Universidad Rey Juan Carlos

E.T.S. Ingeniería de Telecomunicación

DEONTOLOGIA Y NORMATIVA EN ROBOTICA

IA en seguridad bancaria

Autor:
Javier Izquierdo Hernández

17 de abril de 2023

Contenidos

Índice de figuras

1 Introducción

La inteligencia artificial cada vez tiene un uso más habitual en la sociedad, y esto se refleja en la incorporación de esta tecnología en otros ámbitos. En este trabajo vamos a indagar más en profundidad en el uso de IA en la banca por motivos de seguridad y en la prevención de fraudes y estafas. También vamos a tratar el otro lado del espectro con las prácticas que conllevan al fraude y estafas usando la inteligencia artificial.

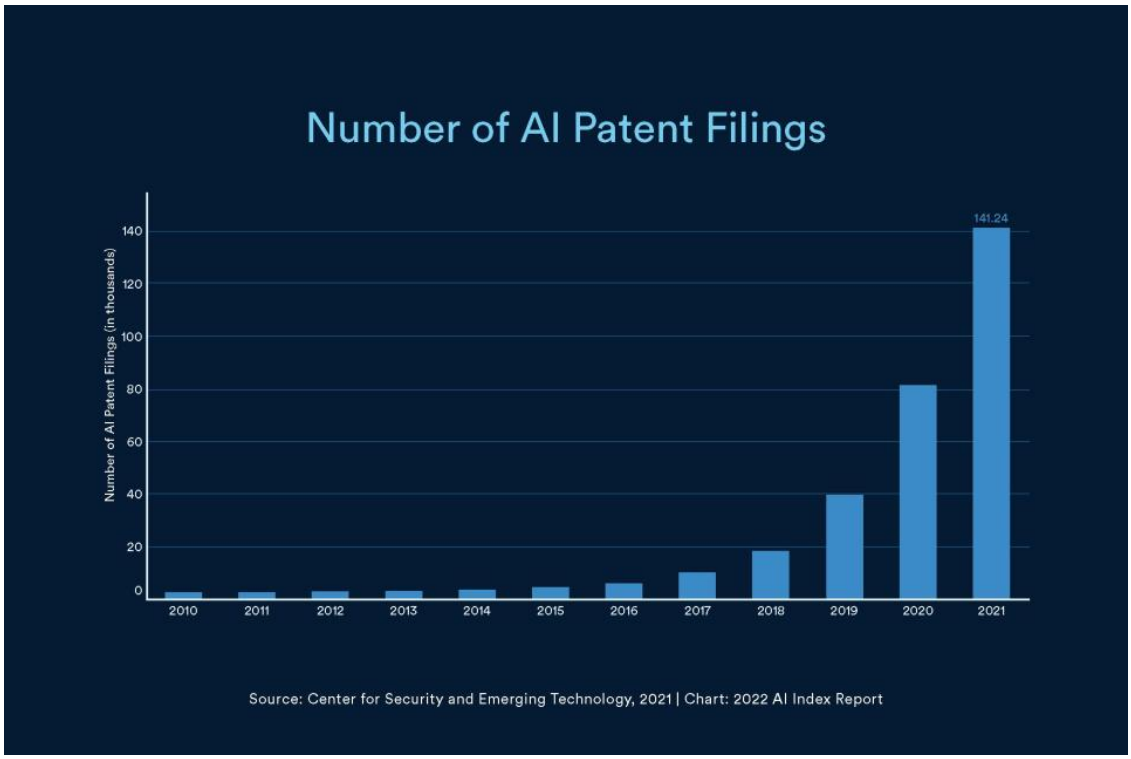


Figura 1.1: Número de patentes de IA en la última década

2 Uso de la IA en la banca

En la sector bancario se empezó a usar la inteligencia artificial hace unos 5 años aproximadamente, por lo que todavía se encuentra en la fase de desarrollo en muchos bancos.
Los usos más principales y donde se hallan los mayores beneficios se pueden dividir en tres partes:

1. *Front office*
2. *Middle office*
3. *Back office*

La primera parte se encarga del trato con los clientes. Su uso es para intentar solucionar los problemas y necesidades de los clientes de forma autónoma de forma que el cliente quede lo más satisfecho posible, esto se llama *conversational banking*. Véase 2.1.

