warren McCulloch y Walter Pitts(1943). En su famoso paper "*A Logical Calculus of the Ideas Inmanent in Nervous Activity*", estos autores no solo definieron un modelo de neuronas artificiales en el cual su estado era definido en "on" o "off" dependiendo de la respuesta a un estímulo, sino que llegaron también a la conclusión de que toda función computable podía convertirse en una red de neuronas interconectadas y que todos los operadores lógicos se podían estructurar en redes.

Dos hitos relevantes que son considerados por muchos como el caldo de cultivo de la IA (Inteligencia Artificial) fueron, en primer lugar, la construcción del primer ordenador con una red neuronal artificial llamado SNARC (*Stochastic Neural Analog Reinforcement Calculator*) en 1951 por Marvin Minsky y Dean Edmonds (Hillis et al.2007); y en segundo lugar, "*Computing Machinery and Intelligence*", el famoso paper de Alan Turing (1950) donde se describe la prueba de Turing y consecuentemente se mencionan aspectos como el -"*machine learning*"-, los algoritmos genéticos o el aprendizaje por refuerzo.

La prueba de Turing o *"imitation game*", es un juego donde un humano, sin conocimiento de si el entrevistado es humano o un ordenador, plantea por escrito preguntas a un tercero, que responderá también por escrito, para que el entrevistador las utilice en su valoración de si está hablando con una máquina o con un humano. El objetivo en este experimento es que la máquina consiga engañar al humano. Si esto ocurriese, debido a los requisitos que este experimento impone a la máquina, se podría considerar que ésta es realmente inteligente. Para pasar la prueba se requiere ser capaz de comprender el lenguaje y expresarlo de forma coherente, almacenar la información que se recibe, utilizar la información para responder y poder formular conclusiones, aprender del comportamiento y del entorno, y poder manipular objetos para poder emitir una respuesta.

2.2.2 La génesis de la IA

Gracias en gran parte a la labor de captación de talento realizada por McCarthy y Minsky, Darthmouth College se convirtió en el lugar de nacimiento de la IA. En 1956 McCarthy consiguió reunir en un "*think tank*" en Darthmouth a diez intelectuales punteros en el área para realizar un estudio de dos meses sobre la inteligencia artificial. Los temas que se trataron fueron: la automatización de los ordenadores, como programar un ordenador para que pueda utilizar el lenguaje, las redes neuronales, la teoría del tamaño del cálculo, el *"machine learning*", la aleatoriedad y creatividad en las máquinas y como conseguir que las maquinas consigan realizar abstracciones. Dentro de ese "*think tank*" se encontraban individuos como Trenchard More de Priceton, Arthur Samuel de IBM, Oliver Selfridge del MIT, o Allen Newell y Herbert Simon, de Carnegie Tech (McCarthy, Minsky, Rochester y Shanon, 2006).

Del encuentro destaca sobre todo la aportación de Newell y Simon en lo que se considera hoy en día por muchos el primer programa de IA creado, el "*Logic Theorist*". Este programa era capaz no solo de pensar lógicamente sino también de interpretar y manipular símbolos. Asimismo, este programa fue capaz de demostrar muchos de los teoremas planteados por Alfred North Whitehead y Bertrand Russel en el capítulo 2 de "*Principia Matemática*" (Longuet-Higgins, 1991).

Este encuentro marcó un antes y un después en el campo de la IA. Los presentes y sus discípulos se encargarían de desarrollar esta materia, permaneciendo a la vanguardia durante muchos años.

2.2.3 Inicios del desarrollo de la Inteligencia Artificial

A pesar de todo el escepticismo inicial y las limitaciones de recursos y capacidades computacionales, los graduales avances convirtieron a los incrédulos en creyentes. El primer gran éxito tuvo lugar en 1959 con el desarrollo del "*General Problem Solver*" por Newell y Simon.

"El GPS es un programa que incorpora medios heurísticos para soluciona una variedad sustancial de problemas, incluyendo, por ejemplo, el descubrimiento de pruebas para teoremas lógicos, demostraciones de identidades trigonométricas y algebraicas, y realización de integraciones formales y diferenciaciones." (Newell y Shaw, 1959: 1)

Otros grandes hitos de esta primera etapa fueron la creación del "*Geometry Theorem Prover*" por Herbert Gelernter en 1959, (Cordeschi, 2002: 191) capaz de deducir teoremas de geometría euclidiana; la producción del lenguaje Lisp por McCarthy en 1958 (McCarthy, 1978); el desarrollo de CTSS (*Compatible Time Sharing System*) por el MIT en 1961 uno de los primeros sistemas operativos de uso compartido (Nilsson, 2009); la fundación del laboratorio de inteligencia artificial en Stanford en 1963 liderado por McCarthy tras discutir en el MIT con Minsky sobre la línea de investigación principal a seguir (Mc Carthy quería centrarse en el estudio de la relación entre el lenguaje y la inteligencia, mientras que Minsky quería centrare en el estudio del aprendizaje automatizado de representaciones sensomotoras y la resolución de problemas a través de modelos del medio ambiente) (Boden, 2006); y el descubrimiento por J. A. Robinson en 1965 de su método de resolución (Murawski, 2006), una regla de inferencia llamada

resolución utilizada, entre otras cosas, para demostrar que ciertos teoremas se pueden demostrar de manera automática (Metlich, 2012).

2.2.4 La inteligencia artificial desde 1966 hasta hoy

Como todo en la vida, a medida que se fue avanzando en este terreno se fueron encontrando obstáculos.

El primero de estos obstáculos fue el hecho de que estos programas no tenían conocimiento de la materia que trataban, sino que llegaban a sus conclusiones por manipulaciones sintácticas Esto se pudo apreciar notoriamente en 1957 cuando la US National Research Council financió programas para la traducción de artículos científicos rusos. Los programas que se crearon con esta finalidad tenían el problema de que la mera traducción palabra por palabra no era suficiente para entender todo el contenido de las oraciones, sino que se requería un conocimiento previo y técnico para poder resolver todas las ambigüedades y poder determinar concretamente el contenido de las oraciones fielmente. Tras 8 años de trabajo el proyecto MT de Georgetown University, en 1962, intentó producir finalmente traducciones automáticas de distintos artículos científicos, no obstante, en todas ellas se tuvo que editar la traducción para poder comprenderla y el coste fue superior a aquel en el que se hubiera incurrido de haberse hecho por un experto de forma manual (National Research Council, 2006).

El segundo gran escollo que se encontró en el camino fue la dificultad de los problemas que se intentaron resolver con esta tecnología. En un principio se pensaba que la resolución de problemas más complejos sería solo una cuestión de conseguir hardware más rápido y memorias más grandes. Sin embargo, pronto se llegó a la difícil conclusión de que a pesar de que un programa pueda resolver teóricamente un problema no implica necesariamente que tenga los mecanismos necesarios para resolverlo en la práctica.

Fruto de estas limitaciones, gran parte de los equipos de investigación pivotaron desde los métodos utilizados anteriormente, denominados "*weak methods*", a sistemas que empleaban gran cantidad de conocimientos de un área concreta con el fin de conseguir más pasos en el razonamiento automático y mejores resultados. Como resultado de este cambio surgieron los denominados sistemas expertos. Entre los casos más sonados nos podemos encontrar el "DENDRAL program", considerado el primer programa experto por automatizar la toma de decisiones para resolver problemas de inferencia de

estructuras moleculares a través de la información dada por un espectrómetro (Buchanan y Feigenbaum, 1993).

Los resultados de este programa animaron a Edward Feigenbaum junto a otros de sus compañeros a crear el *Heuristic Programming Proyect* en Stanford, un programa diseñado para ver en qué áreas se podían aplicar estos nuevos métodos. (Buchanan y Feigenbaum, 1980).

Como resultado de esta nueva visión en los setenta, cabe destacar MYCIN, un sistema de IA encargado de diagnosticar determinadas infecciones y recomendar las medicinas correspondientes en las dosis correctas o INTERNIST, un programa desarrollado por Pope and Myers encargado de diagnósticos diferenciales en el campo de la medicina interna (Feigenbaum, 1981).

Este creciente interés y desarrollo en el campo de la inteligencia artificial, en opinión de Nilsson (2009), tuvo dos razones fundamentales. La primera razón fue que el desarrollo en la materia y los distintos avances que se habían realizado, ahora si permitían que se encontrasen utilidades realistas con opción a ser comercializadas. La segunda razón, y la más importante bajo su punto de vista, fue la creciente financiación a proyectos de esta rama por parte del Ministerio de Defensa Americano principalmente a través de DARPA (*Defense Advanced Research Proyects Agency*) al haberse eliminado las restricciones del "*Mansfield Amendment"*, el cual limitaba al departamento de defensa de los Estados Unidos a solo poder financiar proyectos con clara finalidad militar.

A partir de 1980 se empezaron a utilizar los primeros sistemas expertos en el mercado. A título de ejemplo, Dupont en 1988 tenía más de 100 en uso y 500 en desarrollo. Con el tiempo, casi todas las grandes corporaciones americanas o tenían estos sistemas ya en uso, o estaban en desarrollo. Esta industria aumento su facturación de unos pocos millones en 1980 a billones de dólares a mediados de los años 80. A pesar de los avances, muchas empresas especializadas en estos sistemas no fueron capaces de cumplir con las expectativas que habían creado. Esto provocó un periodo que se conoce como "*AI Winter*", caracterizado por burbujas financieras, obsolescencia tecnológica como la del lenguaje LISP, quiebras y promesas incumplidas. (Russel y Norvig, 2009).

Aun con un pequeño periodo de crisis entremedias, el avance de la IA fue imparable. A mediados de 1980 hubo grandes desarrollos en algoritmos evolutivos y "*data mining*". Asimismo, cabe destacar el cambio de perspectiva que se ha efectuado en los últimos años. En vez de poner el foco en los algoritmos, se ha pasado a ponerlo en los datos. Este cambio de perspectiva fue provocado en gran medida por "*papers*" como los de Banko y Bill (2001) donde se mostraban que el desempeño de los algoritmos se podía incrementar simplemente incrementando el número de datos que disponen para entrenarse.

El avance de la Inteligencia Artificial ha sido incesante. En 1997 el programa Deep Blue consiguió vencer al campeón mundial de ajedrez Garry Kasparov (García, 1997); en 2002 se empezó a comercializar el famoso Roomba, un robot que limpia los suelos de forma autónoma (Sánchez, 2017); en 2004 Boston Dynamics desarrollo su "*Big Dog*", un robot con la misión de transportar equipamiento militar de forma autónoma (Boston Dynamics, s.f.) y en 2011 se comercializó el primer teléfono móvil con asistente virtual (Bosker, 2013).

Por último, cabe destacar dos de los últimos avances que probablemente sean los que mayor impacto vayan a tener en el futuro. Estas innovaciones son: el desarrollo de las Redes Generativas Antagónicas (Bengio et al, 2014) y los avances realizados en la conducción autónoma.

Las Redes Generativas Antagónicos son algoritmos cuyo fundamento consiste en crear dos modelos distintos, uno diseñado para generar una serie de datos basados en una muestra dada y otro diseñado para adivinar si los datos que analiza vienen del otro algoritmo o de la muestra. El modelo que se ocupa de la generación de datos será entrenado y tendrá la misión de maximizar el error del otro modelo (Bengio et al, 2014). Esta tecnología es muy prometedora y es la culpable del surgimiento reciente de los "*deep fakes*" (o videos falsos). Recientemente, está tecnología ha sido utilizada tanto por la NASA como por Airbus para el diseño y manufactura de piezas. Pero sus usos no se agotan ahí, también ha sido utilizada en la composición musical y en el diseño de prótesis dentales (Hidalgo, 2020).

Por otro lado, los avances en la conducción autónoma han permitido a empresas como Tesla llegar al nivel 3 de conducción autónoma (Jones, 2019). El nivel de autonomía en la conducción se divide en 6 niveles distintos que van del 0 (cuando no hay ninguna ayuda

automática en la conducción) al 5 (cuando el vehículo es plenamente autónomo y no necesita de intervención humana) El nivel 3 de autonomía indica que el coche puede circular de manera casi autónoma, pudiendo analizar sus alrededores y detectar obstáculos, aunque necesita de la supervisión de un conductor y de su intervención ocasional (Toyota, s.f.). De todos los avances en inteligencia artificial, la conducción autónoma es probablemente el campo de desarrollo que más impacto pueda tener en la economía global. Si finalmente se llega a desarrollar un modelo de nivel 5, millones de trabajos poco cualificados serán destruidos, haciendo además que la colocación de esa mano de obra en otros sectores productivos sea muy complicada.

3. "*High frequency trading*" y "*trading*" algorítmico

3.1. Introducción y definiciones

Una de las mayores revoluciones en los mercados de valores ha sido sin duda su digitalización. Esta circunstancia ha permitido que proliferen nuevas estrategias de inversión difícilmente imaginables en épocas anteriores. Un instrumento que ha permitido esta gran revolución indudablemente ha sido el uso de algoritmos tanto en las estrategias de inversión, como en la compraventa de productos financieros.

Hendershott y Riordan (2009: 2) definen el trading algorítmico como "el uso de algoritmos computacionales para tomar decisiones de compraventa, emitir ordenes al mercado y gestionarlas después de su emisión, de forma totalmente automatizada."

El "*high frequency trading*" o trading de alta velocidad (HFT) es considerado como una subcategoría más específica del trading algorítmico (AT). A pesar de todas las distintas variantes que este sistema tiene, Brogaard, Hendershott, y Riordan (2014) lo definen de modo genérico como una estrategia de inversión donde instrumentos financieros son comprados, mantenidos durante segundos o incluso milisegundos, y vendidos inmediatamente después, normalmente con el fin de obtener un beneficio.

