Universidad de
SanAndrés

Universidad de San Andrés

Escuela de Negocios

Licenciatura en Administración de Empresas y Contador Público

EL USO DEL DEEP LEARNING COMO HERRAMIENTA PARA LA DETECCIÓN DEL FRAUDE CORPORATIVO

Autor: María Victoria Orlandi

Legajo: 30255

Mentor: Pablo Sciolla

Buenos Aires
2022

RESUMEN

El fraude es una práctica delictiva que afecta a todas las organizaciones. Sus consecuencias son tan importantes que hasta pueden generar la quiebra de una compañía. Este es el motivo por el que resulta importante analizar nuevos mecanismos para que su detección sea más eficiente. Es por esto que el presente trabajo de investigación tiene como objeto de estudio indagar en una herramienta particular para su identificación: el *deep learning*. Para esto, se investigó sobre cuáles son las técnicas que se utilizan en la actualidad y los beneficios y limitaciones que presenta esta rama de la inteligencia artificial. Finalmente, se alcanzaron diferentes conclusiones vinculadas al *big data*, *real time*, los datos no estructurados, entre otros, que permiten afirmar que es eficiente para esta tarea.

Palabras claves: inteligencia artificial; deep learning; fraude corporativo; datos estructurados; datos no estructurados; auditoría interna; auditoría externa; equipos de fraude.

ÍNDICE

Agradezco a mi Prof. Pablo Sciolla por dirigir mi investigación, motivarme a asumir una actitud interrogativa y por incentivarme a combinar aprendizajes de mis carreras con las nuevas tendencias tecnológicas.

Gracias a los profesores entrevistados por su esfuerzo y tiempo empleado en ayudarme en la realización de este trabajo.

También me gustaría agradecer a mi familia y amigos que me acompañaron durante mi formación académica.

1. Introducción

La honestidad en el ámbito de trabajo debería ser una buena práctica replicada en todas las organizaciones. Sin embargo, el *fraude corporativo* se constituye como un riesgo inherente a estas, independientemente de la industria en que se encuentre. Esto quiere decir que ninguna empresa se salva de estas prácticas criminales. Eventualmente, alguien dentro de la compañía, realizará acciones tendientes a beneficiarse a costa de la firma.

Las consecuencias derivadas del fraude tienen un impacto generalizado, en otras palabras, “no solo se perjudica la imagen y confianza tanto de la empresa como de sus gestores, sino también de los inversores y hasta equipos y socios comerciales” (Gutiérrez, 2020, p. 2). Pensemos en uno de los escándalos más importantes de principios de siglo: el caso Enron. El objetivo principal de los dirigentes de esta empresa era convertirse en la mejor compañía del mundo. Para esto, desarrollaron una serie de actividades e inversiones que le generaron muchos ingresos. No obstante, “el balance de Enron, por sí solo, no era lo suficientemente amplio como para poder hacer soporte al impresionante crecimiento que la empresa estaba experimentando” (Bavo, 2015, p. 15), motivo por el cual, comenzaron a utilizar maniobras para eliminar la mayor cantidad de deuda posible de sus cuentas, creando una estructura financiera muy compleja (Bravo, 2015).

Cuando se descubren estas prácticas, las acciones de la compañía se desploman afectando no solo a los inversores, sino que también a todas las personas de Estados Unidos que habían aportado a planes de jubilación que mantenían el valor del dinero invirtiendo en compañías rentables, como parecía ser Enron (Blackburn, 2002, p. 31) . En consecuencia, cuando el valor de las acciones cae, también lo hacen esos fondos. Este ejemplo muestra que el fraude también tiene un impacto social. Por lo tanto, vemos que, si bien es solo

orquestado por miembros de la compañía, sus efectos repercuten tanto en sujetos internos como ajenos a la empresa. Es por esto que indagar en mecanismos que permitan su temprana detección es importante, no solo para disminuir las pérdidas monetarias generadas por estas prácticas, sino también para atenuar las externalidades negativas que generan en la sociedad.

Pensar en la materialización de los riesgos y en formas de mitigarlos es lo que me motiva a estudiar el objeto de mi tesis. Este se centra en analizar si el *deep learning* es una herramienta que permite la detección del fraude corporativo. Para esto, en una primera instancia se realiza un planteo de la problemática teniendo en consideración los análisis de diferentes autores sobre estos temas. Luego, se presentan las preguntas y subpreguntas de investigación, junto con los objetivos que se esperan lograr. A continuación, en el marco teórico se exponen conceptos claves para comprender el desarrollo de la presente tesis.

Una vez alcanzado el cuerpo del escrito, nos encontraremos con dos partes: en una primera parte, se hace mención a las formas en que distintas áreas de la compañía y agentes externos a ella detectan el fraude en la actualidad. En la segunda parte, se explica cómo puede ser detectado por medio del *deep learning* junto a sus beneficios. Finalmente, se exhibe un apartado con las conclusiones derivadas de todo lo estudiado, que pretenden ser una excusa para provocar nuevas lecturas e intervenciones a la hora de detectar fraude en las corporaciones.

1.1 Planteo de la problemática

El *fraude corporativo* (o fraude empresarial) es una problemática a nivel mundial. Según lo publicado en *Report to the Nations* (ACFE, 2022), el cinco por ciento de los ingresos de las compañías se pierden producto de esta práctica. Esto repercute no solo a nivel económico, sino también en la reputación de las compañías. En palabras de Karpoff, Lee y Martin, las pérdidas como consecuencia de la mala reputación construida suelen ser 7,5 veces mayor a las penalidades impuestas por sistemas legales y regulatorios

(2008, p. 582). Algunas historias emblemáticas se constituyen en buenos ejemplos: *Enron*, *Arthur Andersen*, *Wirecard*, *Xerox*, han mostrado que el fraude se puede manifestar de diferentes maneras pero que, si no es detectado a tiempo, las consecuencias suelen derivar en la quiebra de la empresa.

Adicionalmente, el *fraude corporativo* puede dividirse en tres secciones: corrupción, apropiación indebida de activos y alteración de los estados financieros. El primero de ellos incluye los casos de sobornos, conflictos de intereses y extorsión. Al mencionar la apropiación indebida de activos, hacemos referencia a siniestros ocasionados por empleados vinculados al robo y mal uso de los recursos de la compañía. Mientras que la alteración en los Estados Financieros implica omisiones o incorrecciones en los Estados Contables de manera intencional (ACFE, 2022).

Ahora bien, diversos autores sostienen que estos tipos de fraude son muy complejos de detectar porque los protagonistas del acto delictivo crean o alteran documentos físicos o electrónicos (Dong, Lial, Zhang, 2018). En este sentido, cuando se analiza esta información intentando encontrar anomalías, no resulta ser muy efectivo porque los números son imaginarios (Kaminski, Wetzel, Guan, 2004*)*. Es por este motivo que la detección del *fraude corporativo* no pasa solo por los datos estructurados (como variables numéricas financieras, ratios, descripciones cuantitativas de las operaciones), sino que también por los datos no estructurados (como discusiones del management, conferencias, videos de cámaras de seguridad, sección MD&A (*management discussion and analysis*) de los Estados Financieros, reportes, mails, entre otros) (Dong, Lial, Zhang, 2018).

Una de las formas por la cual estos datos toman sentido y son utilizados como herramienta para la detección del *fraude corporativo* es por medio del *deep learning*. El *deep learning* forma parte de la inteligencia artificial y es un tipo particular de *machine learning*, el cual “utiliza redes neuronales, que se organizan en capas para reconocer relaciones y patrones complejos en los datos” (Rouhiainen, 2018, p. 18). Sus principales aplicaciones son dos: el

procesamiento del lenguaje natural y el reconocimiento de imágenes. El primero sirve para el análisis del texto y voz. Los autores Craja, Kim y Lessmann (2020) retoman estudios de investigadores en psicología social para explicar que las emociones y procesos cognitivos de los sujetos que intentan realizar actos fraudulentos se pueden manifestar en señales lingüísticas. Por lo tanto, es posible encontrar patrones en los discursos de los managers para detectar el fraude.

En el caso de David F. Larcker y Anastasia A. Zakolyukina (2012), se detienen a estudiar las conferencias de CEO y CFOs y explican que aquellos que pueden ser considerados como *liar* utilizan mayor referencia a conocimiento general, menor cantidad de emociones positivas, menos referencias al valor de la compañía y marcada utilización de emociones negativas. Siguiendo esta línea de análisis, los autores Tang y Karim (2019) comentan que es posible encontrar estos mismos patrones en las *brainstorming sessions*[1] realizadas por los auditores.

En segundo lugar, el *deep learning* se extiende en otra rama denominada reconocimiento de imágenes, que permite utilizar tanto fotos como videos para la detección del *fraude corporativo*. Por ejemplo, los autores Tang y Karim (2019) comentan que es posible combinar los videos de las cámaras de seguridad junto con los registros de inventarios físicos para identificar la existencia de un robo.

Sobre la base de lo detallado, se considera que investigar la implementación del *deep learning* como herramienta para la detección del fraude es relevante para la profesión contable. Este aporta elementos que permiten la detección temprana del *fraude corporativo* de las empresas, reduciendo, de este modo, las consecuencias negativas para las compañías que asesora. El tiempo que transcurre entre el suceso de fraude y su detección resulta clave para proteger los activos de las empresas. Según lo publicado en *Report to the Nations*

[1] Las Normas Internacionales de Auditoría obligan a los auditores a llevar adelante *brainstorming sessions* con el objetivo de discutir con los miembros de la empresa los casos potenciales de fraude y cómo responderían ante ellos.

(ACFE, 2022), en promedio, el tiempo que dura identificar un acto fraudulento es de doce meses y que, entre mayor tiempo pasa, aumentan las pérdidas financieras.

1.2 Preguntas y Subpreguntas de investigación

Pregunta principal

¿Qué aporta el *deep learning* como herramienta para la detección de *fraudes corporativos*?

Subpreguntas

- ¿Qué características del *deep learning* permiten detectar *fraudes corporativos*?
- ¿Por qué es posible que el *deep learning* logre una detección más eficiente del *fraude corporativo*?
- ¿Cuáles son las ventajas de utilización de datos no estructurados en complemento de los datos estructurados para la detección de *fraudes corporativos*?

1.3 Objetivos de la investigación

Objetivo principal

Identificar la importancia del uso del *deep learning* para detectar el *fraude corporativo*.

Objetivos específicos

- Reconocer los aportes del *deep learning* como herramienta de recuperación de datos no estructurados para la detección de anomalías.
- Estudiar las formas actuales de detección del fraude.
- Identificar los beneficios que aporta el *deep learning* para la detección de *fraudes corporativos*.

1.4 Justificaciones y razones del estudio

El *fraude corporativo* es una problemática a nivel mundial. Diferentes casos históricos han demostrado las consecuencias sociales y económicas, de imagen social y de legitimación empresarial que generan estas prácticas delictivas. Es por este motivo que como temática de la presente tesis se propone el estudio del *deep learning* como herramienta para la detección de fraudes en las corporaciones. Utilizar esta metodología resulta muy enriquecedor porque, a diferencia de las herramientas preventivas, las detectivas son aquellas que identifican el fraude una vez ocurrido y, como se explica en diferentes escritos, su temprana detección hace que las consecuencias negativas disminuyan.