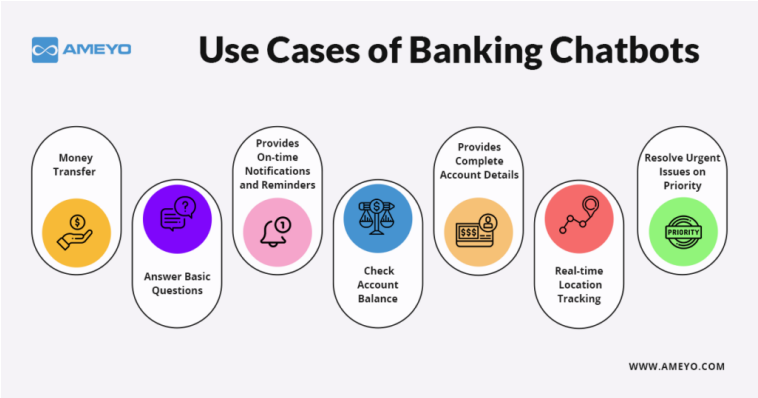


Figura 2.1: Usos de asistentes en las aplicaciones bancarias

En la siguiente parte ó *middle office* se usa la inteligencia artificial con el fin de reducir el riesgo de fraude y para manejar otros peligros. Esta parte la veremos en

más detalle más adelante.

Y por último en *back office* se usa para *underwritting*[1]. A esta parte no entramos más en detalle ya que no se encuentra en el ámbito de este trabajo.

Todas estas medidas son tomadas por algunos de los bancos más importantes a nivel mundial, como por ejemplo los mencionados en [3]: Capital One, Citi, HSBC, JPMorgan Chase, Personetics, Quantexa y U.S. Bank.