La U.S Securities and Exchange Comision (2014: 4) estableció que la mayoría de los "*high frequency traders*" poseen las siguientes características:

> "1. Utilizan una velocidad extraordinaria y programas extremadamente sofisticados para generar, dirigir y ejecutar órdenes.
>
> 2. Emplean los servicios de –"housing" o "co-location services"- y de datos de las bolsas y de otros agentes involucrados para minimizar las latencias.
>
> 3. Utilizan intervalos de tiempo muy cortos para establecer y liquidar posiciones
>
> 4. envían gran cantidad de ordenes al mercado que pueden ser canceladas inmediatamente después.
>
> 5. Terminan los días de operaciones lo más cerca posible a una posición neutral en el mercado (lo que quiere decir que evitan al máximo tener una alta exposición a los riesgos financieros que una posición sin cubrir pueda entrañar). "

Dejando claro, además, que debido a las distintas estrategias que estos operadores pueden adoptar, no todos compartan esta serie de peculiaridades.

Ahlstedt y Villyson (2012) establecen que la diferencia principal entre el trading algorítmico y el trading de alta velocidad se encuentra en el tiempo que se requiere para desarrollar la estrategia diseña, siendo este intervalo en el caso del trading de alta velocidad medido muchas veces en milisegundos. Estos autores mencionan también que el volumen de ordenes también podría ser considerado una de las diferencias entre estas dos tecnologías, siendo mucho más elevado en el caso del trading de alta velocidad con carácter general; no obstante, reiteran que el filtro de diferenciación principal debe ser el intervalo de tiempo de ejecución de la estratega.

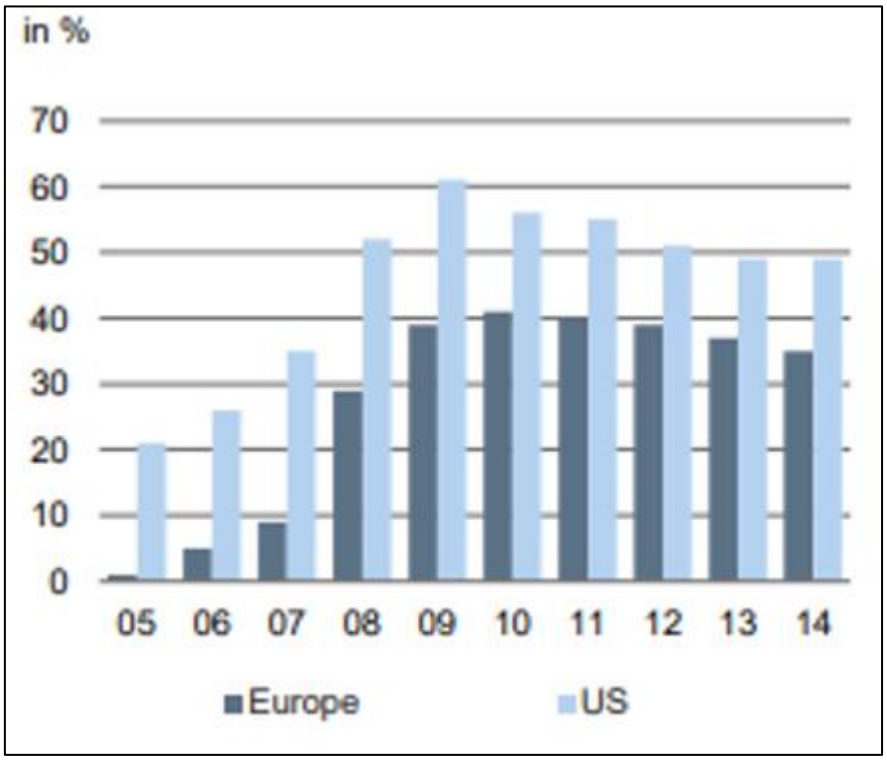
3.2. Análisis de la actualidad

El HFT es un fenómeno relativamente nuevo. Prueba de esto es que uno de los pioneros en este campo, Tradebot Systems, fue fundado en 1999 (Tradebot Systems, s.f). Brogaard et al (2014) consideran que dos han sido los acontecimientos que han precipitado la expansión de este tipo de sistemas: la decimalización de las cotizaciones (anteriormente las acciones se negociaban en octavos) y la evolución de la tecnología, lo que ha permitido que se pueda analizar información y transportarla de manera mucho más rápida.

En 2009 Tabb Group, una consultura internacional especializada en mercados de capitales estimó que el 73% del volumen diario de compraventa de acciones en las bolsas americanas era atribuible al HFT, un incremento del 43% con respecto a 2005 (Mackenzie, 2009).

A pesar de esta revolución, recientemente se ha podido apreciar un declive global en la participación global de estas estrategias. Después de la crisis del 2008 la participación del HFT en el trading global ha decaído de forma constante.

Tabla 2: Porcentaje del "*high frequency trading*" en el "*trading*" global



Fuente TABB Group, 2014 (Citado en Kaya, 2016)

Kaya (2016), analista del Deutsche Bank, explica esta tendencia a través de dos fenómenos: el incremento de la competencia en este sector, lo que ha provocado una reducción de los márgenes; y el desarrollo de los "*dark pools*".

Los "*dark pools*", son redes que permiten a sus participantes comprar y vender grandes cantidades de activos financieros sin que el resto de participantes sepan quien es el comprador o vendedor o el precio al que se ofrecen o demandan estos activos. Solamente se conoce el precio de adquisición una vez se ha producido la transacción. A pesar de que los "*dark pools"* hayan sido criticados por su falta de transparencia (dado que el acceso a estos mercados está restringido), y por posiblemente desvirtuar los precios de los mercados, históricamente han tenido la finalidad de ser el lugar donde se efectuaban muchos "*block trades*" (órdenes muy grandes de compraventa activos financieros (Chen 2019)) para reducir la volatilidad de los mercados públicos (Grant, Grene, y Preece, s.f.).

Debido al incremento de la participación del HFT, cada vez más inversores institucionales han decidido acudir a estos mercados para conseguir un precio más beneficioso para ellos (Kaya 2016).

El CFA Institute (s.f) estima que en la primavera 2017 el 40% de todas las transacciones de activos financieros tuvo lugar fuera de las bolsas reguladas, siendo el 15% atribuible a los "*dark pools*".

A pesar de la notable influencia de los "*dark pools"* en los resultados de este sector, no se puede obviar el impacto de la competencia. Atraídos por las altas rentabilidades iniciales, muchos agentes económicos decidieron emprender en este sector. Esto avivó la competencia e hizo que las estrategias que antes se empleaban fueran inservibles o las firmas tuvieran que invertir ingentes cantidades de dinero para poder competir en velocidad con sus competidores. Actualmente el mercado está saturado, lo que provoca que solo los agentes que operan con grandes volúmenes puedan sobrevivir con tan poco margen (Bullock, Rennison y Mayer, 2018).

3.3. Estrategias más utilizadas

El trading algorítmico y el HFT admiten muy diversas estrategias y uso. A modo ejemplificativo se comentarán las más utilizadas

3.3.1. Estrategias pasivas de creación de mercado

El Congresional Research service (2016) definen las estrategias de creación de mercado como "aquellas que proporcionan liquidez casando ordenes de compraventa, ya sea comprando en los mercados o utilizando su propio inventario de acciones cuando un "*market maker"* no puede inmediatamente ejecutar la operación."

A pesar de esta definición, lo dicho no implica que los "*high frequency traders*" no puedan operar como "*market makers*", o que los "*market makers"* no puedan emplear esta tecnología para proporcionar sus servicios.

En este tipo de estrategias el beneficio se obtiene con el diferencial de precios. Este diferencial puede ser muy pequeño, pero al realizar muchas operaciones el beneficio total puede ser considerable.

3.3.2. "*Volume Weighted Average Price*"

El "*Volume Weighted Average Price"*o VWAP es una estrategia consistente en dividir una orden en ordenes más pequeñas, basado en un modelo histórico del volumen de actividad del instrumento financiero, y distribuirlas a lo largo del tiempo con el objetivo de acercarse lo máximo posible al "*Volume Weighted Average Price*" (que no es más que el sumatorio de la cantidad de activos comprados por su precio, dividido por el total de acciones compradas (Mandes, 2016).

Una variante de esta estrategia es el "*Time Weighted Average Price*", similar al VWAP, pero cuya diferencia fundamental es que no atiende al volumen de activos financieros intercambiados sino al precio medio de la acción en un intervalo de tiempo determinado (Cesari, Marzo y Zagaglia, 2012).

3.3.3. Arbitrajes financieros

Bestinver define de forma simple pero elegante los arbitrajes financieros como una "estrategia financiera que consiste en aprovechar la diferencia de precio entre diferentes mercados sobre un mismo activo financiero para obtener un beneficio económico" (Bestinver, s.f.).

Los arbitrajes más comunes se pueden encontrar con Forex, futuros, opciones o rebalanceos de fondos indexados, aunque los que más polémica suscitan son sin duda los arbitrajes de latencia.

Los arbitrajes de latencia son considerados por muchos como una práctica predatoria que debería ser eliminada. Este tipo de estrategias utilizan tecnología de última generación, estar lo más cerca posible de los servidores de la bolsa donde operan y la compra de información bruta de los mercados para crear su propia bolsa, la cual, debido a la diferencia de tiempo existente entre la información que compran, y la velocidad a la que se procesa una orden de mercado ordinaria, permite a los operadores de este tipo de estrategias adelantarse a la operación ordenada por otro agente de mercado (Arnuk y Saluzzi, 2009).

Arnuk y Saluzzi (2009:2), en su artículo "*Latency Aritrage: The Real ower Behind Predatory High Frequency Trading*" ponen un ejemplo muy ilustrativo de arbitraje aprovechándose de un inversor institucional que emplea un algoritmo VWAP:

"1. El mercado para ABC pide un precio de 25,53$ y se ofrece 25,54.

2. Debido al arbitraje de latencia, el ordenador que utiliza la estrategia sabe que hay una orden que moverá dentro de un instante la horquilla de precios a 25,54$ "bid" y 25,66$ "*ask*"

3. El "*High Frequency trader*" investiga en todos los mercados que pueda y compra todas las acciones que haya de ABC a 25,54 y más baratas.

4. El inversor institucional no consigue cerrar la operación u

y la horquilla de precios se mueve a 25, 54$ "bid" y 25,56$ "ask"

5. Mediatamente después, el "*High Frequency Trader*" ofrece el valor ABC a 25,5$ o 25,56$

6. Como el inversor institucional emplea un algoritmo VWAP, éste fuerza al inversor a comprar las acciones disponibles a 25,55$ o 25,56$

7. El "*High Frequecy Trader*" gana 0,01$-0,02$ por acción a costa del otro inversor"

3.3.4. Estrategias de momento

Introducidas por Jeegadeesh y Titman (1993) la estrategia consiste en comprar aquello que haya tenido un buen desempeño reciente y vender aquello que haya tenido un desempeño negativo. Estos autores medían el desempeño en un intervalo de 6 meses y clasificaban las acciones en función del desempeño para determinar posteriormente que acciones iban a ser compradas y cuales iban a ser vendidas.

Grandes inversores como George Soros aplican variantes de esta estrategia para especular. El famoso concepto de reflexividad de Soros claramente se fundamenta en este tipo de estrategias. Soros se dio cuenta que, en determinadas ocasiones, los prejuicios de los inversores podían afectar al precio de determinados activos financieros. Asimismo, estos cambios en los precios podían reforzar los prejuicios preexistentes de los inversores y acentuar aún más la tendencia en un proceso claramente reflexivo (Soros, 1994: 46-55).

3.4. Impacto en los mercados financieros

Es innegable que esta tecnología ha transformado de manera considerable la industria financiera. Solo hace falta echar un vistazo a los parqués de las bolsas para darse cuenta de que algo ha cambiado. El "*high frequency trading*" y el trading algorítmico ha desplazado poco a poco a los brókeres y "*traders*" tradicionales, pero su impacto no se queda ahí. Esta tecnología ha afectado a la liquidez de los mercados, los costes de transacción, la calidad y volatilidad del mercado y a la determinación del precio objetivo de los activos financieros.

3.4.1. Liquidez

El impacto en la liquidez de los mercados financieros depende en gran medida en la estrategia que ejecuten los algoritmos. Existen estrategias que proporcionan liquidez al mercado, sobre todo cuando los agentes actúan como creadores de mercado, pero también es verdad que hay estrategias de signo inverso que la drenan. Hendershott, Jones y Menkveld, (2011) estudiaron si efectivamente los "*high frequency traders*" proporcionaban liquidez en la bolsa de Nueva York. Tras su estudio llegaron a la conclusión de que sí la proporcionaban en tiempos de bonanza económica, no obstante, mantenían un sano escepticismo a la hora de afirmar que en tiempos de crisis la proporcionarían también, dado que nada impediría a estos "*brokers"* apagar sus máquinas para no sufrir pérdidas en tiempos turbulentos.

3.4.2. Costes

La digitalización de las bolsas ha permitido que muchas transacciones se hagan de manera virtual. Este factor ha permitido el surgimiento de economías de escala derivadas de la implementación de ordenadores. Esta digitalización ha permitido una considerable reducción de costes. Claro ejemplo de esta tendencia es Robin Hood. Robin Hood es un bróker estadounidense que no cobra comisiones por transacciones (Robin Hood, 2020), algo impensable hace unos años.