Asimismo, considero como estudiante de las carreras de Contador Público y la Licenciatura en Administración de Empresas que es importante lograr conectar los conocimientos contables y del *management*, que forman parte del lenguaje de las empresas, con las nuevas tecnologías para así contribuir al entendimiento del fraude y su detección.

2. Marco teórico

Para abordar la temática propuesta en el presente trabajo de investigación, resulta necesario comprender, en primer lugar, qué es el *fraude corporativo* y cuáles son sus características principales. En segundo lugar, qué es el *deep learning* y su vinculación con el fraude. Luego, la diferencia entre datos estructurados y no estructurados. Adicionalmente, se agregan explicaciones sobre otros conceptos que serán utilizados a lo largo del escrito.

2.1 Fraude corporativo

Las Normas Internacionales de Auditoría (NIA) definen al fraude como “un acto intencionado realizado por una o más personas de la dirección, los responsables del gobierno de la entidad, los empleados o terceros, que conlleve la utilización del engaño con el fin de conseguir una ventaja injusta o ilegal” (2009, p. 139). Siguiendo esta línea de análisis, cuando se menciona al *fraude corporativo* se hace referencia a este acto intencional que tomará como protagonistas a sujetos que forman parte de la compañía (como directores, gerentes, empleados, entre otros). En cambio, otros tipos de fraude, como los cibernéticos, son llevados a cabo por agentes externos a la empresa quienes, en general, se aprovechan de los integrantes de ella para realizar el acto fraudulento.

Resulta importante destacar que el *fraude corporativo* se categoriza en: apropiación indebida de activos, corrupción y fraude en los estados financieros. La primera involucra a un empleado robando o haciendo una incorrecta utilización de los recursos de la compañía. Esta es la práctica más común pero la que menos pérdidas genera. Puede lograrse de diversas formas: malversación de ingresos, sustracción de existencias o de material de desecho

para uso personal, haciendo que una entidad pague por bienes o servicios que no ha recibido (como pago a proveedores ficticios), entre otros (NIA 240, p. 147).

La corrupción, como segunda categoría, incluye los casos de soborno, extorsión y conflictos de intereses (ACFE, 2022). El ejemplo más común es la coima.

Por último, el fraude en los estados financieros se refiere a las “incorrecciones intencionadas, incluidas omisiones de cantidades o de información en los estados financieros con la intención de engañar a los usuarios de estos” (NIA, 2019, p. 146). Esta es la de menor frecuencia, pero las pérdidas que genera quintuplica a las otras manifestaciones de fraude. Puede lograrse mediante: la manipulación, falsificación o alteración de registros contables o documentación respaldatoria, falseamiento de transacciones, aplicación errónea de principios contables, entre otros (NIA 240, p. 147).

Además, se menciona en esta norma y en el texto publicado por los autores Huang, Lin y Yen (2016), que los factores que explican que una persona cometa fraude se concentran en un modelo denominado *el triángulo del fraude*, creado por Donald R. Cressey en 1973 y cuyos elementos son: la motivación, la oportunidad percibida y la racionalización. El primero refiere a la causa o razón para cometer el acto, el que se constituye como consecuencia de alguna presión externa percibida por el sujeto. Por ejemplo, los autores mencionan que la presión ejercida por alcanzar las ganancias proyectadas crea la razón para cometer fraude. En la ISA 240 se enuncian diferentes elementos que generan una presión excesiva y que pueden desencadenar en la apropiación indebida de activos o en el fraude por información financiera fraudulenta:

- Ejemplos de presión que puede llevar a la apropiación indebida de activos:
    - Malas relaciones entre la entidad y los empleados que tienen acceso a activos susceptibles de ser sustraídos, como pueden

ser: futuros despidos conocidos o previsibles por los empleados, cambios en la remuneración incongruentes con sus expectativas.
    - Obligaciones financieras personales (como deudas).
- Ejemplo de presión que puede llevar al fraude en los estados financieros:
    - Expectativas irracionales de rentabilidad por parte de inversores o terceros.
    - Necesidad de obtener financiación adicional para seguir siendo competitivos.
    - Capacidad ilimitada para cumplir con los requerimientos asociados a la cotización en bolsa.
    - Efectos negativos de informar menos resultados.
    - Intereses financieros significativos en la entidad.
    - Una parte significativa de su retribución depende de alcanzar un objetivo desmesurado.

El segundo es la oportunidad percibida, entendida como la percepción de la existencia de un ambiente favorable para cometer fraude, como puede ser el caso de la falta o ineficiencias de controles internos en distintos procesos de la compañía. Nuevamente, la ISA 240 brinda diferentes ejemplos:

- Ejemplo de oportunidad que pueden llevar a la apropiación indebida de activos:
    - Manipulación de una sola persona de grandes cantidades de efectivo.
    - Activos comercializables que carecen de una identificación de titularidad.
    - Controles internos deficientes como la falta de segregación de funciones, el registro inadecuado de los activos, ausencia de documentación sobre transacciones.
- Ejemplo de oportunidad que pueden llevar al fraude en los estados financieros:
    - Transacciones significativas con partes vinculadas.
    - Utilización de estimaciones significativas.

- Transacciones realizadas en una fecha cercana al cierre del ejercicio.
- Existencia de cuentas bancarias u operaciones de una sociedad dependiente de una sucursal en jurisdicciones que sean paraísos fiscales.
- Inexistencia de supervisión por los responsables del gobierno de la entidad.
- Controles internos deficientes.

Finalmente, como tercer elemento se menciona la racionalización, que implica la justificación del hecho. Desde *Association of Certified Fraud Examiners* (ACFE) se explica que la gran mayoría de las personas que cometen el fraude no se consideran a sí mismos como criminales. Es por este motivo que buscan justificar sus actos delictivos de alguna manera, por ejemplo, manifestando que sus salarios son muy bajos para la tarea que realizan, que lo hicieron para solventar las necesidades de sus familias, entre otras.

El concepto de *fraude corporativo* es una problemática que atraviesa a todas las organizaciones. Esta situación es expuesta en *Report to the Nations* (2022), emitido por ACFE, en el cual se estudiaron dos mil ciento diez casos, de ciento treinta y tres países generando como resultado diversas conclusiones. Por ejemplo, en el texto se expone que como consecuencia del fraude las empresas analizadas por ACFE tuvieron en promedio una pérdida de $1.783.000 USD[2]. También, se comenta que el período de tiempo promedio que se demora para detectar un caso de fraude es de doce meses, situación problemática porque a medida que se prolonga el plazo, mayores son las pérdidas monetarias.

Ahora bien, un dato fundamental para el análisis de esta temática es que en el 85% de los casos, la persona que comete el acto delictivo presenta lo que denomina *bandera roja o red flags* (ACFE, 2022, p. 58), es decir que en su

[2] Los datos del informe emitido por ACFE fueron proporcionados por 77 CFE (*certified fraud examiners)*, quienes participaron en una encuesta global sobre fraudes desarrollados e investigados durante enero de 2020 y septiembre de 2021.

comportamiento se pueden ver reflejadas actitudes que permiten vislumbrar la posibilidad de que esté involucrado en un fraude, algunos ejemplos son: dificultades financieras, irritabilidad, comportamiento defensivo y realizar gastos por encima de los ingresos. Esto hace posible detectar el fraude a través de distintas técnicas, porque constituyen un *input* que es posible de analizar.

2.2 Deep Learning

Este apartado es fundamental para comprender el objeto de la presente tesis porque se explicará uno de los conceptos claves: el *deep learning*. Para esto, será necesario transitar la lectura de otras dos terminologías, inteligencia artificial y *machine learning*, dado que el *deep learning* existe gracias al surgimiento de estas dos.

2.2.1 Inteligencia Artificial

Para comprender qué es el *deep learning*, primero será necesario estudiar qué es la inteligencia artificial (IA). La definición que brinda la Real Academia Española es la siguiente: "disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico". Como explica el autor Jon Krohn (2020) el objetivo de la IA es el logro de la "inteligencia general" es decir, de alcanzar amplias capacidades de razonamiento y resolución de problemas (p. 143).

Adicionalmente, los autores Norving, Stuart y Russell (2008), posicionándose en el enfoque que estudia a la IA centrado en un entorno de racionalidad[3], explican que esta tecnología puede considerarse como un agente racional porque "actúa con la intención de alcanzar el mejor resultado o, cuando hay incertidumbres, el mejor resultado esperado" (p.5) en función de su conocimiento (p.2). En este sentido, la inteligencia artificial es una ciencia que estudia la capacidad de las máquinas de aprender a partir de datos y de tomar decisiones racionales, es decir, de manera similar a un humano.

[3] Existe otra corriente de pensamiento cuyo enfoque para estudiar la IA es centrado en los humanos. Es decir, que miden el éxito de la IA en base a si logra o no ciertas cualidades humanas.

Un subgrupo de la Inteligencia Artificial es el *machine learning*, el cual será descripto en el siguiente apartado.

2.2.2 Machine Learning

El *machine learning* (o aprendizaje automático) “se trata de un aspecto de la informática en el que los ordenadores o las máquinas tienen la capacidad de aprender sin estar programados para ello” (Rouhiainen, 2018, p. 16). En línea con esta idea, el autor Krohn (2020) explica que esta rama de la IA es un campo de la informática en el cual se configura un software para que este pueda reconocer patrones en los datos sin la presencia de un programador que tenga que guiarlo en dicho proceso.

Existen tres subconjuntos del aprendizaje automático. El primero de ellos es el *aprendizaje supervisado* y es en el que se apoya el *machine learning* tradicional. En este “los algoritmos usan datos que ya han sido etiquetados previamente para indicar cómo tendrían que ser categorizada la nueva información” (Rouhiainen, 2018, p.18). El autor Krohn (2020) explica que en este tipo de problemas se tiene una variable X que representa los datos que se le provee al modelo como *input* y una variable Y que es un *outcome* ya determinado por el programador. En general, se dividen en dos tipos:

- *Regresión*: en el cual se estima la relación entre variables. Algunos ejemplos incluyen predecir el número de ventas de un producto o el precio futuro de un activo.
- *Clasificación*: permite, a partir de datos ya clasificados, inferir la pertenencia de un dato a una clase. Por ejemplo, permite clasificar a los clientes entre “abandonadores” o no.

El segundo es el *aprendizaje por refuerzos* en el cual se le pide al programa que logre un estado final deseado y se le otorgan recompensas o castigos dependiendo de su curso de acción. Explica Krohn (2020) que la particularidad de este tipo de aprendizaje es que el agente (que puede ser un algoritmo

jugando al Pacman), recibe un *feedback* directo dependiendo de las acciones que toma (como puede ser ganar o perder puntos) (p. 150).

Finalmente, se encuentra el *aprendizaje no supervisado*. Aquí los algoritmos utilizan datos que no se encuentran etiquetados y, por sí solos, buscan maneras de clasificarlos a partir de la identificación de patrones. Aún más, se tienen datos que forman la variable X (*input*) pero no se determina cuál tiene que ser la variable Y (*output*). En este sentido, el objetivo es que el modelo descubra estructuras o patrones escondidos en los datos (Krohn, 2020, p. 150). Esta forma de aprendizaje solo se aplica al *deep learning*.