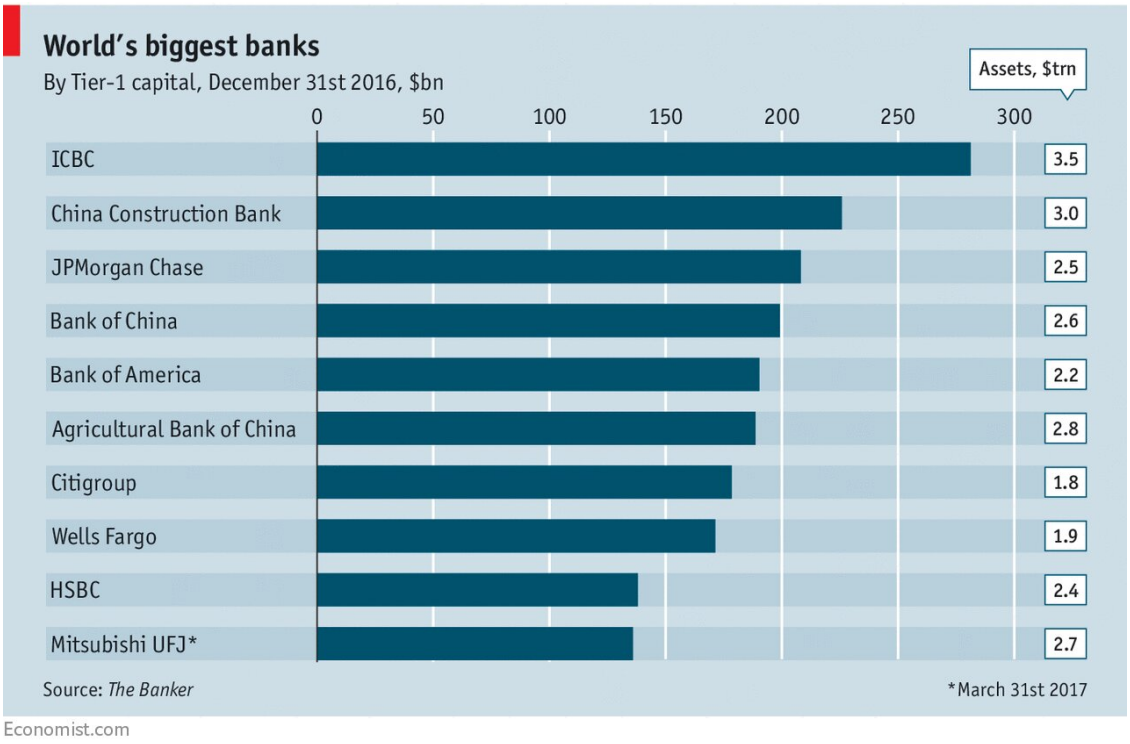


Figura 2.2: Bancos con mayor capital 2016

[1]Underwriting (cobertura, suscripción de seguro, aseguramiento; dado y aceptado en general después de evaluar riesgos) es el contrato celebrado entre una entidad financiera y una sociedad comercial, por medio del cual la primera se obliga a prefinanciar, en firme o no, títulos valores emitidos por la sociedad, para su posterior colocación. Su existencia se debe a la necesidad de las empresas de obtener recursos financieros y en la actualidad su utilización es cada vez más constante.
Si bien el contrato de Underwriting se caracteriza por la prefinanciación de los títulos valores, es también parte de la esencia del contrato la prestación de un servicio de asesoramiento previo a la decisión de emitir los títulos. De [5]

3 *Middle office*: control de riesgos

Los bancos en esta era digital se enfrentan a varias amenazas o riesgos de forma directa o indirecta.

Los riesgos directos son aquellos en los que la propia entidad bancaria sufre perdidas de nivel económico o de reputación. Estos pueden ser:

1. Crédito: dar dinero sin saber si este va a ser devuelto. En grandes cantidades esto puede causar a la entidad bancaria a incurrir en una deuda mayor.

2. Operacionales: errores en las operaciones bancarias pueden causar una brecha en la seguridad o una interrupción del servicio de la entidad.

3. Mercado: crisis o inestabilidad en Íla economía global causadas por diferentes causas pueden causar un gran detrimento a la entidad o incluso su disolución. Por ejemplo la crisis del 2008, causo una gran cantidad de perdidas a entidades bancarias y el cierre de varias como Lehman Brothers que causo el estallido de esta.

4. Liquidez: el banco no puede dar el dinero a sus usuarios de forma inmediata, o a corto plazo.

5. Ciberseguridad: ataques informáticos con el fin de obtener información sobre el banco y sus usuarios pueden causar una gran pérdida a nivel económico y de reputación, además de un severo problema para sus usuarios que pueden ver sus ahorros desvanecerse.

6. Reputación: puede ser causado por cualquiera de estos problemas, ya que estos causan descontento a los usuarios. También puede ser causados por una baja satisfacción de los usuarios debido a una mala interacción con ellos por ejemplo en las aplicaciones de banca online.

7. Negocio: si un banco no se adecúa a la era actual puede causarle la perdida de usuarios.

8. Legislativo: si no se adapta a las leyes, esto puede causarle problemas legales que conllevan la perdida de reputación y pueden llegar a causar la disolución de la entidad por incumplimiento de estas leyes.

En estos tipos de riesgos, la inteligencia artificial tiene un factor primordial en multitud de ellos, tales como los: operacionales, de mercado, ciberseguridad, reputación y negocio.

Ahora entraremos en detalle en cada uno de ellos para explicar el uso de la IA:

3.1. Riesgos Operacionales

La inteligencia artificial se puede usar con el fin de identificar brechas en el servicio antes de que los humanos puedan percatarse y repararlas antes de que puedan causar un daño mayor.