Domowitz y Yegerman (2005) tras un estudio exhaustivo, llegaron a la conclusión de que, a pesar de que en ordenes grandes las diferencias no eran tan significativas, por lo general el empleo de algoritmos reducían los costes de compraventa de instrumentos financieros.

Además, el empleo de estas tecnologías ha permitido reducir incluso aún más los costes de transacción debido a la eliminación de muchos sesgos cognitivos humanos como el de anclaje, sesgo cognitivo donde se suele tener demasiado en consideración la información que se ha recibido primero; el de confirmación, consistente en buscar y valorar en mayor medida aquella información que esté de acuerdo con nuestras juicios iniciales; o el de último evento, que hace que le asignemos más valor a los acontecimientos más recientes. (Rubio, 2014)

3.4.3. Calidad del mercado

Otro de los mayores impactos de estas tecnologías es su efecto en la calidad del mercado. Existen autores que analizan desde un punto de vista teórico este fenómeno y concluyen que estos avances provocan deterioros en el mercado. Los exponentes más importantes de esta opinión Bias y Foucault (2014). Estos autores ven un posible problema de endogeneidad entre las distintas estrategias algorítmicas de los distintos agentes de mercado

> "Asimismo, las variables dependientes de la calidad del mercado y el trading de alta frecuencia son endógenos. Ambos reflejan una optimización del comportamiento o de los participantes del mercado, sus reacciones a las condiciones del mercado, y sus respuestas a las reacciones de otros. Por ejemplo, mientras el HFT afecta a la volatilidad del activo con el que opera, este está también afectado por esta volatilidad". (Bias y Foucault, 2014: 12)

Este riesgo de endogeneidad se puede apreciar claramente en lo que se denominan "*flash-crashes*". El más importante de todos estos es el que se produjo en el 6 de mayo de 2010. El "*crash*" de 6 de mayo fue el declive en solo día más importante de la historia del Dow Jones Industrial Average (998,5 puntos) (De Prado, Easley y O'hara, 2011).

Este incidente fue desencadenado principalmente por una sola transacción, la venta en menos de 20 minutos de 4.1Billones de dólares en contratos de futuros E-Mini S&P por un inversor institucional. (CFTC y SEC, 2010). En vez de ejecutar la operación manualmente este inversor utilizó un algoritmo, lo cual finalmente provocó la reacción en cadena debido a la alta endogeneidad y correlación existente en el mercado.

3.4.4. Volatilidad

Debido a la alta heterogeneidad de estrategias y mercados, y a la dificultad intrínseca del estudio de este tema, no se puede afirmar de manera categórica que el trading algorítmico o el "*high frequency trading*" reduzcan o aumenten la volatilidad. Distintos autores han llegado a posiciones distintas. Chaboud et. al (2009) realizaron un estudio analizando entre otras cosas, el impacto de los AT y HFT en la volatilidad de tres mercados distintos y llegaron a la conclusión de que, en media, estas tecnologías reducían la volatilidad del mercado. Sin embargo, no descartaban la posibilidad de que pudieran incrementarla considerablemente durante determinados periodos de tiempo. A conclusiones similares llegaron Hasbrouck y Saar (2013), que, con el "*flash crash*" de 2010 en mente, tampoco descartaron la posibilidad de que el HFT pudiera en ocasiones provocar fallos en el mercado.

"While our results suggest that market quality has improved, we believe it is as yet an unresolved question whether low-latency trading increases the episodic fragility of markets, and we hope that future research will shed light on this issue" (Hasbrouck y Saar ,2013: p 677).

Contrariamente, Boehmer, Fong y Wu (2012) a través de una muestra internacional de acciones llegaron a la conclusión de que el empleo de algoritmos incrementaba la volatilidad en los mercados, volatilidad que, por cierto, no es atribuible al ajuste eficiente de precios debido a la emisión de nueva información relevante para el mercado. Asimismo, también llegaron a la conclusión de que sus efectos no son constantes a lo largo del tiempo y que las acciones más afectadas por esta volatilidad parecen ser la de las empresas pequeñas o aquellas con precios bajos.

3.4.5. Determinación del precio objetivo

Brogaard et al (2014) analizaron los "high frequency traders" y llegaron a la conclusión de que favorecen la determinación de un precio objetivo. Muchos de ellos operan incorporando la información más reciente sobre el precio del activo financiero en sus transacciones, comprando cuando estos están infravalorados y vendiendo cuando estos están sobrevalorados. La alta velocidad a la que se llevan estos ajustes y la incorporación de toda la información pública al precio del activo financiero permite que los mercados se acerquen más al concepto de mercado eficiente semi-fuerte de Fama (1970). Una

eficiencia semi-fuerte se consigue cuando el precio de los activos financieros descuenta toda la información pública disponible. Fama (1970) también hace referencia a otros dos tipos de eficiencias, la débil y la fuerte. La eficiencia débil se consigue cuando el precio de los activos financieros toma en cuenta toda la información de los precios pasados y la eficiencia fuerte cuando el precio de los activos reflejase toda la información disponible, incluyendo la privilegiada o privada.

4. La lucha contra el cibercrimen

4.1. Introducción

Debido a la creciente digitalización de las relaciones, la gran cantidad de datos que se generan, la alta movilidad internacional de las relaciones empresariales y la falta de comunicación efectiva entre administraciones de distintos países e incluso del mismo país; el número de cibercrímenes ha aumentado considerablemente. En 2018, sólo en España, la policía registro un total de 110 613 posibles ciberdelitos, un 36% más con respecto al año anterior (Gabinete de Coordinación y Estudios, 2018). El principal problema de este tipo de delitos es su porcentaje de impunidad. De todos los ciberdelitos investigados, en 2017 solo el 27,2% fueron esclarecidos (Instituto Nacional de Estadística, s.f. citado en Baños, 2019). Cybersecurity Ventures (s.f., citado en Morgan, 2019) estima que en 2021 los daños por el cibercrimen serán de alrededor de 6 trillones de dólares anuales.

Tanto las empresas como el sector público son conscientes de esta coyuntura y han decido adaptarse a estos nuevos tiempos. A título de ejemplo, entre las mediadas comunitarias destaca la creación de ENISA, y el programa Horizon 2020 "*Secure societies*".

La ENISA (la Agencia de la Unión Europea para la Ciberseguridad) es una organización vinculada con la Unión Europea encargada de ofrecer soluciones, asesoramiento y ayuda en materia de ciberseguridad a los estados miembros, con el fin de que estos puedan equiparse y estar preparados para evitar, descubrir y responder a los problemas de ciberseguridad que puedan ocurrir.("About ENISA", s.f.).

El programa Horizon es el programa de investigación y desarrollo más grande de la Unión Europea, con alrededor de 80 billones de inversión ("What is Horizon 2020", s.f.). Dentro del programa Horizon 2020, uno de los proyectos más importantes es el proyecto "*Secure societies*". Dentro de los objetivos de este proyecto están incluidos, la protección de infraestructuras críticas con la última tecnología disponible y proporcionar ciberseguridad a los miembros y ciudadanos de la Unión Europea ("Secure societies", s.f.).

Esta preocupación no es exclusiva del sector. La grave situación actual ha provocado que el resto de agentes económicos busquen remedios para paliar esta situación. Según un estudio de Capgemini (2019), 1 de cada 5 de los ejecutivos entrevistados declaró que su

organización había sufrido un ataque cibernético que había resultado en un acceso no autorizado a su red, máquinas, aplicaciones o datos en 2018. Además, el 20% registró pérdidas de más de 50 millones por este motivo. Asimismo, un estudio de 2011 de la división de ciberseguridad de la empresa Norton descubrió que, en 2011, había en Estados Unidos 74 millones de personas afectadas por este tipo de crímenes, estimando además las pérdidas en alrededor de 32 billones de dólares (citado en Panda, Rao y Saini, 2012). El tema no es baladí. Los negocios se encuentran asediados por ataques informáticos y tienen la necesidad de mejorar sus defensas para poder responder a la ingente cantidad de ataques que sufren.

En este entorno se encuentra el sector bancario. Parte del modelo de negocio de la banca consiste en conseguir que sus clientes confíen en ellos. La confianza como elemento vertebrador de la relación cliente-banco sobre todo destaca en la banca corporativa y comercial. Sin esta confianza, nadie realizaría depósitos en los bancos, o lo que es peor, intentaría retirar su dinero. Todos recordamos la escena del banco de Merry Poppins, que, aunque se trate de una película, no dista mucho de la realidad en nuestro sistema de reserva fraccionaria. Un sistema de reserva fraccionaria implica que los bancos solo están obligados a mantener como reserva un porcentaje de los depósitos de sus clientes, pudiendo disponer del resto, normalmente a través de la concesión de préstamos (Husillo Vidic, s.f.). El problema es evidente, si todo el mundo pierde la confianza en el banco y reclama su dinero depositado, es muy probable que vuelvan con las manos vacías.

El sector bancario, sobre todo la banca comercial y corporativa, ha experimentado cambios muy drásticos. Debido al desarrollo del comercio electrónico y las facilidades ofrecidas por la tecnología, cada vez es más frecuente que se realicen las gestiones bancarias de forma online (Prodanova, San Martín & Torres, 2015). Como reacción a este cambio tendencial, podemos apreciar la creación reciente de bancos online, como N26 o Revolut, o el desarrollo de las aplicaciones móviles de bancos tradicionales como el BBVA, el Santander o CaixaBank.

A pesar de este cambio de contexto, la confianza sigue siendo igual de importante. Ahora los clientes no solo deben preocuparse de que el banco pueda devolverles su dinero, sino que también tienen que preocuparse de que toda la infraestructura online que es ofrecida es segura. Esta preocupación también es predicable con respecto a otras empresas del

sector financiero, como los "*brokers*" o los proveedores de productos financieros. Debido a las cantidades de dinero que manejan, las empresas de este sector son jugosos objetivos para los ciberdelincuentes. De hecho, existen grupos de cibercriminales especializados en el sector financiero (normalmente en el sector bancario). Algunos de estos grupos son incluso financiados por los gobiernos, como el caso del Bueau 121 de Corea del Norte. El Bureau 121 es una división de elite del gobierno norcoreano encargada de coordinar y ejecutar ciber ataques a lo largo de todo el mundo (Lee: 2015). Los éxitos de esta organización han permitido a Corea del Norte avanzar en el desarrollo de su programa nuclear a pesar de todas las sanciones internacionales que se le habían impuesto. Dentro de sus éxitos destaca sobre todo su ataque al Banco Central de Bangladesh en febrero de 2016 (Buchanan, 2020).

Cada año los ataques al sector financiero aumenta en cantidad y en complejidad. Las empresas de este sector no suelen ser totalmente transparente en cuanto al número de ataques y su impacto global, no obstante, los aumentos de inversión en ciberseguridad permiten afirmar que el problema no es intrascendente. El BBVA ya ha declarado que los ataques han aumentado otra vez en el último año e incluso han añadido un apartado sobre ciberseguridad en sus cuentas anuales (citado en Abril, 2020).

Las entidades financieras están preparándose para este nuevo futuro y siendo una de las piezas del armamento de defensa más preciada las distintas técnicas de inteligencia artificial, piedra angular en la detección, predicción y respuesta de las defensas de última generación.

4.2. Conceptos.

Gordon y Ford (2012: 14) definen el cibercrimen como: "cualquier tipo de crimen que es facilitado o cometido usando un ordenador, una red o un dispositivo de hardware." Asimismo, dividen los tipos de cibercrímenes en dos categorías: el tipo 1 y 2.

El cibercrimen de tipo 1 se caracteriza por generalmente ser un evento único desde el punto de vista de la víctima (por ejemplo, leer un email), y cometerse con ayuda de la introducción de un fragmento de software maligno como un virus, "*rootkits", o keyloggers*- aprovechándose habitualmente de puntos débiles en los sistemas

informáticos. Dentro de esta categoría se encuentran crímenes como el phishing, el robo o manipulación de datos, el robo de identidad, o el fraude bancario o en el "*e-commerce".*

La segunda categoría incluye delitos como el ciberacoso o la extorsión y se caracterizan por ser cometidos por programas que no tienen la consideración de software malicioso, los servicios de mensajería instantánea, y que desde el punto de vista de la víctima existen múltiples eventos.

Como subcategoría dentro de los cibercrímenes están los ciberfraudes.

Llinares (2013) define desde una perspectiva criminológica el ciberfraude como: "variedad de conductas en las cuales las redes telemáticas se convierten en instrumento esencial mediante el cual lograr un beneficio patrimonial ilícito derivado de un perjuicio patrimonial a una víctima".

4.3. Mayores amenazas actuales

4.3.1. Ransomware

Symantec Corporation (2012: 2) define el "*ransomware*" como: "un tipo de software malicioso que cuando se ejecuta desactiva una funcionalidad del ordenador". Habitualmente, este tipo de software bloquea por completo el ordenador y exige una cantidad de dinero a cambio de restaurar las funciones del aparato.

El principal problema que existe con este tipo de software es la asimetría que existe entre el riesgo y la recompensa. Debido a la libertad que ofrece internet, y a la falta de coordinación internacional entre determinadas jurisdicciones, los criminales pueden esconderse detrás de legislaciones muy favorables a sus intereses económicos sin correr muchas veces el riesgo de ser detenidos o que se conozca su identidad (Prada, 2015). Como apuntan Luo y Liao (2007) esta situación provoca que se desincentive la participación en el comercio electrónico. Esto es un problema para gran parte de la industria financiera. Existen muchas empresas del sector que están involucradas en alguna etapa del comercio y una reducción en esta actividad podría ser devastadora para ellas. Que la población no confié en la contratación por Internet tampoco beneficia a empresas del sector financiero que ofrezcan servicios o productos online. Es por ello por lo que Luo y Liao (2007) proponen que el sector bancario adopte iniciativas para educar a la población en como evitar estos problemas y operar de forma segura online.