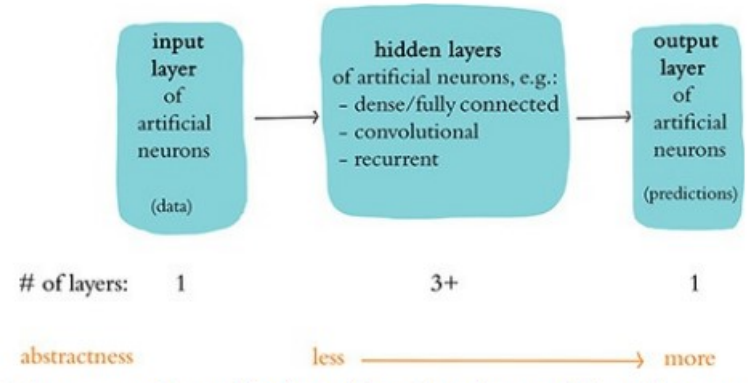
2.2.3 Deep Learning

El *deep learning* se presenta en este trabajo como una herramienta alternativa que facilita la detección del *fraude corporativo*. El autor Jon Krohn (2020) explica que esta rama de la inteligencia artificial se estructura en diferentes capas conectadas entre sí por medio de un tipo de estructura matemática particular: redes neuronales artificiales.

Este sistema adquiere dicho nombre por estar inspirado en las redes neuronales humanas. Quien descubre cómo fluye la información en el cerebro humano es Ramón y Cajal a finales del siglo XIX. Él identifica que las neuronas son unidades individuales que se componen básicamente de tres elementos: dendritas, cuerpo celular y axón. Lo importante de este hallazgo es la forma en que se comunican: los axones de una neurona transfieren la información a la otra neurona, la cual la recibe por medio de las dendritas. Esto es lo que se denomina sinapsis (Klein, 2017).

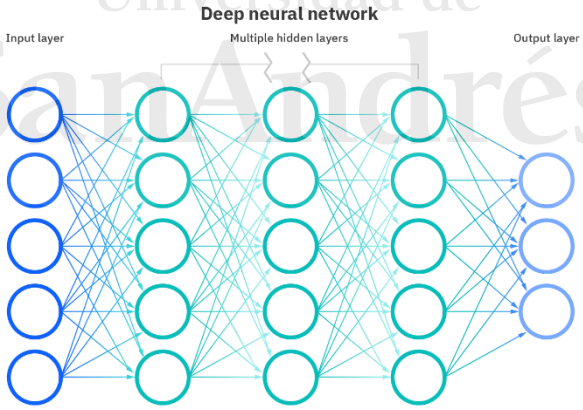
De este descubrimiento se inspiran las redes neuronales artificiales. Estas se componen de *nodos* (análogos a las neuronas) los que transfieren información entre las diferentes estructuras generando un resultado final denominado *output*. Entonces, la estructura es de la siguiente manera: una capa que recibe la información del ambiente (como las dendritas); otras capas escondidas donde se procesa la información y una capa de salida (como los axones),

donde se manifiestan las predicciones (Krohn, año, p.145-146). La forma en que se conectan unas con otras simulan una sinapsis.



Generalization of ***deep learning*** model architectures. Jon Krohn (2022).

Si bien el *machine learning* también se estructura de esta manera, la particularidad del aprendizaje profundo es que su *network* es mucho más complejo porque incorpora más capas para su procesamiento. Esta estructura, sumado a la forma de aprendizaje no supervisado, son las que permiten el desarrollo de su característica principal: emular las capacidades del ser humano (ver, oír y entender).



Redes neuronales del *deep learning*. IBM (2020)

Sus aplicaciones se pueden dividir en dos: el *deep learning* como herramienta para el procesamiento del lenguaje natural, y como herramienta para el reconocimiento de imágenes. El primero implica tomar conversaciones

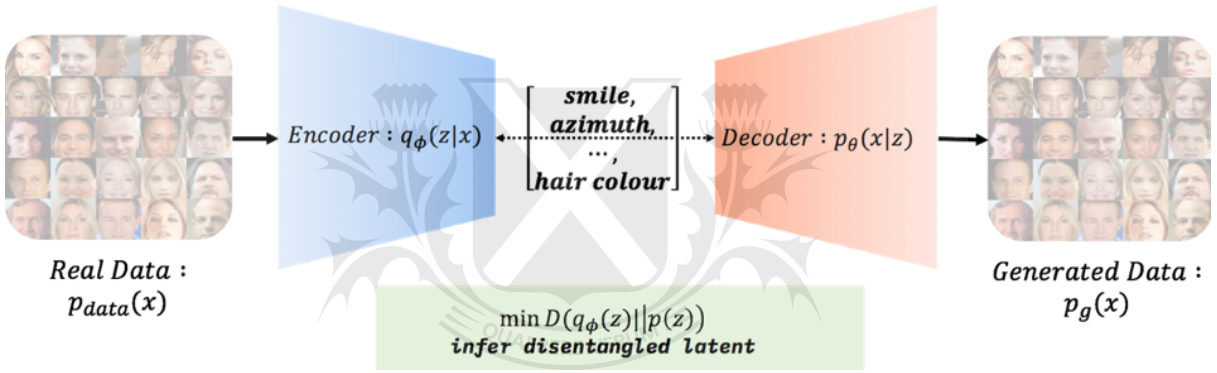
habladas o escritas y procesarlas para diferentes fines, como clasificar documentos y la creación de *chatbots* (Krohn, 2020). En el caso de la detección del fraude, esto será útil para revisar los mails y/o conferencias y detectar patrones en el habla que indiquen la posible presencia de actos fraudulentos. Sobre este punto, Craja, Kim y Lessmann (2020) comentan en *Deep Learning for detecting financial statement fraud* que estudios en psicología social han demostrado que quien comete fraude manifiesta señales lingüísticas que facilitan la identificación del acto. Por ejemplo, suelen utilizar con más frecuencia palabras de connotación negativa y menores autorreferencias (Larcker, Zakolyukina, 2010).

El autor Jon Krohn define al reconocimiento de imágenes como la capacidad de la inteligencia artificial de *ver*, es decir de reconocer objetos ya sea desde una distancia fija como navegando en el mundo real (2020). Por ejemplo, se pueden tomar como *input* para el algoritmo los videos de las cámaras de seguridad y detectar quién ingresa a una determinada área de la compañía sin el permiso correspondiente.

Gracias a estas aplicaciones es entonces que las funcionalidades del *deep learning* pueden dividirse en el análisis de texto, sentimientos, imágenes, video y voz.

- ***Text analytics***: permite extraer valor de grandes cantidades de datos no estructurados (emails, reportes, websides, blogs, redes sociales, etc.).
- ***Sentiment analytics***: permite extraer sentimientos u opiniones subjetivas de texto, video o audio.
- ***Image analytics***: permite extraer información, significado e *insights* de imágenes como fotografías, imágenes médicas o gráficos. Se basa en el reconocimiento de patrones, geometría digital y procesamiento de señales.
- ***Video analytics***; permite extraer información, significado e *insights* de videos. Puede analizar comportamientos.
- ***Voice analytics***; es el proceso de extraer información, significado e *insights* de audios de conversaciones.

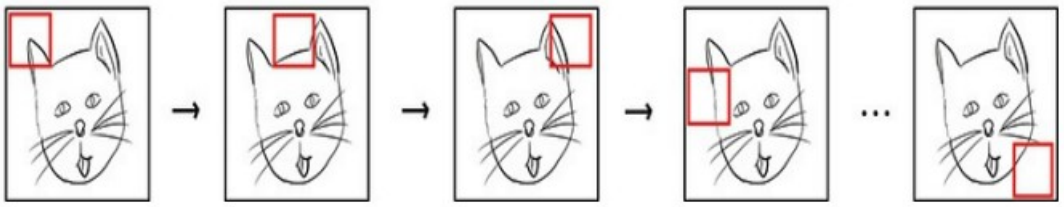
Cabe aclarar que se utilizan diferentes tipos de redes neuronales dependiendo del objetivo que se quiera alcanzar. Por ejemplo, un tipo de red se denomina *autoencoder*. Esta toma *inputs* y aprende cómo comprimirlos y codificarlos en algo que se denomina *code*. El *code* se transfiere a otra capa que se denomina *decoder* la cual aprende a reconstruir esa representación codificada y crea un *output*. La particularidad de esta red es que el *output* es igual al *input*. Esto permite reconocer cuando algo no forma parte del *status quo*, lo que se denomina detección de anomalías. Por eso, es que se utiliza para los casos de errores, fraudes o detección de intrusos (IBM 2022).



IBM (2018)

Otra red muy utilizada, principalmente para el análisis de imágenes, es la *convolutional neural networks (CNN)*. Gracias a ella es posible el reconocimiento de patrones para la identificación de objetos. En esta red se aplica el aprendizaje supervisado, es decir que será necesario que un humano le presente una enorme cantidad de datos etiquetados para que el algoritmo aprenda a identificar el elemento.

Para alcanzar este objetivo, dentro de las capas ocultas se encuentra algo denominado *filters* (o filtros) (IBM, 2021). Cada uno de estos filtros es como una pequeña ventana que escanea la imagen, lo que técnicamente se denomina *the filter convolves* (Krohn, 2020, p. 345):

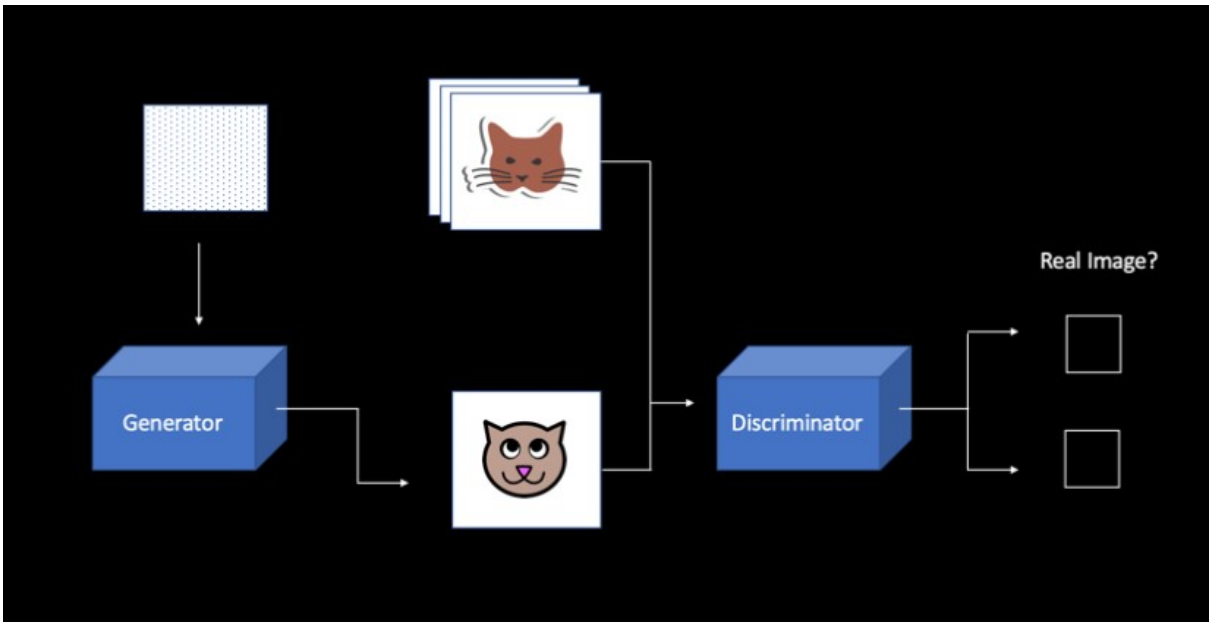


Representación del escaneo de una imagen. Jon Krohn (2020).