3.2. Riesgos de mercados

En este ámbito el uso dado a las IA es el de la especulación del estado del mercado global con el fin de poder anticiparse ante las posibles crisis económicas y así sufrir un menor impacto.
También es usada para decidir cuales operaciones de capital le dará un mayor beneficio, así como cuales inversiones son más rentables.

3.3. Ciberseguridad

Al incrementar los ataques informáticos de manera exponencial en los últimos años 3.1, una de las maneras más eficientes de protegerse de ellos es usando la inteligencia artificial para la detección y detención de estos. Las IA se pueden usar de diferentes formas como por ejemplo la explicada en el paper [6] o en [7]

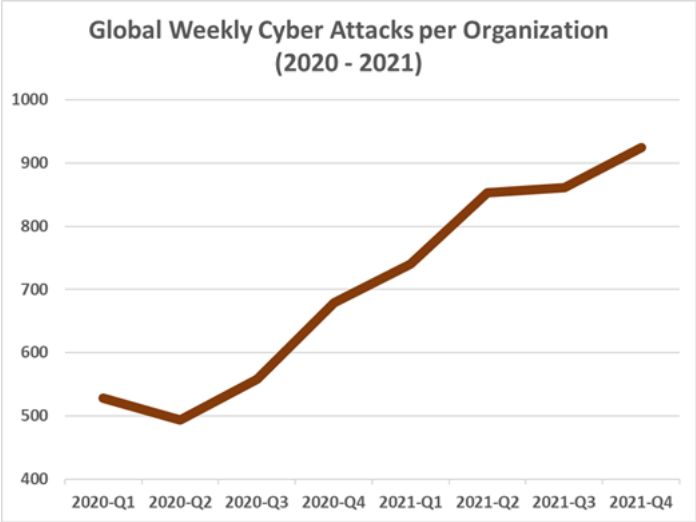


Figura 3.1: Ciberataques por semana a organizaciones 2020-2021

3.4. Reputación

Esta parte también incluye la parte de *front office* con las aplicaciones de la IA siendo por ejemplo los asistentes virtuales en las aplicaciones de banca online.

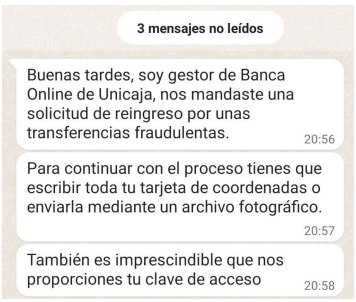
3.5. Negocio

Este parte incluye todas la anteriores. Por ejemplo si un banco no introduce la IA para detener ciberataques, no será capaz de proteger su información por lo que los clientes se irán. Otro sería si no implementan los asistentes virtuales o si no usan la IA para buscar las inversiones más rentables, tendrán un mayor riesgo de perder dinero y reputación.

4 *Middle office*: detección de fraudes

El fraude es un tipo de riesgo que afecta de forma indirecta a los bancos, pero de forma directa a los usuarios de estos.
Las entidades bancarias deciden ayudar a los usuarios a identificar estos fraudes para que ellos se sientan más seguros en depositar su dinero en ellos, en vez de tenerlo guardado en efectivo.

Estos fraudes normalmente se basan en un mensaje de teléfono (SMS), en un correo electrónico o en redes sociales en el que se hacen pasar por las entidades bancarias y piden al desconcertado usuario que se dirija a una página web aparentemente de su banco para rellenar unos datos "*necesarios*"para solventar algún tipo de problema en su cuenta. Posteriormente el estafador procede a extraer el dinero de la cuenta del usuario hasta que esta se encuentra vacía, y pasa a la siguiente víctima. Véase 4.1.