4.4.2. Ataques DoS y DDoS

Los ataques DoS o ataques de denegación de servicio son ataques a redes o hardware que tienen la finalidad de inutilizar determinados servicios inundando los servidores de actividad de tal forma que estos no puedan gestionar tal cantidad de datos de forma simultánea. La diferencia entre los ataques DoS y DDoS o ataques de denegación de servicio distribuido, radica en cuantos sistemas (normalmente se utilizan redes de -*bots*-) se emplean simultáneamente para lanzar el ataque. Si el atacante emplease dos o más sistemas en un ataque de estas características, entonces el ataque se podría catalogar como DDoS (Khajuria y Srivastava, 2013).

Los ataques de este estilo pueden también explotar puntos débiles en el software, aunque lo más normal es que se centren en consumir recursos como la banda ancha, la memoria o el poder de procesamiento de la víctima (Cheng, Kung y Tan, 2002).

Los ataques DoS y DDoS han sido frecuentes en entidades financieras. Destacan los ataques al HSBC en 2016, los cuales bloquearon el acceso a su plataforma online durante horas en Reino Unido (Osbourne, 2016); y los ataques a Bank of America, Citigroup, JP Morgan Chase, Wells Fargo U.S Bank y PNC en septiembre de 2012, los cuales ralentizaron e incluso bloquearon el acceso a los servicios online de estas empresas en Estados Unidos (Goldman, 2012).

4.3.2. "*Phishing*"

Antifishing working group (2008) (citado en Jaishankar, 2008: 11) define el "*phising*" como:

> "El mecanismo que emplea tanto la ingeniería social como subterfugios técnicos para robar la información personal y financiera de los consumidores. En los esquemas de ingeniería social, los criminales se hacen pasar por negocios o agencias existentes y legales llegando a emplear emails con sus direcciones o copias de sus páginas web con la intención de que los consumidores sean engañados y depositen ahí su información personal o financiera. Los planes que emplean subterfugios técnicos plantan en los ordenadores "*crimeware*" para robar directamente los credenciales o para corromper la infraestructura y que redirija a los consumidores a las páginas web falsificadas (o a las originales pero infiltrando un software de "k*eylogging*")."

Los "*keylogging*" son software, habitualmente integrados en "*bots*", que tienen la finalidad de registrar e interceptar toda la actividad del usuario, incluyendo el tecleado o los "*clicks"* que realiza. (Al- Hammadi y Aickelin, 2008).

La industria financiera también ha sido víctima de estos ataques. El caso más claro es de la banda que diseño el "*malware*" Carbanak y Cobalt. Esta banda criminal consiguió robar a más de 100 instituciones financieras un total de un billón de dólares. Esta banda utilizaba el "*fishing*" con altos ejecutivos de empresas financieras. Estos criminales mandaban emails haciéndose pasar por otras empresas para que estos ejecutivos se descargasen el malvare que habían diseñado, el cual infecta la infraestructura y conseguía que se realizasen determinadas transferencias que convenían a los criminales, que se inflasen los saldos de determinadas cuentas, o que determinados cajeros automáticos dieran dinero gratis (Eurpol, 2018).

4.4. Empleo de la Inteligencia artificial en la lucha contra el cibercrimen

La inteligencia artificial se puede emplear en la detección, predicción y respuesta ante el cibercrimen. En concreto en la detección y prevención de ataques DoS, en la detección de spam, en la detección de ordenadores zombis, en la clasificación del "*malware"* y como herramienta en las investigaciones de fraude (Tyugu, 2011).

4.4.1. Los agentes inteligentes

Los agentes inteligentes son sistemas de ordenadores autosuficientes e interconectados creados para comunicarse entre ellos y coordinarse para enfrentarse a las amenazas que puedan surgir. Los agentes inteligentes, dada su alta adaptabilidad y flexibilidad son utilizados normalmente como defensa para los ataques DDoS (Anwar y Hasan, 2017).

4.4.2. Las redes neuronales artificiales

Aygin, Çakir y Dilek, (2015: 25) definen las redes neuronales artificiales como "un mecanismo computacional que simula la estructura y funcionalidad de las redes neuronales existentes en sistemas biológicos. Su funcionamiento les hace ideal para situaciones en los que se requiera predicción, clasificación o control en entornos computacionales complejos y dinámicos" Las neuronas pueden ajustar sus parámetros y

estructura por medio de algoritmos de aprendizaje. De esta forma, la red neuronal puede adaptarse, minimizando los errores y proporcionando una solución que se adapte mejor al problema (Salas, 2000).

Ya se han realizado estudios de cómo aplicar las redes neuronales en la ciberseguridad.

Linda, Manic y Volmer (2009) en su paper "*Neural Network Based Intrusion Detection System for Critical Infrastructures"* describen consiguieron crear un sistema de detección de intrusiones informáticas adaptado a infraestructuras críticas que empleaba dos algoritmos de aprendizaje de redes neuronales, y que tenía una ratio de detección perfecto y sin falsos positivos.

Asimismo, Abdullah, Ahmad y Alghamdi (2009) en su "*paper"* "*Application of Artificial Neural Networks in Detection of DOS Attacks*" describen cómo incluyeron en su sistema de detección de ataques informáticos redes neuronales y consiguieron un 96,1% de precisión en la detección de ataques, porcentaje sustancialmente mayor del que se obtuvo utilizando otras aproximaciones al problema.

También destaca la aportación de Barman y Khataniar (2012), los cuales consiguieron diseñar un sistema de identificación de amenazas con redes neuronales con la misma efectividad que otros sistemas, pero 20.5 veces más rápido a la hora de detectar un tipo de ataque DoS.

Las redes neuronales ya se han implementado en la ciberseguridad de la industria financier. BBVA (2018) comenta que esta tecnología se utiliza sobre todo en la detección del fraude, detección de actividades de lavado de dinero y en la prevención de riesgos. Además, menciona como ejemplo a Brighterion, una empresa del sector financiero especializada en proporcionar este tipo de soluciones con redes neuronales artificiales y otras tecnologías de inteligencia artificial.

4.4.3. Sistemas inmunes artificiales

Nunes de Castro y Timmis, en su libro "*An Introduction to Artficial Inmune Systems: A New Computational Intelligence Paradigm*." (citado en Cruz, 2004), define los sistemas inmunes artificiales como: "sistemas adaptativos, inspirados por la teoría inmunológica, funciones, principios y modelos inmunológicos observados, los cuales son aplicados a la solución de problemas."

No existe una serie de características comunes a todos los sistemas inmunes artificiales. Aunque como regla general, los sistemas inmunes artificiales intentan: clasificar y/o detectar los elementos invasores; reaccionar ante el ataque invasor; aprender y ajustarse al entorno y al resultado de sus actuaciones; y tolerar aquellos elementos que son parte integrante del sistema que intenta proteger (Madhok, Gupta y Grover, 2016).

Por sus características, los sistemas inmunes en la ciberseguridad son utilizados principalmente en sistemas de identificación del spam y de amenazas en redes, y en sistemas de eliminación de dichas amenazas. También es frecuente su empleo en defensas contra los ataques DoS (Dasgupta y González, 2003).

Los sistemas inmunes artificiales suelen emplear 4 tipos de algoritmos: algoritmos de selección negativa, algoritmos de selección clonal, redes inmunitarias artificiales y la teoría del peligro (García, Maestre y Sandoval, 2015).

4.4.3.1. Tipos de algoritmos que emplean

Los algoritmos de selección negativa se fundamentan en el principio de la discriminación entre los elementos propios y los que no lo son. Su finalidad es intentar detectar elementos que discrepen de lo que se ha definido como normal o aceptable para el sistema que se analiza. Para realizar esta labor, se crean elementos detectores, encargado de distinguir que es propio del sistema y que no lo es, que luego serán cribados en función de su desempeño (Berry, Dasgupta, KrishnaKumar, Wong, 2004). Las propiedades de estos algoritmos los hacen idóneos para encontrar "*malware*" o detectar actividades fraudulentas.

Los algoritmos de selección clonal se basan en la teoría de selección clonal de inmunidad adquirida y en la maduración de la afinidad. Esta teoría explica como los linfocitos B y T se adaptan para luchar contra determinados antígenos. Los linfocitos B y T poseen una clase de receptor especializado en detectar un único antígeno. Cuando el linfocito detecta ese antígeno es entonces cuando se activan y producen el anticuerpo para destruir la amenaza. De esta forma, los linfocitos que son capaces de detectar el antígeno son seleccionados para pasar a la siguiente generación. La maduración de la afinidad es un proceso mediante el cual la respuesta de los anticuerpos producidos mejorara con la exposición a los patógenos. Este proceso se realiza también por selección natural,

seleccionando para la siguiente generación los linfocitos con mejores resultados en la respuesta ante el elemento invasor (Bautista, Diaz, Gómez y Luna, 2013).

Los algoritmos de redes inmunes se basan en la teoría de redes inmunes de Jerne y Perelson. Esta teoría defiende que el sistema inmunitario este compuesto por células y moléculas que son capaces de reconocerse unas a otras incluso en los casos de ausencia de antígenos. Cuando exista la presencia de antígenos y se detecten, determinados anticuerpos se activan. Estos anticuerpos que han sido activados a su vez activaran a otros y estos a otros, lo que al final provoca que se cree una especie de red donde todos los anticuerpos se detectan entre ellos (González, s.f.). Este tipo de algoritmos intentan crear este tipo de redes, eliminando aquellas partes poco útiles o mejoradas por otras en el proceso de entrenamiento de la red. Las redes inmunes artificiales se han utilizado en funciones como el análisis y clasificación de datos, el reconocimiento de patrones y proceso de optimización (Argüello, Ariel y Cuadrado, 2012).

Los algoritmos basados en la teoría del peligro se inspiran en la teoría del peligro de Polly Matzinger, la cual defiende que el sistema inmune no es capaz de diferenciar entre lo que es propio y lo que no lo es. Sin embargo, el sistema inmune si es capaz de diferenciar entre lo que es peligroso y lo que no lo es. Esta diferenciación es posible gracias a los tejidos lesionados, los cuales emitirían señales de alarma ante una amenaza que activaría al sistema inmune. Este tipo de algoritmos cuentan con operador de peligro encargado de detectar las amenazas y alertar al sistema (Pinilla, 2018).

4.4.4. Algoritmos genéticos

Los algoritmos genéticos son un tipo de algoritmos que incorporan elementos de la teoría evolutiva como la selección natural. Estos algoritmos modifican su composición aleatoriamente con cada generación e incorporan los avances que proporcionan los mejores resultados a la generación siguiente, donde el mismo proceso es repetido. De una forma más técnica, Goldberg (1989) (citado en Dorado et al, 2010: 11) los define como:

> "Algoritmos de búsqueda basados en la mecánica de selección natural y de la genética natural. Combinan la supervivencia del más apto entre estructuras de secuencias con un intercambio de información estructurado, aunque aleatorizado, para constituir así un algoritmo de búsqueda que tenga algo de las genialidades de las búsquedas humanas"

Los algoritmos genéticos son muy utilizados en sistemas de detección de intrusos y son idóneos para generar reglas de detección de anomalías. Llevan siendo aplicados en ciberseguridad desde los años 90 y son utilizados incluso hoy (Aziz et al, 2012).

4.4.5. Sistemas expertos

Los sistemas expertos son sistemas informáticos que emulan a un experto en un área concreta. Estos sistemas normalmente son capaces de almacenar procesar información y aprender (Castillo, Gutiérrez y Hadi, 1997).

Los sistemas expertos son la herramienta de inteligencia artificial más utilizada. Debido a su especialización estos sistemas pueden tener muy diversas funciones. Las más habituales suelen ser funciones de diagnóstico y de resolución de problemas complejos. En ciberseguridad los sistemas expertos son utilizados en la detección de amenazas y en decidir como distribuir de manera eficiente los recursos computacionales escasos (Anwar y Hassan, 2017).

4.5. Ventajas de las distintas técnicas de inteligencia artificial en la ciberseguridad

El uso de técnicas de inteligencia artificial en la ciberseguridad aporta grandes ventajas. La tabla 3 resume estas ventajas en función de las técnicas de inteligencia artificial.

Tabla 3.

Tecnología	Ventajas
Redes neuronales artificiales	• Aprenden con el ejemplo • Son capaces de operar de manera eficaz con funciones complejas no lineales • Manejan de manera excepcional funciones diferenciales complejas • Son resilientes a los datos ruidosos y a los datos incompletos
Agentes inteligentes	• Siempre intentan completar la tarea, incluso cuando tienen objetivos contradictorios. • Actúan de forma racional a la hora de completar sus objetivos. • Se adaptan con facilidad al entorno y a las preferencias del usuario.