En general, existen una gran cantidad de filtros en una red CNN porque cada uno le permite al *network* aprender una representación del dato de una forma única (Krohn, 2020, p. 348). A medida que la red se vuelve más profunda, los filtros reaccionan a combinaciones cada vez más complejas y abstractas. Es por esto que en una primera instancia logran identificar líneas simples, luego colores y finalmente texturas y formas complejas (p. 349).

Luego del escaneo, el algoritmo compara qué tan parecida es la imagen analizada con los filtros y así es como identifica el objeto (IBM, 2021).

Otra red importante se denomina GAN (*generative adversarial network*). Esta utiliza dos redes neuronales en su arquitectura las cuales, en el caso de que hablemos del análisis de imágenes, serán CNN (IBM, 2021). El objetivo es que estas dos se enfrenten en una *adversarial relationship*. La primera se denomina *generator network* que es la encargada de crear un *output* falso a partir de datos aleatorios que se le brindan como *input*. La segunda se denomina *discriminator network* y tiene como tarea determinar si los ejemplos que le envía la red *generator* son falsos o no (Krohn, 2020, p. 525).



Representación de una red neuronal GAN. IBM (2019)

A medida que estas dos redes van iterando, (sin la intervención humana) se vuelven cada vez más expertas en sus tareas (Krohn, 2020, p. 526). El hecho de que alcancen un nivel de aprendizaje elevado es muy importante porque permiten el reconocimiento de fotos o videos falsos, los cuales, muchas veces, pueden utilizarse para difamar a una persona u organización[4].

Estas redes neuronales se nutren de datos no estructurados. Por este motivo el *deep learning* puede focalizarse en un área que es difícil de analizar por los auditores (internos o externos) por las características que se desarrollan en apartado 2.3.

2.2.4 Diferencias entre *deep learning* y *machine learning*

Suele ser común la confusión entre *deep learning* y *machine learning*. Lo que debe quedar en claro es que el *deep learning* es un subgrupo del *machine learning* y que ambos forman parte de la inteligencia artificial. En segundo lugar, la forma de aprender es distinta. Por un lado, el *machine learning* tradicional suele apoyarse en el aprendizaje supervisado, para lo que utiliza

[4] Video que ejemplifica esta problemática: https://www.youtube.com/watch?v=gLoI9hAX9dw

datos etiquetados por los humanos para realizar predicciones. Por otro lado, el *deep learning* aprende principalmente de una manera no supervisada, lo que implica que su algoritmo descubre patrones ocultos en los datos que se le aportan como *input* y sin la presencia de un humano (IBM, 2022). Finalmente, se distinguen por la cantidad de capas que utilizan en su procesamiento, mientras que en el *machine learning* solo hay tres (*input*, procesamiento y *output*), en el *deep learning* habrán más de tres. (IBM, 2022).

2.3 Datos estructurados y no estructurados

Los autores Inmon & Lindstedt (2015) comentan en su libro *Data Architecture: a primer for the data scientist* que los datos de una corporación pueden dividirse en dos grupos: datos estructurados y datos no estructurados. Los primeros mencionados son aquellos que tienen un formato predecible y regular y, en general, se almacenan en bases de datos en las cuales se pueden determinar sus atributos claves. Los segundos son aquellos que no cuentan con una estructura reconocible y, en consecuencia, resulta difícil utilizarlos.

Adicionalmente, este último grupo puede subdividirse en dos partes. Por un lado, los datos no estructurados repetitivos, que son aquellos sin un formato definido y que se generan muchas veces durante un período de tiempo, como es el caso de llamadas telefónicas o sistemas de monitoreo. Por otro lado, los datos no estructurados no repetitivos no cuentan con una frecuencia alta de ocurrencia, como pueden ser, correos electrónicos, contratos y registros de garantía (Inmon & Lindstedt, 2015).

Los autores Dong, Lial & Zhang (2018) comentan en *Leveraging Financial Social Media Data for Corporate Fraud Detection* algunos ejemplos de datos estructurados dentro de las organizaciones, como variables numéricas financieras, ratios, descripciones cuantitativas de las operaciones. Mientras que los datos no estructurados son: discusiones del management, conferencias, videos de cámaras de seguridad, sección MD&A de los estados financieros, reportes, mails. Adicionalmente, explican en su texto que intentar detectar el hecho fraudulento únicamente a partir de la utilización de datos estructurados

resulta insuficiente debido a que los participantes del acto delictivo tienen la posibilidad de modificar la información.

El problema que se presenta con los datos no estructurados es que, dado su gran volumen y velocidad de ocurrencia, resulta complejo distinguir cuáles son relevantes o no para la detección del fraude. Es por este motivo que el *deep learning* se presenta como una herramienta innovadora, debido a que permite analizar los datos no estructurados y así facilitar la detección de hechos delictivos.

2.3.1 ¿Cómo se recolectan y almacenan los datos?

Los datos estructurados se obtienen de diferentes fuentes, como SAP, Salesforce, Excel y Oracle. Para poder ser utilizados, es necesario que atraviesen un proceso denominado **ETL** (*Extract*, *Transform* y *Load*). Este tiene los siguientes pasos:

- Extracción: se extraen los datos desde los sistemas de origen.
- Transformación: se aplican una serie de reglas de negocio sobre los datos para poder ser cargados.
- Carga: los datos se cargan en la fase de destino.
    - Se suele utilizar una etapa intermedia denominada ***data staging*** que sirve para realizar la carga al almacén por medio de bloques. Esto es muy útil cuando se trabaja con una gran cantidad de datos y sirve para evitar errores. Entonces, entre la extracción y transformación hay un *data staging*, mismo que entre la transformación y la carga (Powerdata, 2013).

A partir de este, es posible que las organizaciones muevan datos desde diferentes fuentes, los transformen y carguen en otra base de datos, como los ***datamart*** (Beoto & Rodriguez, 2012). Un *datamart* “es una base de datos departamental, especializada en el almacenamiento de los datos de un área de negocio específica” (p. 5), por ejemplo, ventas, cobranzas y atención al cliente. Todos ellos forman el ***datawarehouse*** que es “una base de datos corporativa que se caracteriza por integrar y depurar información de una o más fuentes

distintas, para luego procesarlas permitiendo su análisis" (p. 2). En este almacén, los datos están formados por **variables o hechos** (valores que se desean analizar, como cantidad de productos vendidos) y **dimensiones** (elementos que permiten ubicar los datos) (p. 2).

Los datos no estructurados, por su parte, se obtienen de las redes sociales, el Internet of Things (IoT), contratos, documentos escritos, grabaciones de voz, mails, videos de cámaras de seguridad, *chats*, entre otros. Aquí también se utiliza el proceso denominado ETL, pero se incorpora otro llamado ***data ingestión***. A partir de este es posible transferir grandes datos de múltiples fuentes a un único sistema de almacenamiento: un ***data lake*** (Sawadogo & Darmont, 2019, p. 104). Un *data lake* es entonces un sistema de almacenamiento para datos que se presentan en múltiples formatos y es utilizado principalmente por especialistas en datos para extraer conocimiento (p. 100).

Finalmente, todos estos datos pueden ser analizados por medio de herramientas de *Analytics*. Estos pueden ser *descriptivo* (para entender el pasado), *predictivo* (para realizar predicciones en base a información histórica), *prescriptivo* (para evaluar decisiones en escenarios futuros) y *minería de datos* (permite descubrir propiedades desconocidas de los datos).

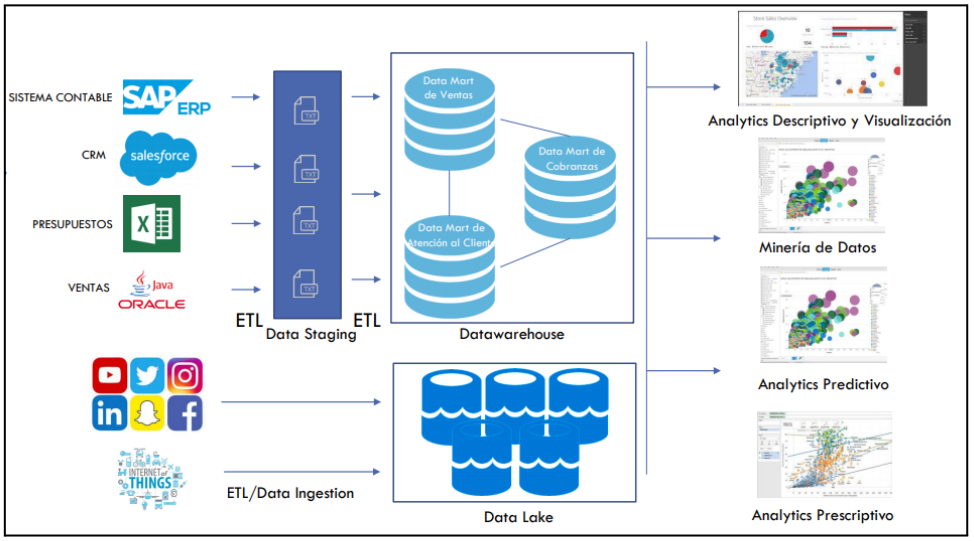


Imagen extraída de una presentación de la materia Procesos y Sistemas de Información. Profesores: Sciolla y Ramos.

2.4 Otros conceptos que serán utilizados en el trabajo de investigación

2.4.1 Big Data

Este concepto “refiere al volumen y tipo de datos provenientes de la interacción con dispositivos interconectados, como teléfonos celulares, tarjetas de crédito, cajeros automáticos, relojes inteligentes (...) y cualquier otro objeto capaz de producir información y enviarla electrónicamente a otro lado” (Sosa Escudero, 2019, p. 31-33). Los datos generados son anárquicos, espontáneos y no estructurados, es decir que no fueron generados con el propósito de crearlos, sino que como resultado de otra acción. Big data se asocia entonces a las tres V (definición brindada por Doug Laney, analista de la consultora Gartner): velocidad, volumen y variedad (este último remite a la naturaleza espontánea del dato) (p. 32-33).

3. Estrategia metodológica

3.1 Tipo de estudio

La temática del presente trabajo de investigación es abordada a través de estudios de carácter exploratorios para comprender el objeto de estudio planteado. Si bien el *fraude corporativo* es una problemática analizada desde distintas perspectivas por diversos autores, se constituye en una limitación la escasa cantidad de antecedentes registrados en publicaciones que profundicen sobre el *deep learning* como herramienta para su detección. La forma de razonamiento será principalmente hipotético deductiva, debido a que el objetivo de este trabajo consiste en estudiar si esta rama de la inteligencia artificial permite la detección del *fraude corporativo*.

3.2 Hipótesis

La hipótesis que se busca comprobar es si el *deep learning* colabora con una detección del *fraude corporativo* de manera más eficiente dado que es una herramienta que permite el análisis de datos no estructurados.