(a) Estafa Whatsapp

(b) Estafa cuenta suspendida SMS

Figura 4.1: Diferente tipo de estafas y fraudes bancarios

Viendo este tipo de estafa, los usos que se le podrían dar y se le dan a la IA varían en varios ámbitos:

- En los sistemas de mensajería y SMS se usa para diferenciar los mensajes reales de las entidades bancarias de los mensajes fraudulentos.
- En las redes sociales al igual que mencionado anteriormente y además para cerrar esas cuentas e identificar a su creador.
- En la parte de los bancos una aplicación sería el distinguir las operaciones normales del usuario de las operaciones que haga el estafador, ya sean estas la ip extraña, la velocidad del fin de la transacción desde el inicio de la misma, o el orden de introducción de los campos, etc...

El problema que presenta la inteligencia artificial en este caso, es que al igual que se esta usando para intentar impedir estos fraudes, también se esta usando para llevarlos a cabo de manera más convincente y de forma más masiva. Con lo que en este punto se puede considerar como un guerra entre las IA *buenas* que intentan defender al usuario de este tipo de estafas y las IA *malas* que atacan al usuario, decidiéndose esta guerra en cual de las dos IA esta más avanzadas. Para más información sobre esto véase `https://www.logicloop.com/fraud-risk/how-fraudsters-can-use-artificial-intelligence-and-chatgpt-to-scam`.

También todo esto se podría solucionar con una mayor educación digital a la población para evitar este tipo de fraudes, al menos por ahora.

5 Conclusión

Ahora mismo estamos en un *boom* del desarrollo de la IA y lo que ahora nos parece imposible dentro de unos meses o años la inteligencia artificial será capaz de ello.

Por esto mismo el desarrollo de la IA en el campo de las finanzas y del los bancos tendrá que ser consecuente con el desarrollo global, ya que cuanto más avance la inteligencia artificial, más difícil será de protegerse de los ataques informáticos que usen a la misma, lo que obligará a todas estas empresas a protegerse usando la IA con ese fin.

A su vez con el intento de desarrollo de AGI (*artificial general intelligence*), no se sabe donde estará el techo de los asistentes virtuales que se usan actualmente en las aplicaciones bancarias y mucho más que nos deparan los próximos años, si estas IAs no son prohibidas por los gobiernos del globo, véase [9].

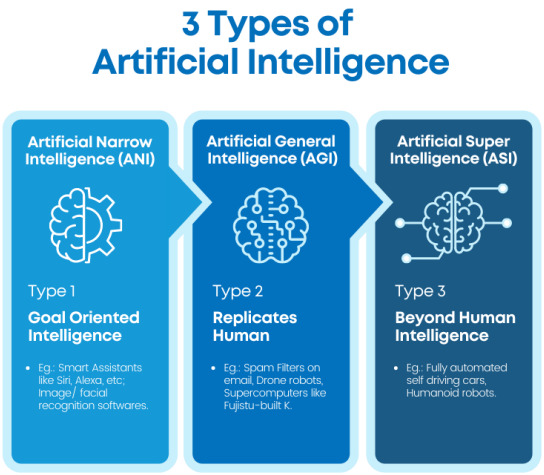


Figura 5.1: Tipos de IA

Bibliografía

[1] https://www.insiderintelligence.com/insights/ai-in-finance/

[2] https://hai.stanford.edu/news/state-ai-9-charts

[3] https://www.businessinsider.com/ai-in-banking-report

[4] https://www.inscribe.ai/financial-risk-management/how-banks-manage-risks#:~:text=Banks%20develop%20risk%20management%20programs,prevent%20them%20from%20re-emerging.

[5] https://es.wikipedia.org/wiki/Underwriting#:~:text=Underwriting%20(cobertura%2C%20suscripcin%20de%20seguro,por%20la%20sociedad%2C%20para%20su

[6] https://www.datarobot.com/resources/ai-in-cybersecurity/

[7] https://www.ibm.com/security/artificial-intelligence

[8] https://www.logicloop.com/fraud-risk/how-fraudsters-can-use-artificial-intelligence-and-chatgpt-to-scam

[9] https://www.reuters.com/technology/germany-principle-could-block-chat-gpt-if-needed-data-protection-chief-2023-04-03/