	• Son cocientes de los errores humanos, por lo que pueden ser programados para revisar las instrucciones e inconsistencias que se le han impuesto.
Sistemas inmunes artificiales	• Tienen una estructura dinámica. • Cuentan con medios de aprendizaje distribuido. • Se adaptan y organizan por si solos, sin necesidad de intervención humana. • Son capaces de seleccionar la mejor respuesta para eliminar la amenaza del sistema. • Optimizan los recursos • Cuentan con varias capas de defensa • Al no ser dependientes de ningún elemento en particular, pueden desprenderse y remplazar cualquiera de ellos por uno que tenga un desempeño más alto
Algoritmos genéticos	• Se adaptan al entorno de manera eficiente • Son capaces de optimizar incluso problemas computacionales complejos. • Permiten evaluar varios tipos de posibles soluciones de manera simultánea.
Sistemas expertos	• Pueden ser empleados para una gran variedad de problemas • Ofrecen soluciones a como distribuir los recursos de manera eficiente

Adaptado de: Aydin, Çakir y Dilek, (2015) y Anwar y Hassan (2017)

4.6. Usos de la inteligencia artificial en la ciberseguridad

La inteligencia artificial tiene un gran potencial en el campo de la ciberseguridad. La inteligencia artificial ya se utiliza en la actualidad, aunque todavía le queda desarrollo. La tabla 4 resume los campos donde más potencial tiene.

Tabla 4

Usos de la inteligencia artificial en ciberseguridad	**Descripción**
Evaluación del riesgo de las redes	Realización de una evaluación del riesgo basado en los datos y el análisis cuantitativo sin depender de los sesgos del analista.
Detección de amenazas	Algunas tecnologías de la inteligencia artificial pueden detectar y atacar cualquier actividad que consideren sospechosa. Asimismo, podría detectar patrones anómalos, como transacciones fuere de lo normal, y alertar al sistema.
Análisis del comportamiento	Identificación de los comportamientos y clasificación de estos dependiendo de si se traten de acciones humanas o no. Gracias a este tipo de análisis se pueden detectar y eliminar de manera automática y con gran precisión muchos de los ataques que se producen en la actualidad como los DoS. Además, esta tecnología podría facilitar mucho las operaciones antilavado de dinero.
Detección del fraude	Detección del fraude y optimización de los procesos a través del "*machine learning*".
Detección del malvare	Utilización de los datos recopilados sobre las características de los distintos tipos de malvare con los que el sistema se ha encontrado u obtenido información acerca de ellos, para detectar futuras amenazas que otros acercamientos al problema puede que no consigan detectar

Adaptado de Capgemini (2019*).*

5. Los "*robo advisors*"

5.1. Introducción

Cárpatos (2015) cataloga a los inversores en dos grupos: los leones (grandes inversores institucionales con gran poder sobre el mercado) y las gacelas (inversores particulares o minoristas que normalmente emplean métodos poco sofisticados para invertir). Como los nombres propuestos sugieren, los leones se suelen alimentar de las gacelas. Debido a su gran tamaño, los inversores institucionales pueden manipular el mercado a su antojo. Claro ejemplo de esto lo podemos apreciar en la crisis del coronavirus, donde varios "*hedge funds*" americanos, con Bridgewater a la cabeza (Bayón, 2020), asediaron el Ibex con posiciones cortas, haciendo que el Ibex tuviera una de las mayores bajadas de su historia, 20.86% en una semana (Igartua, 2020).

Tal fue la bajada que estos fondos provocaron que primero el 12 de marzo de 2020 la CNMV tuviera que prohibir las ventas en corto durante un día. Como la medida seguía siendo insatisfactoria, el 16 de marzo, la CNMV decidió prohibirlas durante un mes entero (Veloso, 2020).

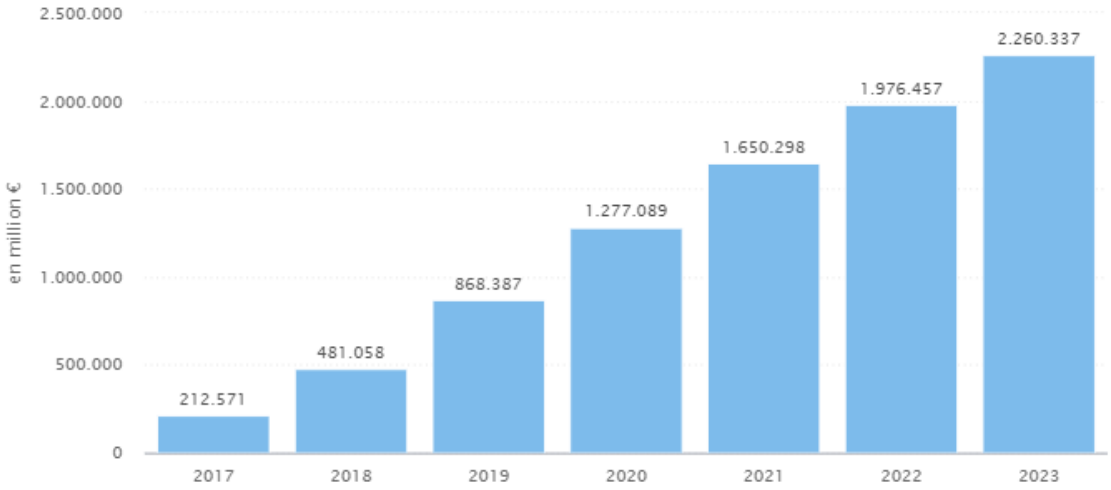
El tamaño no es el único factor determinante en el éxito de un inversor. Sin duda, la metodología y la técnica juegan un papel fundamental. Por regla general el inversor minorista tiene menos conocimiento sobre los mercados financieros y sobre las distintas técnicas de inversión que el inversor institucional. Estas carencias se pueden observar sobre todo en las inversiones de CFD (contratos por diferencia). Sin entrar mucho en detalle, los CFD son: "contratos en el que se intercambia la diferencia entre el precio de compra y el precio de venta de un activo. Como por ejemplo una **acción**, pero sin necesidad de tener en propiedad esas acciones" (Sevilla, 2020). La falta de conocimiento de los inversores minoristas en la gestión de riesgo y el alto grado de apalancamiento que estos instrumentos hacen que la mayoría de los particulares que operan con ellos pierdan dinero. Entre el 65% y el 86% de los inversores minoristas que operan con estos productos pierden dinero con ellos (Martín, 2018).

Dentro del duro mundo de los mercados financieros, un avance que ha ayudado a miles de personas a sobrevivir, incrementar su patrimonio y nivelar el campo de juego, ha sido el desarrollo de los *"robo-advisors*". Los "robo-advisors" son "servicios online de

asesoramiento financiero y gestión del patrimonio que emplean algoritmos para proveer sus servicios de manera automatizada y sin apenas intervención humana" (Frankenfield, 2019). Los algoritmos que emplean son capaces de recomendar una asignación optima de los recursos disponibles de entre todos los activos a su disposición, en virtud de los objetivos económicos del cliente y su perfil de riesgo. Asimismo, algunos algoritmos son capaces de rebalancear las carteras ellos mismos, o reinvertir los dividendos generados (Montoya, 2018).

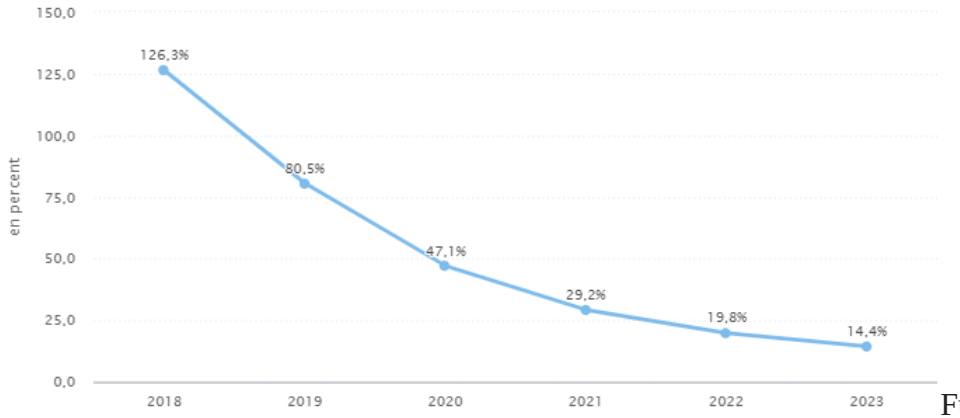
La disrupción en el mundo de la gestión de patrimonio y la inversión es evidente. A raíz de sus bajos costes y su alto rendimiento, los activos bajo gestión de estos servicios no han parado de aumentar. Statista (2020) estima que en 2017 los "*robo advisors"* tenían bajo gestión 212.571 millones de euros. Esta cantidad en 2020 asciende a 1.277.089 millones de euros. Statista estima que esta cantidad crecerá hasta 2023 a un 23% anual

Gráfico 2: Proyección de los activos bajo gestión de los "*robo advisors*"



Fuente: Statista (2019)

Gráfico 3: Crecimiento de los activos bajo gestión de los robo advisors



Fuente: Statista (2019)

5.2. Funciones de los "*robo advisors*"

Bjerknes y Vukovic (2017) dividen el funcionamiento de la mayoría de los "robo *advisors*" en 5 categorías

5.2.1. Establecimiento del perfil de riesgo del cliente

Antes de poder asesorar a un cliente sobre posibles alternativas de inversión es necesario saber cuál es el nivel de riesgo que éste está dispuesto a aceptar. La mayoría de "*robo advisors*" basan sus recomendaciones en un modelo de análisis de media-varianza por lo que conocer el nivel de riesgo del cliente es la única manera de poder construir una cartera de acuerdo con sus expectativas. Estos modelos se basan en los principios del modelo de carteras introducido por Markowitz, y desarrollado en la teoría moderna de carteras.

Los modelos de media-varianza tienen el objetivo de obtener una cartera que, para una rentabilidad esperada, obtenga el mínimo riesgo posible, o para un riesgo determinado, la mayor rentabilidad. Se utiliza la denominación media-varianza para definir a estos modelos porque el riesgo es medido a través de la varianza de las rentabilidades de la cartera y la rentabilidad a través de la media de las rentabilidades esperadas (Villalba, 2016: 53-54).

Para conocer a sus clientes, estas empresas realizan encuestas orientadas a conocer el perfil de riesgo del cliente, sus objetivos de inversión y cualquier otra característica relevante para poder construir el porfolio óptimo para esa persona (Bradford, 2018).

5.2.2. Selección de la clase de activos

El segundo paso en el asesoramiento de inversiones es seleccionar la clase de activos que se van a valorar cumplir con los requisitos del perfil del inversor. A la hora de construir la cartera es esencial encontrar activos con baja correlación para conseguir una buena diversificación. Los "*robo advisors*" suelen barajar una amplia gama de activos los más frecuentes siendo las acciones, los bonos y las "*commodities*" como el oro. La selección de una determinada clase de activos puede venir motivada por diversos motivos. Los más comunes son: obtener crecimiento en la cartera, conseguir flujos de caja estables, proteger la cartera ante la inflación o alcanzar la eficiencia fiscal.

5.2.3. Selección del vehículo de inversión

Seleccionada la clase de activos en los que se va a invertir, el siguiente paso para el "*robo advisors*" es seleccionar el vehículo de inversión. Existen múltiples vehículos de inversión a disposición del "*robo advisors*". Algunos ejemplos son los fondos de inversión, fondos de inversión indexados (fondos de gestión pasiva que replican un índice), los "*hedge funds*", las SICAV o la compra directa de los instrumentos financieros.

5.2.3.1. Las SICAV

"Las Sociedades de Inversión en Capital Variable (en adelante, SICAV) son una de las modalidades que, de acuerdo con la Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva (en adelante, LIIC), tienen como objeto la adquisición, tenencia, disfrute, armonización y enajenación de valores mobiliarios y de otros activos financieros." (Luque, 2014: 2).

Los motivos por los que se emplean estos instrumentos de inversión colectiva son de índole fiscal. Estas sociedades tributan al 1% de Impuesto de Sociedades y permiten diferir el pago del impuesto por los inversores hasta cuando ellos recuperen su inversión, lo que permite que se pueda hacer una buena planificación fiscal ("¿Qué son las Sicavs?", 2014).

Apenas son utilizados por este tipo de asesores, aunque nada impide que en el futuro su uso se haga más frecuente

5.2.3.2. Los "Hedge funds" o Fondos de cobertura

Debido a su alta heterogeneidad no existe una defición de "hedge fund" aceptada universalmente. Como aproximación al concepto, se puede decir que son vehículos de inversión que pueden adoptar la forma de fondo de inversión o sociedad de inversión colectiva, entre otras formas jurídicas, que se caracterizan por su escasa regulación; su libertad a la hora de invertir, muchas veces sin más limites que los impuestos en sus reglamentos; el empleo de derivados (instrumentos financieros cuyo valor depende del valor de otro activo subyacente) y de posiciones cortas a través de préstamos de valores (venta de activos prestados realizada con la finalidad de que durante el periodo de préstamo del activo el valor de éste baje y se pueda comprar cuando se devuelva más barato); utilizar grandes niveles de apalancamiento; y estar domiciliados en paraísos fiscales (Hurtado, s.f.).

Las rentabilidades que ofrecen estos fondos suelen ser elevadas fruto de su gran apalancamiento, sin embargo, su volatilidad también suele ser bastante alta.

Apenas son utilizados por estos asesores. Normalmente son empleados por inversores institucionales o individuos con un alto patrimonio con una alta tolerancia al riesgo. Estos fondos habitualmente cobran altas comisiones. Lo normal es que tengan una comisión del 1.5% de los activos bajo gestión (denominado el "*management fee*") y una comisión del 20% sobre los rendimientos que supere un "*benchmark*" definido (denominado "*incentive fee*") (Chen, Ibbotson y Zhu, 2011).

Por regla general, los "*robo advisors*" suelen elegir fondos cotizados (normalmente indexados) y fondos con pocas comisiones.