3.3 Casos de estudio y recolección de datos

La información que se utiliza para el estudio de esta temática fue recolectada fundamentalmente de dos maneras. Por un lado, se realizó una revisión documental de trabajos de investigación, artículos académicos y reportes de diferentes organismos, para obtener datos del tipo secundario. Por otro lado, se coordinaron entrevistas con profesionales de diferentes áreas: Auditoría Externa, Auditoría Interna y *Data Analytics & Artificial Intelligence*, con el objetivo de comprender cómo se trabaja con el fraude en la práctica y cuáles son las características que debe tener una herramienta para que detecte el fraude de manera eficiente.

4. Mecanismos actuales para la detección del fraude corporativo

En el siguiente apartado se hará referencia a las diferentes maneras en las cuales el fraude es detectado en la actualidad. Se piensa este análisis a partir de la identificación de diferentes equipos de trabajo, externos o internos a la compañía, que, por las características de su labor, pueden reconocer casos fraudulentos.

4.1 Auditoría Externa

Con el objetivo de indagar sobre la manera en la que el equipo de auditoría externa detecta el fraude se han realizado tres entrevistas con Contadores Públicos. En una ellas el protagonista fue Gabriel Alejandro Gómez Paz, quien cuenta con el título de *Certified Public Accountant* y, en la actualidad, es socio de Deloitte. La segunda charla, fue con Ernesto Mario San Gil, quien fue Presidente de EY durante los años 2014 a 2017 y, hoy en día, es el Director de la carrera *Negocios Digitales* en la Universidad de San Andrés. Finalmente, Pablo Moreno, socio de EY hasta el año 2022, especialista en auditoría externa en la industria de *retail* y consumo masivo.

Para comenzar, es necesario recordar que una auditoría de estados contables es el examen de los Estados Financieros de un ente realizado por un auditor externo, de acuerdo con las normas de auditoría aplicables, a los fines de emitir un informe con su opinión sobre dichos estados con relación a las normas contables aplicables[5].

El auditor externo, para llevar a cabo su trabajo, se debe apoyar en diferentes tipos de normas de auditoría dependiendo del país en que se realice el

[5] Definición brindada por Gabriel Alejandro Gómez Paz en la materia Formación Práctica en Auditoría e Impuestos.

encargo. En Argentina y en la Unión Europea las más importantes son las Normas Internacionales de Auditoría emitidas por la Federación Internacional de Contadores (IFAC), de la cual la Federación Argentina de Consejos Profesionales de Ciencias Económicas (FACPCE) es miembro. En el presente trabajo de graduación nos enfocaremos en la sección 240, dado que es allí donde se comenta sobre el rol que ocupa el auditor externo en la detección del fraude.

Se explica en dicho escrito que los principales encargados de la prevención y detección del fraude son los responsables del gobierno de la entidad y la dirección. En consecuencia, tienen el compromiso de crear una cultura de honestidad y comportamiento ético, y de realizar una supervisión activa para evitar el acto fraudulento.

Por su parte, “el auditor es responsable de la obtención de una seguridad razonable de que los estados financieros considerados en su conjunto están libres de incorrecciones materiales debidas a fraude o error” (NIA 240, p. 138). En este sentido, debido a las limitaciones inherentes a una auditoría, la norma aclara que es posible que no se detecten dichas incorrecciones. Aún más, especifica que “el riesgo de no detectar incorrecciones materiales debidas a fraude es mayor que el riesgo de no detectar las que se deben a error” (NIA 240, p. 138), dado que el fraude implica la creación de planes sofisticados y organizados para su ocultación. No obstante, sí se manifiesta que en la auditoría se debe prestar especial atención a dos tipos de riesgos significativos: *management override of controls* y *revenue recognition*.

El primero de ellos, afecta a los estados contables en su conjunto e implica el riesgo de que la gerencia sobrepase al control interno de la compañía y manipule la información contable. Con el objetivo de evaluar este riesgo, el equipo de auditoría externa realiza diferentes procedimientos sustantivos, los cuales no se focalizan en probar los controles o procesos de la compañía. Por el contrario, buscan encontrar representaciones erróneas en los estados financieros.

En línea con esta idea, fueron comentados en las entrevistas diferentes expresiones de dichos procedimientos, dentro de los que se encuentran:

- **Testeo de asientos al cierre**. Un riesgo para el auditor es que la gerencia incluya asientos contables al final del ejercicio para alcanzar distintos objetivos (por ejemplo, aumentar las ventas para lograr el resultado *target*). Es por esto que, de acuerdo al juicio profesional, el auditor toma una muestra de los asientos al cierre de la cuenta que se desea analizar.
- **Revisar asientos que acrediten ventas y que no tienen contrapartida en créditos por ventas**. Una práctica fraudulenta común implica aumentar las ventas de manera ficticia a través de uno o más asientos, pero, para no alterar la cuenta créditos por ventas, como contrapartida se ponen otras (como bienes de uso, gastos de comercialización).
- **Analizar asientos incluidos en la contabilidad un día feriado**. Como no es común que se trabaje en los feriados, estos asientos son de especial importancia para el auditor. Para encontrarlos, se utilizan herramientas que permiten filtrar los asientos contables en base a diferentes características. De esta manera se logran identificar aquellos que, para el auditor, representan potenciales indicadores de fraude.
- **Comparar las estimaciones realizadas por la empresa con los hechos reales**. Las estimaciones, por su naturaleza, implican un gran grado subjetividad por parte de la gerencia de la compañía. Por lo tanto, por ser una aproximación a la realidad, pueden ser utilizados para cometer fraude.

El segundo riesgo significativo que se manifiesta en la NIA 240 refiere a *revenue recognition*. Estas “suelen tener su origen en una sobrevaloración de los ingresos mediante, por ejemplo, su reconocimiento anticipado o el registro de ingresos ficticios” (ISA 240). Si bien este riesgo puede ser refutado por el auditor con argumentos que deben ser manifestados en su informe, se explican en la norma diferentes procedimientos para su estudio. Algunos de ellos son:

- Comparar ingresos registrados mensualmente y por línea de producto o segmento de negocio durante el periodo actual de información con periodos anteriores que sean comparables.
- Confirmar con clientes determinados términos contractuales relevantes y la ausencia de acuerdos paralelos.
- Indagar entre el personal de ventas y marketing de la entidad sobre ventas o envíos realizados en una fecha cercana a la finalización del periodo.
- Verificar que las transacciones generadoras de ingresos han ocurrido y se han registrado adecuadamente.

Del análisis de las herramientas utilizadas en la auditoría para la detección del fraude se observan algunas limitaciones. La primera de ella es compartida tanto por Ernesto como por Gabriel y se vincula al hecho de que, si el fraude es orquestado por la alta gerencia, será casi imposible su detección. Esto es así porque este grupo cuenta con los medios necesarios para crear Estados Contables ficticios y, en consecuencia, los procedimientos de auditoría dejan de ser suficientes para detectar el hecho fraudulento.

La segunda limitación es remarcada por Pablo Moreno y refiere a la improbabilidad de detectar fraudes con los procedimientos sustantivos y analíticos de auditoría. Esta opinión es compartida por varios autores, como Tang y Karim, quienes expresan que los estándares de auditoría son insuficientes para abordar la cantidad de ambigüedad y variación entre los diferentes tipos de fraude realizados por distintos individuos y organizaciones (2018, p. 327). Además, agregan que los procedimientos de auditoría no pueden abordar de manera efectiva el riesgo de fraude presente en la información no financiera (p. 325).

Adicionalmente, los pensadores Yoon, Hoogduin y Zhang (2015), reflexionan acerca de sí es posible obtener evidencia de auditoría suficiente y adecuada sobre el riesgo de fraude a partir de los procedimientos actuales de auditoría. Explican que es difícil obtener pruebas de fraude porque estas están

relacionadas muchas veces con el estilo de vida de la persona, su conducta y moralidad, ninguno de los cuales es necesariamente observable en la información financiera (p. 433). Es por este motivo que proponen al *big data* como evidencia complementaria de la auditoría.

El Contador Público Pablo Moreno acuerda con estas ideas y expresa que desde su perspectiva la auditoría se irá transformando hacia lo que se conoce como *audit analytics*, que refiere al uso de *data analytics* a los fines de la auditoría aprovechando al *big data*. Los objetivos de esta práctica son diversos[6], por ejemplo:

- Permite comparar la información financiera y operativa de la entidad con la de la industria y competidores a los fines de identificar su desempeño relativo.
- Posibilita una comparación más detallada ("granular") de la información y así profundizar la identificación de cuestiones relevantes y su posible origen.
- En base al total de la población de interés de auditoría o universo permite identificar áreas de interés particular, secciones de mayor o menor riesgo en función de sus atributos específicos.
- Al efectuar una evaluación de los riesgos de manera más profunda, granular, posibilita identificar mejor las áreas de riesgo de la auditoría y direccionar los procedimientos pertinentes.
- Con las poblaciones completas a disposición puede realizarse un muestreo y selección más rápidos y por ende más eficientes.
- Pueden desarrollarse estimaciones para procedimientos analíticos sustantivos considerando múltiples factores que mejoren la precisión de la prueba: información histórica de la entidad, datos del segmento del mercado y/o competidores, información macroeconómica, cálculo de correlaciones estadísticas entre variables, etc.

[6] Los beneficios fueron expuestos por Gabriel Alejandro Gómez Paz en la materia Formación Práctica en Auditoría e Impuestos.

Adicionalmente, en el *The CPA Journal* (2017) se explica que la transición de la auditoría tradicional a las auditorías del futuro se produce principalmente por los cambios del cliente a auditar en su modelo de negocio. Comentan que el uso de *big data* en las compañías implica que la información contable se construya en base a datos estructurados y no estructurados y que, en consecuencia, el auditor tiene que familiarizarse con estos conceptos. Por ejemplo, las llamadas para realizar ventas a los consumidores pueden ser combinadas con los ingresos por ventas para armar la cuenta "ventas".

De todas maneras, a pesar de los grandes beneficios que presenta esta herramienta, Pablo Moreno explica que no se utiliza en gran medida en la actualidad por diferentes motivos. En primer lugar, por la reticencia de algunas empresas para brindar toda su información. En segundo lugar, por la falta de implementación de herramientas tecnológicas en las compañías que puedan capturar los datos. Finalmente, por la incapacidad de muchos estudios de auditoría de realizar las inversiones necesarias para implementar *softwares* de análisis de datos.

Del estudio en conjunto de estas limitaciones expuestas en esta sección es posible considerar que estos son los motivos por los cuales, según lo manifestado por ACFE, auditoría externa solo ha detectado el 4 % de los casos de fraude que han estudiado durante el 2022.

4.2 Equipos de fraude

En esta sección, nos enfocaremos en el análisis de las diferentes herramientas que son utilizadas por los equipos de fraude para la detección de estos crímenes. Para esto, se hará uso de una charla desarrollada durante la cátedra *Control Interno* y protagonizada por Leandro Dores, *Assurance Partner* en EY y Ramón Pacheco, ambos miembros del servicio forense de EY.

Para la detección del fraude se apoyan en el *forensic data analytics* que consiste en la recopilación y análisis de datos estructurados (por ejemplo: libro mayor, datos de transacciones, datos contractuales, SAP, Oracle) así como no

estructurados (ej. *email*, *Whatsapp*, *free text fields*) para analizar transacciones, hechos o patrones de comportamiento relacionados con conductas inapropiadas, fraude o incumplimientos.

En línea con esta idea, una de las herramientas que usan para encontrar fraudes se denomina *Discovery*. A partir de ésta, se realiza un proceso de identificación y recolección de datos relevantes sobre las comunicaciones de los miembros de la empresa. Este programa se nutre de diferentes técnicas que le permiten identificar dichos documentos, las cuales son: palabras claves (por ejemplo: maltrato, sobre), uso de conceptos donde la coincidencia no se basa en términos específicos sino en un significado conceptual (por ejemplo: debajo de la mesa) y asociación de palabras con otros términos o archivos.

Otro de los mecanismos utilizado por estos equipos se denomina r*evisión asistida por tecnología (TAR)*. Gracias a esta, se desarrolla un modelo de análisis personalizado para que identifique documentos relevantes para su posterior revisión. Un sistema similar se utiliza para el estudio de los emails: el *email threading*. Esta herramienta reduce el tiempo y la complejidad de la revisión de correos electrónicos dado que tiene la capacidad de juntar toda la actividad vinculada a un mismo usuario.

Comentan además que la manera en que detectan fraudes ha ido evolucionando con el paso del tiempo. Por un lado, en lo que respecta a los datos estructurados, el enfoque tradicional se focalizaba más en combinar, agrupar, ordenar y filtrar en base a reglas predeterminadas. El enfoque actual busca detectar anomalías por medio de análisis basado en estadísticas.

Por otro lado, asociado a los datos no estructurados, antes solo se realizaba una búsqueda de palabras claves. Hoy en día, realizan una exploración, minería y visualización de datos basados en conceptos y el análisis del lenguaje en un contexto más amplio.

Es posible reconocer diferentes desventajas vinculadas a las metodologías utilizadas por los equipos de fraude. La primera se vincula a la falta de integración de las diferentes fuentes de datos para poder combinarlos y obtener otro tipo de conclusiones.

Además, no utilizan herramientas predictivas, solo toman datos históricos para sus investigaciones. Esto se constituye como una limitación porque la manera en que se orquesta el fraude cambia a lo largo del tiempo. Por lo tanto, predecir comportamientos permitiría detectar el fraude con anticipación.

Finalmente, explican que sus servicios son solicitados cuando auditoría externa o miembros de la alta gerencia reconocen situaciones o patrones que denotan ciertas anomalías. Es por esto que trabajan el fraude luego de que este ya se perfeccionó, lo que aumenta el costo y las repercusiones negativas de la práctica delictiva.

4.3 Auditoría Interna

Auditoría interna es un área dentro de las compañías que enfrenta el fraude. Según el Instituto de Auditores Internos, auditoría interna es una actividad independiente, de consultoría, diseñada para mejorar las operaciones de una organización. Su objetivo consiste en agregar valor a las empresas a partir de la evaluación y mejora de los procesos de gestión de riesgos y de control.

En consecuencia, auditoría interna trabaja con los riesgos, es decir, todo aquello que podría impedir que la organización alcance alguno o más objetivos. Uno común a todas las organizaciones es el de fraude. Para mitigarlos, auditoría interna sigue una serie de pasos que permiten su administración[7]:

1. **Identificación de los riesgos**. Aquí el equipo de auditoría identifica los objetivos de negocio de la compañía para evaluar los riesgos asociados.
2. **Evaluación de los riesgos**. En este paso se evalúan y priorizan los riesgos identificados. Para esto, se calcula la criticidad del riesgo inherente, es decir sin la presencia de controles mitigantes, en su estado

[7] Estos pasos fueron expuestos en la cátedra Control Interno y Sistema Contable.

puro. Este valor es el resultado de calcular el impacto por la probabilidad de ocurrencia. El impacto es el efecto medible en la compañía en caso de que el riesgo ocurra, mientras que la probabilidad de ocurrencia hace referencia a la cantidad de veces que ese riesgo puede ocurrir en un período determinado.

3. **Evaluación de la capacidad de respuesta**. Refiere a la competencia de la empresa para hacer frente a los riesgos. Existen cuatro tipos:
    a. *Evitar la actividad*. Implica dejar de cumplir el objetivo del negocio.
    b. *Mitigar por medio de controles*. Esto es implementar sistemas de control interno que pueden ser preventivos o detectivos. Los primeros son aquellos que se anticipan a la ocurrencia del riesgo, como por ejemplo los controles de acceso para restringir el uso de activos. Los segundos, se ejecutan una vez ocurrido el riesgo y buscan identificar el error o fraude con posterioridad, como es el caso de las conciliaciones bancarias.
    c. *Transferir a un tercero*. Algunos ejemplos son: asociarse con otra compañía, contratar seguros y utilizar contratos de cobertura.
    d. *Aceptar*. Esta opción se utiliza cuando el impacto y la probabilidad de ocurrencia son bajos, motivo por el cual la compañía puede seguir operando sin gestionar este riesgo.
4. **Mejoras en la administración de riesgos**. En este paso se busca mejorar el nivel general de las competencias de la empresa para la administración de riesgos, principalmente a partir de la actualización continua de los controles y de los riesgos.

Con el objetivo de indagar sobre el rol de auditoría interna en la detección del fraude, entrevistamos a Alejandro Ernesto Hordij, *Associate Partner* en EY. En su posición, se encarga de los servicios de auditoría interna, control interno y administración de riesgos de negocio para clientes locales e internacionales. En la charla, Alejandro hizo foco en la importancia de controles internos robustos para poder detectar y prevenir los hechos delictivos. De todas maneras, agrega que auditoría interna no suele identificar el universo de casos de fraude porque “no mira todo”, por el contrario, se trabaja con muestras.

Vinculado a este punto, en un artículo publicado por KPMG (2016) se explica que la existencia de controles internos débiles fueron la causa del 61 % de los fraudes[8]. Continúa diciendo que esta carencia queda reflejada en el hecho de que un número importante de fraudes (14 %) fueron detectados por accidente y no por los controles internos. Incluso, notan un crecimiento en la cantidad de sujetos que realizan actos delictivos al ver una oportunidad en la falla de controles internos. Se pasó de un 18 % en 2013 a un 27 % en 2015.

Continuando con esta temática, Alejandro explica que desde auditoría interna se puede trabajar en cerrar las oportunidades para cometer fraude, pero no siempre es posible. En línea con esta idea, en la publicación de KPMG (2016) se sostiene que "si bien la existencia de controles internos fuertes es importante, no es la panacea" (p. 14), el 21 % de las personas que cometen fraude simplemente lograron evitar los controles.

Adicionalmente, Alejandro comenta que dentro del control interno hay una máxima: cuando dos personas o más se ponen de acuerdo para realizar un fraude, es casi imposible que los controles puedan identificarlo. Por ejemplo, en el estudio de KPMG, el 62 % de los casos de fraude fueron realizados en grupo. Estas colusiones se arman porque necesitan cómplices para evadir los controles o porque, para evitarlos, necesitan cierta información o habilidades que tiene otra persona (p. 15).

La falta de controles internos o su ineficiencia no son la única crítica que hace KPMG. Esta compañía comenta en un artículo llamado *Companies Failing to Leverage Technology to Combat Fraud* (2016) que las empresas no utilizan suficientes herramientas tecnológicas para detectar el fraude. Phil Ostwalt, jefe global de investigaciones en KPMG, explica que los sistemas de monitoreo y *data analytics*, son herramientas imprescindibles para identificar comportamientos anómalos o sospechosos.

[8] Basado en una encuesta mundial de profesionales de KPMG que investigaron a 750 estafadores entre marzo de 2013 y agosto de 2015.

Finalmente, Alejandro comenta que la auditoría interna puede ser una fuente de identificación de fraude pero que, en general, suele salir a la luz por denuncias anónimas. Los *tips*, sus ventajas y limitaciones serán estudiados en el próximo apartado.

4.4 Mecanismos adicionales para la detección del fraude

Otras formas de detectar el fraude son comentadas en el Reporte a las Naciones (2022), como es el caso de: revisión de documentación, confesiones, vigilancia y monitoreo, por accidente. Sin embargo, el más importante es el *tip*, es decir, que miembros de la compañía o agentes externos identifican los casos de fraude y deciden comunicarlos por diferentes medios (como mails o llamadas telefónicas). En el texto se manifiesta que esta fue la forma en que se descubrieron el 42 % de los casos. Además, en un artículo publicado por KPMG (2016) se explica que este es el principal método utilizado para detectar los fraudes realizados en grupo.

Si bien este mecanismo resulta ser el más eficiente para detectar fraudes, cuenta con algunas desventajas. La consecuencia más importante es que los fraudes demoran más en ser detectados y, por lo tanto, generan mayores pérdidas promedio. Esto es así porque, para que funcione, es necesario que el sujeto conocedor del hecho delictivo comente la situación.

Para que esto suceda, se comenta en el Reporte a las Naciones, que es necesario construir espacios en los cuales la persona se sienta segura. Es por esto que desde la organización se crean *hotlines*, es decir, canales de comunicación para que el sujeto pueda contar el hecho en un marco de confidencialidad y confianza (Hayes, 2010, p. 67).

De todas maneras, es fundamental que los casos de fraude comentados en los *hotline* sean analizados para pensar acciones futuras. Caso contrario, la herramienta pierde credibilidad y, en consecuencia, disminuye su efectividad. Tal vez esta es la razón por la que el 70 % de las organizaciones estudiadas

por ACFE contaban con *hotlines* y, aun así, el tiempo promedio para la detección del fraude fue de doce meses (ACFE, 2022, p. 21 - 24).

5. El *deep learning* como herramienta para detectar el fraude corporativo

Para estudiar el uso del *deep learning* como herramienta para la detección del fraude corporativo, se ha realizado una entrevista a Nelson Ponzoni. Nelson se desempeña como Manager y científico de datos en el área *Data Analytics & Artificial Intelligence* en EY. Es ingeniero en Informática egresado de la Universidad Nacional del Litoral, Santa Fe, Argentina. Se especializa en áreas relacionadas al aprendizaje maquinal, análisis masivo de datos y visualización.

Durante la charla, el entrevistado comenta que ha hecho uso del *deep learning* para combatir el fraude en una empresa de *e-commerce* de Argentina. Este proyecto consistía en la identificación de movimientos fraudulentos en transacciones financieras con características manuales. La particularidad de la compañía a la que se le presta el servicio es que, por su tamaño y cualidades de negocios, el número de transacciones es muy grande. Por lo tanto, herramientas manuales u otras incapaces de procesar gran cantidad de datos resultan insuficientes. Es por este motivo que comienzan a indagar en nuevos mecanismos tecnológicos para solucionar la problemática.