5.2.4. Construcción del porfolio

La inmensa mayoría de los "*robo advisors*" utilizan el modelo de optimización de media-varianza, o alguna de sus variantes, para construir su cartera. Este tipo de modelos seleccionan los activos en los que se va a invertir, así como los pesos de esos activos en la composición de la cartera, minimizando la varianza de la cartera para una rentabilidad determinada (medida a través de la media de los retornos de los activos), o maximizando la rentabilidad en función de una volatilidad determinada (medida a través de la varianza de la rentabilidad esperada) (Villalba, 2016: 53-54).

El fundamento de este modelo es que, al incrementar la diversificación de la cartera, se puede conseguir más rentabilidad por unidad de riesgo (Lam, 2016). Además, al ser relativamente sencillo de calcular, resulta un modelo muy atractivo.

5.2.5. Supervisión, rebalanceo y cosecha de pérdidas fiscales

La mayoría de los "*robo advisors*" siguen una estrategia de inversión pasiva. Estos asesores se suelen indexar a un índice, reajustando la cartera en caso de desviaciones significativas en los valores. El empleo de algoritmos les permite realizar los reajustes de forma fácil, eficiente y sin que los sesgos cognitivos humanos se pongan de por medio. A pesar de que normalmente los "*robo advisors*" funcionan a través de la inversión pasiva, nada impide que puedan operar con estrategias de inversión activa.

Las principales desventajas del rebalanceo de la cartera son los impuestos y los costes de transacción que se generan. No obstante, la naturaleza de estos asesores permite optimizar estos procesos a través de modelos matemáticos y algoritmos.

Otra función que pueden desempeñar este tipo de asesores es la cosecha de pérdidas fiscales. Betterment (s.f.) define la cosecha de pérdidas fiscales como:

> "la práctica de vender instrumentos financieros que hayan incurrido en pérdida para compensar los impuestos generados por otras ganancias de capital o rendimientos del capital mobiliario dentro de las rentas del ahorro, para acto seguido comprar activos similares que mantendrán la forma ideal de la cartera de valores."

Algunos "*robo advisors*" son capaces de optimizar esta función y ahorrar a sus clientes cientos de euros en impuestos.

5.3. Tipos de "robo advisors"

5.3.1. En función de sus prestaciones

No todos los "*robo advisors*" que hay en el mercado son iguales. Esta tecnología ha evolucionado de ser una simple herramienta utilizada por algunos gestores de fondos a poder sustituirlos por completo. Deloitte (2016) divide los "*robo advisors"* en cuatro grupos en función de su sofisticación y prestaciones.

5.3.1.1. "Robo advisors" 1.0

Este tipo de "*robo advisors"* ofrecen solamente o un producto determinado, o un porfolio basado en las respuestas que el inversor haya podido dar a un cuestionario sobre su perfil de riesgo y sus expectativas económicas. En este caso es el cliente quien tiene que ejecutar las transacciones para construir el porfolio y realizar los ajustes necesarios en función del mercado con su propia cuenta

5.3.1.2. "Robo advisors" 2.0

En este supuesto, los "robo advisors" emiten recomendaciones de porfolios y productos ajustados al perfil de riesgo del cliente, pero son los gestores profesionales los que supervisan, rebalancean y realizan las transacciones necesarias.

5.3.1.3. "Robo advisors" 3.0

En este caso las decisiones de inversión, las transacciones necesarias para ejecutar la estrategia y el rebalanceo de las carteras de inversión, es realizado de forma automática por el "*robo advisor*" a través de algoritmos. Las reglas de estos algoritmos son predefinidas por los gestores, los cuales supervisan también el trabajo de esta tecnología.

5.3.1.4. "Robo advisors" 4.0

Los "*robo advisors*" de esta categoría son sin duda los más sofisticados. A parte de las prestaciones que ofrecen los "*robo advisors*" anteriores, los de esta categoría ofrecen también sistemas de gestión del riesgo, sistemas de "*machine learning"* para mejorar de forma constante el rendimiento y sistemas de adaptación de las carteras a tiempo real en función de las condiciones de mercado y las preferencias del inversor. En estos casos debido a la gran complejidad de los sistemas la intervención y supervisión humana es muy escasa, por no decir inexistente.

5.3.2. En función de la intervención humana

Los "*robo advisors*" también se pueden dividir en dos categorías en función del grado de intervención humana a la hora de tomar las decisiones de inversión. Estas dos categorías son: los automatizados y los que son utilizados como una simple herramienta (Price Waterhouse Coopers, 2017).

5.3.2.1. Automatizados

Dentro del grupo de los automatizados nos podemos encontrar tres subgrupos: los independientes, los segmentados y los integrados.

5.3.2.1.1. "*Robo advisors*" independientes

Los "*robo advisors*" independientes se ocupan de definir por sí solos el perfil de riesgo de los clientes, construir la cartera en función de su tolerancia al riesgo y sus objetivos económicos, y reajustarla.

La normativa Mifid II en su artículo 24.7 (Real Decreto 1464, 2018) establece dos requisitos necesarios para que el asesoramiento se considere independiente. Estos requisitos son:

1º Que se ofrezcan y consideren una amplia gama de instrumentos financieros tanto en lo que se refiere a su tipo como en lo concerniente a su proveedor, con el fin de garantizar de satisfacer las pretensiones del inversor y sin que los instrumentos ofrecidos se limiten a solo los emitidos por una sola empresa de servicios de inversión, entidades que tengan vínculos estrechos con la empresa de servicios de inversión u entidades con las que las empresas de servicios de inversión puedan tener vínculos estrechos, económicos o jurídicos, que puedan incidir en la independencia del servicio.

2º Que no se acepten honorarios, comisiones u otros beneficios monetarios u de otro tipo por un tercero o alguien relacionado, por la prestación del servicio al cliente.

5.3.2.1.2. "*Robo advisor*" segmentados

Este tipo de "*robo advisors*" están a caballos entre la independencia y la dependencia. Es común que en estos casos se tengan acuerdos de distribución con el proveedor de los productos financieros, lo que hace que su independencia se ponga en entredicho. Este tipo asesores están incluidos dentro de grupos bancarios o grupos de empresas de inversión, pero no están integrados dentro del grupo. Dentro de esta categoría se pueden encontrar dos modelos distintos dependiendo de si se cobran incentivos del proveedor de activos o grupo o no.

5.3.2.1.3. "*Robo advisors*" integrados

Este tipo de "*robo advisors*" están integrados dentro del banco o el grupo de inversión y proporcionan servicios dentro de la estructura de la empresa. En este caso dependen

íntegramente de la empresa de la que son parte y no son ni un asesor independiente ni una entidad legal separada.

5.3.2.2. "Robo advisors" como herramientas

En este caso los "*robo advisors"* son utilizados como una plataforma de soporte para asesores humanos. Estos tomarán en cuenta las recomendaciones emitidas, sin embargo, la decisión finalmente recae en el juicio discrecional del asesor. En este supuesto el contrato de asesoramiento y/o gestión será entre el cliente y el asesor, no entre el cliente y el "*robo advisor*".

5.4. Ventajas y desventajas de los "*robo advisors*".

5.4.1. Ventajas

Entre las ventajas de los "*robo advisors*" podemos mencionar las siguientes:

1. Los "*robo advisors*" suelen exigir cantidades muy pequeñas para poder operar con ellos. La mayoría suelen exigir un balance inicial de entre 1000- 10 000 dólares, aunque existen algunos que no exigen requisitos mínimos (Fein, 2015).

2. Un asesor humano suele exigir una comisión de entre el 1 y 2% de los activos bajo gestión. Un "*robo advisors*" por regla general exige comisiones de entre 0 y 50 puntos básicos. Esta reducción en los costes es principalmente producida por el aprovechamiento de las economías de escala y en la reducción de personal que este modelo de negocio conlleva (Center, Fisch, Laboure, Turner, 2017).

3. Otra ventaja que otorgan los "*robo advisors*" es su inmediatez y su facilidad de uso. Después del alta online en la plataforma que proporciona los servicios, los dos únicos trámites adicionales que el inversor debe cumplimentar son: responder a una encuesta para determinar su perfil de tolerancia al riesgo y expectativas; y realizar un depósito para que el "*robo adivsor*" conforme la cartera (esto no es siempre así debido a que hay casos donde los "*robo advisors"* solo prestan asesoramiento) (Becker, 2019).

4. Accenture (2015) señala que a muchos clientes de estos servicios les gusta la experiencia que ofrecen, en particular, la alta privacidad que otorga una solución digital. No todo el mundo se siente cómodo revelando su riqueza ante un extraño. Los "*robo advisors*" en este sentido ofrecen una solución con mayor discreción.

5.4.2. Desventajas

A pesar de sus múltiples ventajas, los "*robo advisors*" cuentan con carencia significativas:

1. La más significativa sin duda es la falta del componente humano. Muchos inversores desean poder hablar con su asesor para que les pueda explicar y guiarles en situaciones complicadas en los mercados. Los clientes no son sistemas informáticos. Como cualquier persona en tiempos turbulentos es posible que actúen de manera irracional. Tener una persona que te pueda asesorar, tranquilizar y resolver tus dudas, sin duda aporta gran valor a los servicios de asesoramiento (BBVA, 2018).

2. Otra desventaja es el hecho de que las decisiones que el "*robo advisor*" toma se fundan en un simple cuestionario que puede o no reflejar la realidad del inversor. Esta falta de fiabilidad puede que haga que el asesoramiento no se ajuste a las verdaderas necesidades del cliente. Es muy frecuente que el cliente no sea del todo transparente o que desconozca cuál es su verdadero nivel de tolerancia al riesgo (Center et al, 2017). Los sentimientos son impredecibles, y muchas veces, hasta que no se han pasado experiencias similares, no se sabe cómo se va a actuar.

3. Un inconveniente más de los" *robo advisors*" es que muchos tienen un universo de inversión limitado. Una gran cantidad de "*robo advisors*" solo consideran un puñado de fondos indexados para construir sus carteras, lo que puede provocar una excesiva estandarización de los servicios ofrecidos. Estos tipos de asesores suelen elegir fondos con comisiones muy bajas, descartando muchas veces fondos que a pesar de que tengan comisiones más altas, puedan ser mucho más rentable (Initio, 2019).

5.5. Futuro de los "*robo advisors"*

Los "*robo advisors"* son una de las tecnologías más disruptivas en el mundo de los servicios financieros. Estos avances han permitido que cientos de personas que antes no podían por no cumplir los requisitos mínimos de capital inicial, accedan a los servicios de asesoramiento de gestión de patrimonios. Asimismo, estos asesores han permitido que cientos de personas, legos en materia de mercados financieros e inversión, pudieran incrementar su patrimonio.

El potencial de esta tecnología es considerable. Los "*robo advisors*" pueden volverse aún más complejos, ajustándose incluso más a las necesidades de sus clientes. Con acceso a datos como los ingresos, gastos o hábitos de consumo de su clientela y con técnicas de inteligencia artificial, el asesoramiento se podría optimizar de manera sustancial.

Koh y Phon (2017) señalan posibles áreas de mejora y desarrollo de los "*robo advisors"* para poder dar un servicio más completo. Las principales áreas son: la estructuración de planes de retiro; las planificaciones sucesorias; las planificaciones fiscales; la gestión de seguros; la educación financiera a la clientela que lo desee; el desarrollo del análisis de datos y de la inteligencia artificial para encontrar inversiones que se adecuen mejor al perfil de los clientes, así como para ofrecer "*insights*" sobre los mercados; y mejorar el servicio de atención al cliente a través de "*chatbots*" que puedan solucionar las dudas más frecuentes.

El avance de este tipo de tecnología es imparable, aunque no parece que a corto plazo vayan a sustituir a los asesores humanos. Las tendencias más recientes apuntan a la adopción de modelos híbridos o mixtos. Ambos tipos de asesores, tanto los "*robo advisors*" como los asesores humanos, cuentan con una serie de ventajas y desventajas que se pueden complementar con facilidad. Tradicionalmente la industria de la gestión de patrimonios estaba reservada para un selecto grupo de personas. Ahora, gracias a los "*robo advisors*", no solo está mejorando la calidad del servicio, sino que cada vez más gente puede acceder a los servicios de asesoramiento y gestión de su patrimonio (Centre, 2017).

6. Conclusiones

A pesar del lento despegue de la inteligencia artificial, su desarrollo reciente ha sido vertiginoso. La implementación del trading algorítmico y el trading de alta velocidad ha eliminado el trabajo de muchos "*traders*" tradicionales, bajado los costes de intermediación, incrementado por regla general la liquidez en los mercados y ayudado a la formación de precios de muchos activos financieros. A pesar de estos avances positivos, esta tecnología también ha incrementado el riesgo de endogeneidad entre los agentes que utilizan esta tecnología. Claro ejemplo de esto es el "*flash-crash*" del 6 de mayo, provocado por un evento que desarrolló una reacción en cadena sin sentido.

El impacto de la inteligencia artificial en la ciberseguridad también ha sido notable. A pesar de que haya empresas que la hayan implementado ya en sus soluciones de ciberseguridad, todavía su uso no es generalizado. Las tecnologías más prometedoras en este campo son las redes neuronales artificiales, los agentes inteligentes, los algoritmos genéticos, los sistemas inmunes artificiales y los sistemas expertos. Los usos potenciales que se le puede dar a estas tecnologías son muy variados, desde la prevención de ataques DoS, hasta el análisis de comportamientos sospechosos o detección del "*malware*".