El ingeniero en informática explica que, en los inicios del proyecto, existían dos alternativas para aplicar: *machine learning tradicional* o *deep learning*. Para la decisión prestaron especial atención a la forma en que cada algoritmo aprende. El *machine learning* se caracteriza por implementar el aprendizaje supervisado. En este sentido, durante su construcción, requiere que el programador le muestren una gran cantidad de datos etiquetados. Para este proyecto, se necesitan datos de transacciones fraudulentas y otros de transacciones normales, para que, de esta manera, el algoritmo logre identificar el fraude cuando ocurra. Entonces, aprende la regla de relación existentes con datos que fueron *tageados* (etiquetados) por humanos. El principal problema que se

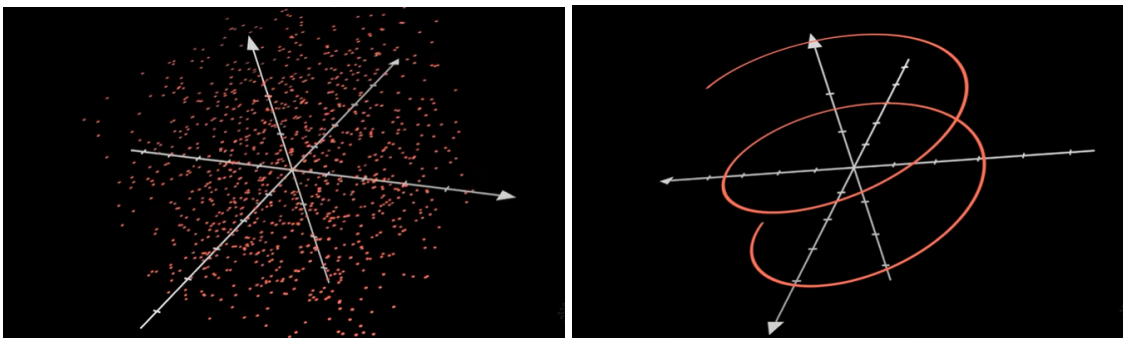
presenta es que el fraude se orquesta de diferentes maneras y, en consecuencia, no es posible extraer una gran cantidad de datos donde se manifieste el hecho delictivo. Es por este motivo que se opta por el *deep learning*.

El aprendizaje profundo se constituye como una herramienta extremadamente poderosa porque aplica el aprendizaje no supervisado. Por eso, durante su puesta en práctica este, por sí solo, extraerá automáticamente las características significativas de los datos, las cuales permitirán hacer conexiones y reconocer el fraude (Voican, 2021, p. 78). A continuación, se explicará con mayor detalle cómo funciona.

El Ingeniero Ponzoni comenta que, para la identificación de movimientos fraudulentos en transacciones financieras (vinculados a pagos y compras), utilizaron un tipo particular de red neuronal denominada *autoencoder*.

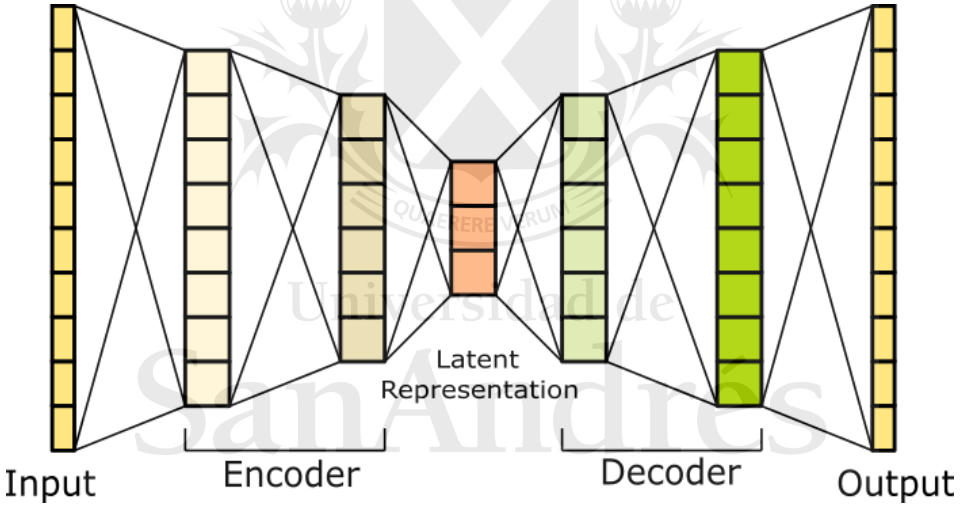
La estructura de esta red neuronal se divide en dos partes, una codificadora (*encoder*) y otra decodificadora (*decoder*). Para explicar cómo funciona, vamos a pensar en las transacciones financieras que comentó Ponzoni. Estas transacciones cuentan con un montón de datos que constituyen diferentes columnas, como puede ser: monto, fecha, nombre del destinatario, etc. La parte codificadora toma esos datos y los comprime. ¿Qué quiere decir esto? Que se arma una especie de resúmen con pocos datos que permitan representar el fenómeno. Técnicamente se dice que alcanzan una dimensión menor, la cual va a contar solo de tres coordenadas que permiten ubicar los datos en un gráfico e identificar los *outliers* (los datos anómalos)[9].

[9] Video útil para entender este tipo de red neuronal: https://www.youtube.com/watch?v=3jmcHZq3A5s



Aquí se observa gráficamente la diferencia entre datos sin comprimir y comprimidos (Jost, 2019)

Finalmente, la capa decodificadora o *decoder* toma la representación latente (*latent representation*) y, por medio de un proceso de reconstrucción, logra como salida la misma entrada. Entonces el *output* es una réplica del *input*.

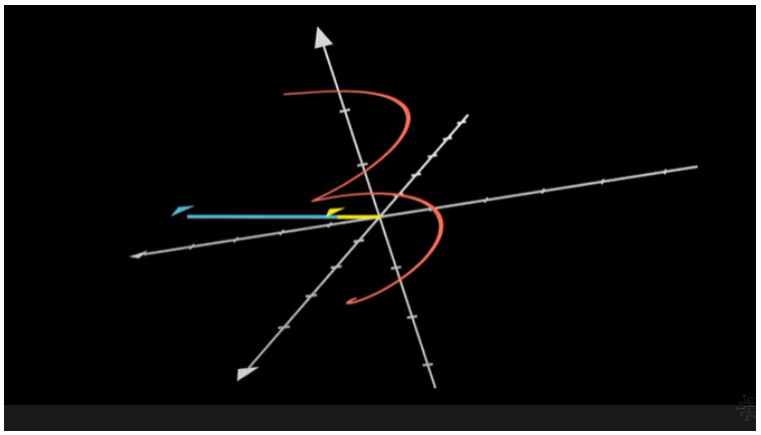


Fuente: html.it

Dado que este tipo de red neuronal aprende a partir de un gran conjunto de datos normales (es decir que tienen los mismos atributos), lo más probable es que la salida sea diferente a la entrada solo cuando se proporcionen como *input* datos anómalos.

Los datos anómalos son aquellos que se desvían significativamente de la forma general en la que se comportan los datos (IBM, 2022). Por ejemplo, si tenemos una lista con dos columnas donde la primera tiene países y la segunda sus

capitales, si hay un dato que tiene como país a España y como capital a Hong Kong, se está desviando de la norma (no cumple con la norma de contener para cada país su respectiva capital), entonces se dice que es anómalo.



Gráficamente, el dato anómalo se representa con la flecha amarilla. Vemos que se distancia del "espiral" (la norma) y por eso se lo considera un posible fraude (Jost, 2019)

En consecuencia, si se lo alimenta con datos que contienen diferencias, no logrará reconstruir el *input*. Es por esto que la variación entre la entrada y la salida se considera como un posible fraude (IBM, 2022). En el ejemplo que explica Nelson, se buscó identificar aquellas transacciones financieras que se alejaban de la norma, como por ejemplo, desviaciones de fondos.

Lo poderoso de esta red es que **produce conocimiento con los datos que se le brindan como *input* sin necesidad de parametrizarlo para obtener un resultado deseado**.

Otros son los usos del *deep learning*. La autora Voican explica en su texto que se utiliza para la detección de casos fraudulentos en la utilización de las tarjetas de créditos. Como las personas siguen una determinada secuencia para hacer pagos, las transacciones realizadas por usuarios fraudulentos tendrán un patrón diferente al aprendido por el modelo (2021, p. 76). Entonces, esa diferencia podrá ser detectada para que los analistas del fraude puedan indagar en ella.

Adicionalmente, Meng y Yen (2018) hacen uso del *deep learning* para enfrentar los fraudes *online*. Comentan que este es muy complejo y diverso y que genera grandes pérdidas en las compañías. Algunas formas de manifestarse son a través de reseñas, me gustas y comentarios falsos, realizados por cuentas falsas o *hackeando* cuentas reales. Explican que existe un mercado ilegal con proveedores preparados para realizar fraude quienes, en realidad, no crean nuevas estructuras, sino que por el contrario hacen uso de los elementos ya presentes en las plataformas online (como el casillero de reseñas/comentarios).

Argumentan que, en un principio, la manera que pensaron para solucionar este problema es por medio del *machine learning* supervisado. Al correr este sistema durante cuatro años, identificaron que existen patrones de comportamiento entre los usuarios que cometen fraude, pero no pudieron reconocer todos. Es por este motivo, que comienzan a indagar en el *deep learning*.

Agregan los autores que el *deep learning* es una herramienta innovadora porque mejora su *performance* a medida que aumentan la cantidad de datos, situación que no ocurre con otros algoritmos de aprendizaje (como *machine learning*).

Además, explican que tratar al fraude como un problema de clasificación (como ocurre con el *machine learning*), no es suficiente. El motivo es que con el *machine learning* tradicional no es posible extraer todas las relaciones existentes entre las distintas formas en que se orquesta el fraude, entonces las clasificaciones son insuficientes. Con el *deep learning* sí se logra un mayor nivel de detalle. Consecuentemente, el algoritmo puede determinar con una probabilidad alta (95 %) si se trata de un fraude o no.

Ahora bien, cabe destacar que se utiliza un tipo de red neuronal distinta dependiendo de la información disponible, dado que requieren procesamientos diferentes. Por ejemplo, para el caso de las imágenes y videos se utilizan las denominadas *convolutional neural network* (CNN). En este tipo de estructura lo

que ocurre es que se aplican filtros en algunas de las capas ocultas, los cuales tienen la capacidad de analizar las imágenes.

En este sentido, el *deep learning* no solo permite detectar fraudes a partir de anomalías. Por el contrario, tienen otras funcionalidades que también pueden ser utilizadas para identificar el hecho delictivo. Estas son explicadas en el escrito *A Survey on Deep Learning: Algorithms, Techniques and Applications* (Pouyanfar et al., 2018):

- **Procesamiento del lenguaje natural**: es una serie de algoritmos y técnicas que principalmente se enfocan en técnicas computacionales para entender el lenguaje humano.
    - *Sentiment Analysis*: permite examinar un texto y clasificar los sentimientos u opiniones del escritor.

  Algunos ejemplos permiten demostrar la existencia de esta funcionalidad y su utilidad. Actualmente, se usa para el *customer experience* y el *employee experience*. La autora Michael Schrage (2016) explica que aplicando el análisis de los sentimientos en las conversaciones de *Slack* o en las llamadas telefónicas es posible identificar qué tan probable es que un empleado abandone la organización. También identifica el nivel de *engagement* de los empleados a partir de sus conversaciones. Otro caso, expuesto por Ajayi y Sodha (2020), es el análisis de los *feedback* para entender cómo se siente el cliente en relación al producto o servicio y así mejorar su experiencia.

  La autora Schrage (2016) comenta que el *sentiment analytic* puede ser utilizado en los casos de fraude en la identificación de cierto significado en el habla. Comparte un ejemplo en el cual, a partir del reconocimiento de un lenguaje poco común de los vendedores de una empresa Fortune 1000, la compañía logró reconocer que estaban realizando negociaciones ilegales con los competidores de la firma.

    - *Machine Translation*: es la traducción automática de textos.