Los "*robo advisors*" han cambiado sustancialmente la industria de la gestión del patrimonio. Existen muchos tipos de "*robo advisors*". Estos se pueden dividir dependiendo de su sofisticación, su independencia o su uso. Tanto los activos bajo gestión de esta tecnología como sus prestaciones han ido aumentando con los años. Este éxito en gran parte es debido a su reducido coste, su privacidad y a las pocas exigencias de capital mínimo. Los "*robo advisors*" han conseguido que gente de clase media e incluso clase trabajadora puedan acceder a servicios de gestión de patrimonios y asesoramiento financiero a un precio asequible.

La gran desventaja de los "*robo advisors*" es sin duda la falta del componente humano y a veces las limitadas soluciones que ofrecen. Todavía estamos muy lejos de un mundo donde los asesores y gestores de patrimonio tradicionales desaparezcan, pero cada vez es más frecuente que se integre esta tecnología en los servicios que se ofrecen para conseguir lo mejor de ambos mundos.

Es innegable que la inteligencia artificial ha tenido una gran influencia en los mercados, sin embargo, bajo mi punto de vista, no ha sobrepasado las expectativas que había generado. Es verdad que ha conseguido reducir el precio de los servicios y productos que se ofrecen en la industria y mejorado la calidad de estos, no obstante, parece que pecan de no valorar bien el componente humano. Los "*high frequency traders*" pueden volverse locos si una persona actúa de manera irracional en el mercado. Los sistemas de ciberseguridad fallan muchas veces por no tomar en cuenta que la gente puede ser engañada y hacer algo estúpido (como ocurre con el "*phishing*"). Los "*robo advisors"* son incapaces de tranquilizar a una persona que ve sus ahorros caer en bolsa y desea vender de inmediato (aunque vaya totalmente en contra de sus intereses), porque no entienden lo que se siente al perder todo el trabajo de una vida. Es evidente que muchas tareas ya han sido automatizadas por esta tecnología y que otras van por este camino, pero no creo que vayan a sustituir otras muchas al carecer de ese toque personal. Hacer una predicción de cómo va a ser el futuro siempre es complicado. En la Edad Media, nadie podría haber adivinado que íbamos a tener gran parte del conocimiento humano en la palma de nuestra mano. Empero, si tuviese que hacer esa predicción yo creo que el futuro es hibrido. Lo más probable es que nos complementemos con la inteligencia artificial para suplir las deficiencias mutuas, pero quien sabe, igual los avances en esta materia nos dejarán obsoletos.

7. Bibliografía

Abdullah, A. B., Ahmad, I., & Alghamdi, A. S. (2009, October). Application of artificial neural network in detection of DOS attacks. En *Proceedings of the 2nd international conference on Security of information and networks* (pp. 229-234). ACM

About ENISA. (s.f). *ENISA*. Recuperado de https://www.enisa.europa.eu/about-enisa

About us. (s.f.). Tradebot System. Recuperado de http://tradebot.com/about.asp

Abril, I. (2020) BBVA alerta del crimen organizado especializado en banca y pone en guardia frente a sus ciberataques. *Expansión*. Recuperado de https://cutt.ly/Qt6zFg1

Accenture. (2015). The Rise of Robo- Advice: Changing the Concept of Wealth Management (15-4356). Recuperado de https://cutt.ly/4tGeEun

Ahlstedt, J., & Villysson, J. (2012). High frequency trading. *Research Paper*, 1-8. Recuperado de https://cutt.ly/Xt6h0A2

Al-Hammadi, Y., & Aickelin, U. (2008, March). Detecting bots based on keylogging activities. En *2008 Third International Conference on Availability, Reliability and Security* (pp. 896-902). Piscataway, Estados Unidos: IEEE

Anwar, A., & Hassan, S. I. (2017). Applying Artificial Intelligence Techniques to Prevent Cyber Assaults. *International Journal of Computational Intelligence Research*, *13*(5), 883-889.

Arbitraje financiero (s.f). *Bestinver*. Recuperado de https://www.bestinver.es/terminos/arbitraje-financiero/

Argüello, H., Ariel, W., & Cuadrado, M. I. (2012). Algorítmo basado en una red inmune artificial para la alineación de patrones de puntos. Revista de la Escuela Colombiana de Ingeniería, 5(86), 25-33

Arnuk, S., & Saluzzi, J. (2009). Latency arbitrage: The real power behind predatory high frequency trading. Recuperado de https://blog.themistrading.com/2009/12/latency-arbitragethe-real-power-behind-predatory-high-frequency-trading/

Aydin, M., Çakir, H., & Dilek, S. (2015). Applications of artificial intelligence techniques to combating cyber crimes: a review. *International Journal of Artificial Intelligence & Applications*, *6*(1), 21.

Aziz, A. S. A., Hanafi S. E. L., Hassanien, & A. E. Salama, M. (2012). Detectors generation using genetic algorithm for a negative selection inspired anomaly network intrusion detection system. In *2012 Federated Conference on Computer Science and Information Systems (FedCSIS)* (pp. 597-602). Piscataway, Estados Unidos: IEEE.

Banko, M., & Brill, E. (2001). Scaling to very very large corpora for natural language disambiguation. En *Proceedings of the 39th annual meeting on association for computational linguistics* (pp. 26-33). Stroudsburg, Estados Unidos: Association for Computational Linguistics.

Baños, D (21 de septiembre de 2019). El cibercrimen, un delito con una impunidad de "casi el 100%" en España. *El Mundo.* Recuperado de https://cutt.ly/BtDYHSq

Barman, D. K., & Khataniar, G. (2012). Design of intrusion detection system based on artificial neural network and application of rough set. *International Journal of Computer Science and Communication Networks*, *2*(4), 548-552.

Bayón, A. (24 de marzo de 2020). Los ocho "hedge funds" que tumbaron al Ibex en su peor semana desde 2008. Cinco días, El País. Recuperado de https://cutt.ly/dtFrjD0

BBVA (2018). "Robo-advisors": que son y por qué hay que tenerlos en cuenta a la hora de invertir. *BBVA.* Recuperado de https://cutt.ly/mtGttEA

BBVA. (2018). Inteligencia Artificial y Big Data aplicados al negocio bancario. Recuperado de https://cutt.ly/Wt5iigl

Becker, M. (29 de octubre de 2019) The Pros and Cons of Investing With Robo Advisors. *The Simple Dollar*. Recuperado de https://cutt.ly/LtGw7om

Bengio, Y., Courville, A., Goodfellow, I., Mirza, M., Ozair, S., Pouget-Abadie, J., … Xu, B. (2014). Generative adversarial nets. En *Advances in neural information processing systems* (pp. 2672-2680). Cambridge, Estados Unidos: The MIT Press

Berry, M. Dasgupta, D., KrishnaKumar, K., & Wong, D., (2004). Negative selection algorithm for aircraft fault detection. En *International Conference on Artificial Immune Systems* (pp. 1-13).

Betterment (s.f.) Tax Loss Harvesting. *Betterment.* Recuperado de https://www.betterment.com/tax-loss-harvesting/

Biais, B. and T. Foucault (2014). Hft and market quality. *Bankers, Markets & Investors* (128), 5–19.

Bjerknes, L., & Vukovic, A., (2017). *Automated advice: A portfolio management perspective on robo-advisors* (Tesis de Máster) Norwegian University of Science and Technology, Høgskoleringen, Noruega

Boden, M. A. (2006). *Mind as machine: A history of cognitive science, Vol. 1.* Oxford, Inglaterra: Oxford University Press.

Boehmer, E., Fong, K., & Wu, J. (2012, March). International evidence on algorithmic trading. *Working Paper*. Recuperado de https://cutt.ly/kt6kaln

Bosker, B. (22 de enero de 2013). SIRI RISING: The Inside Story Of Siri's Origins — And Why She Could Overshadow The iPhone. *Huffington Post*. Recuperado de https://cutt.ly/3tONQDZ

Boston Dynamics. Legacy robots, The robots that built the groundwork for today´s portfolio. (s.f.). *Boston Dynamics*. Recuperado de https://www.bostondynamics.com/legacy

Bradford, D. (2018). La nueva era de la industria de corretaje en Colombia con la llegada de los robo-advisors (Trabao de fin de grado) Bogotá, Colombia

Brogaard, J., Hendershott, T., & Riordan, R. (2014). High-frequency trading and price discovery. *The Review of Financial Studies*, *27*(8), 2267-2306.

Buchanan, B. (2 de febrero de 2020). How North Korean Hackers Rob Banks Around the World. *Wired*. Recuperado de https://cutt.ly/Xt7SvUb

Buchanan, B. G., & Feigenbaum, E. A. (1980). The stanford heuristic programming project: Goals and activities. *AI Magazine*, *1*(1), 25-25.

Buchanan, B. G., & Feigenbaum, E. A. (1993). DENDRAL and Meta-DENDRAL: roots of knowledge systems and expert system applications. *Artificial Intelligence*, 59(1-2), 233-240.

Bullock, N., Rennison, & Mayer, G. (2018). How high-frequency trading hit a speed bump. *Financial Times.* Recuperado de https://cutt.ly/ZtA9kUe

Capgemini. (2019*). Reinventing Cybersecurity with Artificial Intelligence* (V06). Recuperado de https://cutt.ly/atDP8oq

Carpatos, J.L. (2014). *Leones contra gacelas: manual completo del especulador*. Madrid, España: Grupo Planeta España.

Castillo, E., Gutiérrez, J. M., & Hadi, A. S. (1997). Sistemas expertos y modelos de redes probabilısticas. Madrid, España: *Academia Española de Ingeniería*.

Center, P. P., Fisch, J. E., Laboure, M., & Turner, J. A., (2017). The economics of complex decision making: The emergence of the robo adviser. The AllianzGI-Oxford Pensions Conference, *Worcester College, September* (pp. 11-12).

Cesari, R., Marzo, M., & Zagaglia, P. (2012). Effective trade execution. Recuperado de https://arxiv.org/ftp/arxiv/papers/1206/1206.5324.pdf

CFA Institute. (s.f). Dark Pool Trading & Finance. *CFA Institute*. Recuperado de https://www.cfainstitute.org/en/advocacy/issues/dark-pools

CFTC, S., & SEC, U. (2010). Findings regarding the market events of may 6, 2010. *Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues*, 104. Recuperado de https://cutt.ly/ttDneUF

Chaboud, A. P., Chiquoine, B., Hjalmarsson, E., & Vega, C. (2014). Rise of the machines: Algorithmic trading in the foreign exchange market. *The Journal of Finance*, *69*(5), 2045-2084.

Chen, J. (2019). Block Trade. *Investopedia.* Recupeado de https://cutt.ly/7t1BZ5Z

Chen, P., Ibbotson, R. G., & Zhu, K. X. (2011). The ABCs of hedge funds: Alphas, betas, and costs. *Financial Analysts Journal*, *67*(1), 15-25.

Cheng, C., Kung, H. T., & Tan, K. S. (2002). Use of spectral analysis in defense against DoS attacks. *IEEE GLOBECOM 2002, Dec.*, *3*(3), 2143-2148.

Congresional Research service. (2016). High frequency trading: Overview of recent developments. (Vol. 4). Recuperado de https://cutt.ly/etA343C

Coppin, B. (2004). *Artificial intelligence illuminated*. Sadbury, Massachusetts: Jones and Bartlett Publishers

Cordeschi, R. (2002). *The discovery of the artificial: Behavior, mind and machines before and beyond cybernetics* (Vol. 28). Dordrecht, Paises Bajos: Springer Science & Business Media.

Cruz, N. (2004). *Sistema inmune artificial para solucionar problemas de optimización* (Tésis doctoral) Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, México DF, Mexico.

Dasgupta, D., Ji, Z., & Gonzalez, F. (2003). Artificial immune system (AIS) research in the last five years. In *The 2003 Congress on Evolutionary Computation, 2003. CEC'03.* (Vol. 1, pp. 123-130). Piscataway, Estados Unidos: IEEE.

De Barrón, I. (14 de mayo de 2019). El Santander propone a los sindicatos 3.713 despidos y el cierre de una de cada cuatro oficinas en España. *El País*. Recuperado de https://elpais.com/economia/2019/05/14/actualidad/1557839461_264862.html

De Prado, M. M. L., Easley, D., & O'Hara, M. (2011). The microstructure of the "flash crash": flow toxicity, liquidity crashes, and the probability of informed trading. *The Journal of Portfolio Management*, *37*(2), 118-128.

Deloitte. (2016) The expansion of Robo-Advisory in Wealth Management. Recuperado de https://cutt.ly/4tF9IrH

Diaz, N. E., Luna, L. J., Gomez, W. A, & Bautista, L. X. (2013). Algoritmo Inmune de Selección Clonal para el problema de Job Shop Scheduling. En *IV Congreso Internacional de Computación e Informática*.

Dickson, S. (28 de marzo de 2019). JPMorgan, Nomura job cuts add to wave of pullbacks in finance. *Bloomberg*. Recuperado de https://www.bloomberg.com/news/articles/2019-03-28/jpmorgan-nomura-job-cuts-add-to-wave-of-finance-firms-chopping

Domowitz, I., & Yegerman, H. (2005). The cost of algorithmic trading: A first look at comparative performance. *The Journal of Trading*, *1*(1), 33-42.

Europol (2018). Mastermind behind eur 1 billion cyber bank robbery arrested in Sapin. *Europol*. Recuperado de https://cutt.ly/rt71x3l

Europol. (2019). *Internet organised crime threats assessment*. Recuperado de https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The journal of Finance*, *25*(2), 383-417.

Fee Schedule. (2020). *Robin Hood*. Recuperado de https://robinhood.com/us/en/

Feigenbaum, E. A. (1981). Expert systems in the 1980s. *State of the art report on machine intelligence.* Stanford, Estados Unidos: Stanford University.

Fein, M. L. (2015). Robo-advisors: A closer look. *Social Science Research Network.* Recuperado de https://cutt.ly/KtF4cPw

Frankenfield, J. (28 de marzo de 2020). What is a Robo Advisor? Recuperado de https://cutt.ly/utFiReV

Gabinete de Coordinación y Estudios, Secretaría de Estado de Seguridad. (2018) *Estudios sobre la cibercriminalidad en España* (126-19-018-9). Recuperado de https://cutt.ly/gtDYwwQ

Gang, Y. (2020). The Freedom Dividen, Defined. *Yang 2020* Recuperado de https://www.yang2020.com/what-is-freedom-dividend-faq/

García, L. (12 de mayo de 1997). El hombre se rinde ante la máquina. *El País*. Recuperado de https://elpais.com/diario/1997/05/12/deportes/863388037_850215.html

García, L. J., Maestre, J. & Sandoval, A. L.(2015). Sistema Inmunitario Adaptativo para la mitigación de ataques de Denegación de Servicio. En *Actas de las primeras Jornadas*

Nacionales de Investigación en Ciberseguridad: León, 14, 15, 16 de septiembre de 2015: I JNIC2015 (pp. 26-31) León, España: Universidad de León.

Goldman, D. (28 de septiembre de2012). Major banks hit with biggest cyberattacks in history. *CNN*. Recuperado de https://cutt.ly/ot7NJi8

González, L. J. (s.f) Sistemas Inmunitarios Artificiales: Teoria Basica y Aplicaciones. Recuperado de https://cutt.ly/qtD1kxK

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

Grant, .J, Grene, S., & Preece, R. (s.f). Definition of dark pools, the purpose of dark pools. Financial Times. Recuperado de http://markets.ft.com/research/Lexicon/Term?term=dark-pools

Hasbrouck, J., & Saar, G. (2013). Low-latency trading. *Journal of Financial Markets*, *16*(4), 646-679.

Hendershott, T., & Riordan, R. (2009). Algorithmic trading and information .*NET institute* working paper no. 09-08. Obtenido de https://cutt.ly/5tAIKKx

Hendershott, T., Jones, C. M., & Menkveld, A. J. (2011). Does algorithmic trading improve liquidity?. *The Journal of finance*, *66*(1), 1-33.

Herrera, J. C. (2011). *Sistema inmune artificial con población reducida para optimización numérica* (Tésis doctoral). Instituto Politécnico Nacional, México D.F., Mexico.

Hidalgo, M. (2020). Machine learning. Así funciona la tecnología que hace posibles los "deepfakes". *El País*. Recuperado de https://retina.elpais.com/retina/2020/03/12/innovacion/1584007649_777029.html

Hillis, D., McCarthy, J., Mitchell, T. M., Mueller, E. T., Riecken, D., Sloman, A., & Winston, P. H. (2007). In honor of Marvin Minsky's contributions on his 80th birthday. *AI Magazine*, *28*(4), 103-103.

Hurtado, R. (s.f.) Hedge Funds. *El Economista*. Recuperado de https://cutt.ly/Mt2wDi4

Husillo Vidic (s.f.) Banca de reserva fraccionaria. *Economipedia*. Recuperado de https://cutt.ly/Ft7vAlJ

Igartua, M. (13 de marzo de 2020). El Ibex firma su mayor caída semanal (-20.85) desde Lehman Brothers. El Confidencial. Recuperado de https://cutt.ly/ytFrGsZ

Initio (2019). How will Robo-Advisors reshape Asset Management. Recuperado de https://cutt.ly/StGyL3c

Jaishankar, K. (2008). Identity related crime in the cyberspace: Examining phishing and its impact. *International Journal of Cyber Criminology*, *2*(1), 10.

Jegadeesh, N., & Titman, S. (1993). Returns to buying winners and selling losers: Implications for stock market efficiency. *The Journal of finance*, *48*(1), 65-91.

Jones, C. (22 de octubre 2019). Tesla´s Musk Is Overpromising Again On Self Driving Cars. *Forbes*. Recuperado de https://www.forbes.com/sites/chuckjones/2019/10/22/teslas-musk-is-overpromising-again-on-self-driving-cars/#1f7507415e98

Kaya,O. (2016). High-frequency trading. *Reaching the limits, Automated trader magazine*, *41*, 23-27.

Keynes, J. M. (1930). Economic possibilities for our grandchildren. En *Essays in persuasion* (pp. 321-332). Londres, Inglaterra: Palgrave Macmillan, London.

Khajuria, A., & Srivastava, R. (2013). Analysis of the ddos defense strategies in cloud computing. *international journal of enhanced research in management & computer applications*, *2*(2).

Koh, F., & Phoon, K. (2017). Robo-advisors and wealth management. *The Journal of Alternative Investments*, *20*(3), 79-94.

Lam, J. W. (2016). Robo-advisors: A portfolio management perspective.(Trabajo de fin de grado) *Yale College*, New Haven, Estados Unidos

Lee, D. (29 de mayo de 2015). Bureau 121: How Good are Kim Jong-un´s elite hackers?. *BBC*. Recuperado de https://www.bbc.com/news/technology-32925503

Linda, O., Manic, M., & Vollmer, T. (2009). Neural network based intrusion detection system for critical infrastructures. En *Proceedings of the 2009 international joint conference on Neural Networks* (pp.1827.1834). Piscataway, Estados Unidos: IEEE.

Llinares, F. M. (2013). La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing. *Revista electrónica de ciencia penal y criminología*, (15), 12.

Longuet-Higgins, H. C. (1991). Renaissance man. *Nature*, *350*(6318), 531-532.

Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security*, *16*(4), 195-202.

Luque, V. A., & Luque, M. A. (2014). A vueltas con la SICAV. Reflexiones críticas desde el punto de vista económico-tributario. *Papeles de Europa*, *27*(2), 1-17.

Mackenzie, M. (28 de julio de 2009). High-frequency trading under scrutiny. *Financial Times*. Recuperado de https://www.ft.com/content/d5fa0660-7b95-11de-9772-00144feabdc0

Madhok, E., Gupta, A., & Grover, N. (2016). Artificial Intelligence Impact on Cyber Security. *IITM Journal of Management and IT*, *7*(1), 100-107.

Mandes, A. (2016). Algorithmic and high-frequency trading strategies: A literature review. *Working Paper*. Recuperado de https://www.econstor.eu/handle/10419/144690

Martín, P. (2018). Los grandes vendedores de CFD revelan que hasta el 86% de sus clientes pierde dinero. Cinco días, El País. Recuperado de https://cutt.ly/jtFu0EA

McCarthy, J. (1978). History of LISP. En *History of programming languages* (pp. 173-185). Nueva York, Estados Unidos: Academic Press

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955. *AI magazine*, *27*(4), 12-12.

McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *The bulletin of mathematical biophysics*, *5*(4), 115-133.

Metlich, P. (2012). Método de Resolución de Robinson. [Diapositiva de Prezi]. Recuperado de https://cutt.ly/0t1H74l

Montoya, A. (2018). *Robo Advisors: la evolución en la forma de invertir en el mercado de capitales* (Tesis de Máster). Universidad EAFIT, Medellín, Colombia.

Morgan, S. (6 de febrero de 2020). 2019 Cybersecurity Almanac: 100 facts, Figures, Predictions and Statistics. *Cybersecurity Ventures*. Recuperado de https://cutt.ly/ZtDUj5j

Murawski, R. (2006). The Present State of Mechanized Deduction, and the Present Knowledge of Its Limitations., *Studies in Logic, Grammar, and Rhetoric*, *22*(9), 31-60.

National Research Council (US). Automatic Language Processing Advisory Committee. (1966). *Language and machines: computers in translation and linguistics; a report* (Vol. 1416). Recuperado de https://cutt.ly/XtAfr7r

Newell, A., Shaw, J. C., Simon, H. A. (1959*). A variety of intelligent learning in a general problem solver*. Santa Mónica, Estados Unidos: The Rand Corporation

Nilsson, N. J. (2009). *The quest for artificial intelligence*. Cambridge, Inglaterra: Cambridge University Press.

Niveles de conducción autónoma. (s.f). Toyota. Recuperado de https://cutt.ly/Rt6kAI9

Osbourne, H. (29 de enero de 2016). HSBC suffers online banking cyber-attack. *The Guardian*. *The Guardian*. Recuperado de https://cutt.ly/8t7BNOs

Panda, T. C., Rao, Y. S., & Saini, H. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.

Perlroth, N. (3 de octubre de 2017). All 3 Billion Yahoo Accounts Were Affected by 2013 Attack. *New York Times*. Recuperado de https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Pinilla, Ávila, E. G. (2018) Modelo de un sistema inmunológico artificial basado en la teoría de la continuidad de Thomas Pradeu (Tesis de maestría). Universidad Distrital Francisco José de Caldas, Bogotá Colombia.

Pospíchal, J., y Kvasnička, V. (2015). 70th anniversary of publication: Warren McCulloch & Walter Pitts-a logical calculus of the ideas immanent in nervous activity.

En *Emergent Trends in Robotics and Intelligent Systems* (pp. 1-10). Nueva York, Estados Unidos: Springer International.

Prada, I. F. (2015). Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. *Revista Electrónica de Ciencia Penal y Criminología*, *17*, 21.

Price Water House Coopers. (2017). Robo Advisory moves forward in Italy. Recuperado de https://cutt.ly/htF9HFc

Prodanova, J., San Martín, S., & Torres, N. H. J. (2015). El presente y el futuro de la banca por móvil según los usuarios espanoles de banca. *Universia Business Review*, (46), 94-117.

¿Qué son las Sicavs?. (25 del junio de 2014). *El Mundo*. Recuperado de https://cutt.ly/PtF0xpO

Ramón, E. (12 de junio de 2019). Un total de 2971 trabajadores solicitan adherirse al ERE de CaixaBank. *Expansión*. Recuperado de https://www.expansion.com/empresas/banca/2019/06/11/5cffead7e5fdeadb2f8b456d.html

Real Decreto 1464/2018, de 21 de diciembre, por el que se desarrollan el texto refundido de la Ley del Mercado de Valores. BOE núm 313. Recuperado el 6 de abril de 2020 de: https://www.boe.es/buscar/act.php?id=BOE-A-2018-17879&p=20181228&tn=3

Reinicke, C. (25 de septiembre 2019). Los bancos acumulan casi 60.000 despidos en 2019 y el gigante alemán Commerzbank prepara la nueva ola de recortes. *Business Insider*. Recuperado de https://www.businessinsider.es/bancos-registran-casi-60000-despidos-2019-todavia-hay-498783

Rubio, J. (2014). Guía para luchar contra tu cerebro: los sesgos cognitivos. *El País: Verne*. Recuperado de https://cutt.ly/9t15mDR

Russell Stuart, J., & Norvig, P. (2009). *Artificial intelligence: a modern approach*. Nueva Jersey, Estados Unidos: Prentice Hall.

Salas, R. (2004). Redes neuronales artificiales. *Universidad de Valparaíso. Departamento de Computación*, *1*.

Sánchez, C. (14 de agosto de 2017). Hablamos con el padre de Roomba: así logró vender 18 millones de aspiradoras robóticas. *El Confidencial*. Recuperado de https://www.elconfidencial.com/tecnologia/2017-08-13/padre-roomba-robot-espia-aspirador_1428064/

Secure societies. (s.f.) *Comisión Europea*. Recuperado de https://cutt.ly/XtDOx7A

Securities, U. S. Exchange Commission (SECC).(2014). *Equity market structure literature review: Part II: High frequency trading.* Recuperado de https://www.sec.gov/marketstructure/research/hft_lit_review_march_2014.pdf

Sevilla, A. (s.f.). Contrato por diferencia. Economipedia. Recuperado de https://cutt.ly/5tFtsKz

Skrycky, M. (10 de febrero de 2018). Bankia y los sindicatos alcanzan un acuerdo sobre el ERE que supondrá 2.000 bajas. *Expansión*. Recuperado de https://www.expansion.com/empresas/banca/2018/02/10/5a7eaff722601d197a8b4649.html

Soros, G. (1994). *The Alchemy of Finance: Reading the Mind of the Market.* Nueva Jersey, Estado Unidos: John Wiley & Sons.

Statista. (2019). Personal Finance Report 2019. Recuperado de https://cutt.ly/0tF1AEU

Symantec Corporation (2012). *Ransomware: A growing menace.* Recuperado de https://cutt.ly/DtDDGtF

Turing, A. M. (1950). Computing machinery and intelligence. En *Parsing the Turing Test* (pp. 23-65). Dordrcht, Paises Bajos: Springer, Dordrecht.

Tyugu, E. (2011, June). Artificial intelligence in cyber defense. En *2011 3rd International Conference on Cyber Conflict* (pp. 1-11). Piscataway, Estados Unidos: IEEE.

Valero, C. (7 de julio de 2019). Deutsche Bank eliminará 18.000 puestos de trabajo, un quino de la plantilla. *El Mundo*. Recuperado de https://www.elmundo.es/economia/empresas/2019/07/07/5d2229abfc6c834b278b4619.html

Veloso, M. (16 de marzo de 2020). La CNMV prohíbe las posiciones cortas en la Bolsa después de que el Ibex haya perdido un 40% en 18 días. ABC. Recuperado de https://cutt.ly/RtFr2l6

Villalba, D. (2016). *Teoría y práctica de la gestión de carteras,* Madrid, España: Bolsa y Mercados Españoles.

What is Horizon 2020. *Comisión Europea*. Recuperado de https://ec.europa.eu/programmes/horizon2020/what-horizon-2020