- *Paraphrase Identification*: es el proceso de identificar dos oraciones y proyectar qué tan similares son, basándose en la semántica escondida.
- *Summarization*: permite extraer la información más significativa y relevante de muchos documentos.
- *Question Answering*: logra interpretar el lenguaje natural, lo razona, y emite una respuesta apropiada.

Aún más, dada esta aplicación (el procesamiento del lenguaje natural), el *deep learning* se convierte también en una herramienta muy valiosa para detectar en *mails* o documentaciones internas, palabras que indiquen la posibilidad de fraude. El aporte que hace en esta forma de detección es a través del reconocimiento o extracción de datos de soportes no estructurados. Es decir, que de una gran masa de datos, el *deep learning*, por su estructura (las redes neuronales) puede hacer uso de esos datos y obtener conocimiento, a pesar de que no estén etiquetados. Luego, se utiliza *machine learning* para su posterior clasificación (identificar si son palabras que denotan o no la presencia de fraude).

- **Procesamiento de datos visuales**: refiere a la capacidad del *deep learning* para realizar tareas que impliquen el análisis de imágenes.
  - *Image Classification*: implica la clasificación de diferentes imágenes en distintos grupos. Esta habilidad ha ido mejorando con el paso de los años. En 2015, el algoritmo hizo una performance increíble en la realización de esta tarea. Alcanzó un 3,6 % de error, mientras que el humano entre un 5 % y un 10 %, siendo esta la primera vez en que una máquina le gana al cerebro humano en la clasificación de imágenes.
  - *Object Detection and Semantic Segmentation*: el *deep learning* puede identificar objetos, pero también tiene la habilidad de comprender una imagen a nivel de píxeles que es necesario para aplicaciones en el mundo real, como conducción autónoma, visión

robótica, entre otros. A esto último se lo denomina *semantic segmentation*.

- *Video Processing*: permite extraer información, significado e *insights* de videos.

- **Procesamiento del habla y audio**: es un área muy estudiada porque es la que posibilita la interacción perfecta entre el humano y la computadora.
  - *Speech Emotion Recognition*: las emociones influencian tanto las características de la voz como el contexto lingüístico del discurso. El *deep learning* puede reconocer no solo las palabras y su significado dependiendo del contexto, también tiene la habilidad de reconocer emociones.

Con la información recolectada podemos pensar en algunos ejemplos. Pablo Moreno hace hincapié en la identificación de una *red flag* para analizar el fraude: cuando un empleado o director vive por encima de sus ingresos. Se podría parametrizar el sistema para que identifique cuándo una persona tiene elementos de lujo. Por ejemplo, por medio de una cámara de seguridad se podría determinar si un empleado cuenta con un reloj *Rolex*.

También, se puede hacer uso del *Social Network Analysis*. Esto es el estudio de las redes sociales, ya sea de una persona o de un grupo (Pouyanfar, et al., 2018, p. 22). En línea con esta idea, se puede sumergir el algoritmo en la red social de un empleado para saber si mantiene un estilo de vida por encima de sus ingresos.

Aún más, otra bandera roja es la irritabilidad. A partir del *sentiment analytics*, el *deep learning* podría reconocer el sentimiento y emitir una alarma. Así como también, puede entender el significado semántico de un posteo en una red social (p.22) y así analizar las emociones del empleado.

Adicionalmente, por medio del *video analytic* podría reconocer si una persona sin autorización ingresa a áreas restringidas de la organización. Incluso si algún trabajador abandona el edificio con elementos de la oficina.

La autora Voican hace una pregunta muy pertinente en su texto: ¿por qué usar *deep learning* ahora si la tecnología tiene varios años? En primer lugar, la respuesta a esta incógnita es que actualmente vivimos en un mundo donde hay una enorme cantidad de datos (*big data*) y este algoritmo tiene la capacidad de poder procesarlos. En segundo lugar, hoy en día se cuentan con *hardware* avanzados que permiten su procesamiento, los que simplemente no existían cuando comenzó a desarrollarse esta tecnología. Esta idea se sustenta en la ley Moore, la cual explica que la potencia del procesamiento general de los ordenadores se duplica cada dos años. En tercer lugar, por la existencia de herramientas que permiten modelar este sistema de una manera mucho más sencilla (2021, p. 75). En el próximo apartado comentaremos con mayor detalle los beneficios del *deep learning* para la detección del fraude.

6. Beneficios de la implementación del *deep learning* para la detección de *fraudes corporativos*

De los análisis desarrollados a lo largo del escrito, es posible identificar diferentes beneficios que posicionan al *deep learning* como una herramienta eficiente para la detección del *fraude corporativo*.

El primero de ellos se vincula con el concepto de *big data*. Su surgimiento es posible gracias al incremento de las capacidades de almacenamiento, al mejoramiento del poder de las computadoras y a la facilidad de acceder a mayor cantidad de datos (IJERT, 2020, p. 2). Estos tres factores impactan en las organizaciones generando que, con el paso de los años, el **volumen** de datos que acumulan sea cada vez mayor (Inmon y Linstedt, 2015, p. 37), se calcula que su crecimiento es de un 40 % por año a nivel mundial (IJERT, 2020, p. 2).

Además, se presentan con mayor **velocidad**, por lo que se requieren algoritmos que trabajen con *real time*. Esto es así porque entre más jóvenes son los datos, más relevantes son para la compañía (Inmon y Linstedt, 2015, p. 38). También, los datos se presentan de formas **variadas**, por ejemplo, a través de páginas web, dispositivos móviles, en formato de video o texto, de forma no estructurada.

Estas tres V´s (volumen, velocidad y variedad) son las que definen al *big data* y las que generan la necesidad de capturar y almacenar casi un número ilimitado de datos para su posterior análisis. El problema que se presenta se vincula a la carencia de tecnologías que puedan manejar esas características (Inmon y Linstedt, 2015, p. 46-47).

El *deep learning* se presenta como una alternativa para resolver esta problemática. Esto es así porque su algoritmo puede analizar y aprender de una gran masa de datos complejos y no estructurados. Por lo tanto, puede trabajar con *big data* y así obtener información valiosa, como por ejemplo de fraude (IJERT, 2020, p. 1). Además, el *deep learning* es una herramienta prometedora porque es capaz de identificar automáticamente características complejas y de aprender sin la presencia de un humano (p.2).

Adicionalmente, el *deep learning*, como fue comentado, puede trabajar con datos no estructurados (estos son los que conforman al *big data*). Se estima que más del 80 % de los datos de una compañía son de este tipo, como pueden ser videos, audio, imágenes, mails, chats (Inmon y Linstedt, 2015, p. 63).

Sin embargo, la mayor cantidad de las decisiones en una organización son tomadas utilizando datos estructurados. Los motivos son diversos, en primer lugar, porque es fácil de automatizar. En segundo lugar, porque se adapta fácilmente a las bases de datos de las compañías y, una vez en ellas, son simples de analizar. En tercer lugar, porque existen una gran variedad de herramientas analíticas para estudiarlos. Pero, lo que las empresas descuidan, es el enorme valor que se encuentra en los datos no estructurados. La dificultad está en desbloquear este potencial (Inmon y Linstedt, 2015, p. 63).

Como se explica en el marco teórico, los datos no estructurados se dividen en dos: repetitivos y no repetitivos. Los autores Inmon y Linstedt (2015) explican que los más valiosos son los no repetitivos. Por ejemplo, los *emails* en los que los clientes expresan su opinión, charlas de los consumidores con los *call center*, contratos, entre otros. El problema que se presenta con este grupo de datos es la dificultad para analizarlos por no ser uniformes. Además, muchas veces se encuentran en forma de texto, lo que requiere un nivel de análisis superior (p. 66).

El *deep learning* es una herramienta que puede trabajar con estas adversidades. Una de sus ramas es el procesamiento del lenguaje natural (*natural language processing* o NLP), a partir de la cual el algoritmo toma un texto (hablado o escrito) y lo procesa para completar una tarea o hacer una actividad más sencilla para el humano. El NLP cuenta con diferentes niveles de complejidad. El más elevado (que es el que se utiliza en el aprendizaje profundo) tiene la capacidad de identificar características sofisticadas del lenguaje (Krohn, 2020, p. 94-96). Una de ellas es la contextualización, es decir, que el algoritmo tiene la habilidad de comprender el contexto de un texto (Inmon y Linstedt, 2015, p. 67). Por ejemplo, vinculado al fraude, la expresión "esto es un robo" puede significar dos cosas: 1) que efectivamente están robando 2) que algo es muy caro. La complejidad en este punto es que el *deep learning* tiene que valerse de otra información más allá de lo escrito o hablando, ya sea el tono en que se dice o la lógica detrás de la palabra (p.69). Afortunadamente, el aprendizaje profundo puede lograrlo.

Aún más, el *deep learning* no solo trabaja con texto, también puede identificar sentimientos u objetos en imágenes y videos. Esta habilidad es fundamental porque el algoritmo puede reconocer ***red flags*** (o banderas rojas) es decir, ciertos comportamientos que realiza la persona cuando comete el fraude y que funcionan como una alarma para que la víctima pueda descubrir el crimen (ACFE, 2022, p. 58). Según ACFE el 85 % de los empleados que cometen este hecho delictivo presentan algún tipo de bandera roja (p. 44). Las más comunes son: vivir por encima de sus ingresos, dificultades financieras, vínculo poco común con vendedores o clientes, irritabilidad, *mobbing*, divorcio y problemas familiares, presión excesiva por parte de la organización, problemas de adicciones, quejas por salarios bajos, entre otros (p.28) (ver anexo 1).

Aún más, la compañía KPMG (2016) ha realizado una investigación cuyo objeto de estudio fueron 750 casos de fraude con el objetivo de comprender el perfil del estafador. Las conclusiones a las que llegaron son las siguientes:

- *Edad y género*: la mayor cantidad de estafadores son hombres entre 36 y 55 años (ver anexo 2).

- *Insiders, Outsiders y Colusión*: el 65 % de los estafadores son empleados de la compañía, y el 21 % ex empleados. Además, los empleados que cometen el fraude suelen estar más de 6 años en la compañía (38 % de los casos). Adicionalmente, en el 62 % de los casos de fraude existe colusión.
- *Level of seniority*: en el caso de los estafadores de género masculino, en el 32 % de los casos ocupan cargos de management y en el 26 % de directores. Para el caso de las mujeres, en mayor proporción (42 %) son miembros del staff y en el 38 % managers.
- *Rasgos personales*: en el 38 % de los casos son personas respetadas en la organización.
- *Controles internos*: en el 44 % de los casos, las personas que cometen fraude tienen autoridad ilimitada, es decir, que fácilmente pueden sobrepasar los controles internos.
- *Tipo de fraude*: el fraude más común es la apropiación indebida de activos, mientras que en segundo lugar se ubica el fraude en los estados financieros.

Claro está que la conducta y las cualidades de quien comete un fraude es un objeto de estudio que ha sido exhaustivamente analizado. Lo valioso es que hay patrones que se repiten entre estos sujetos. Por lo tanto, contar con una herramienta que pueda identificarlos agregaría mucho valor a la compañía porque disminuiría las pérdidas generadas por fraude. El *deep learning* es una de ellas.

Continuando con otro análisis, recordemos que uno de los objetivos de este trabajo de investigación consiste en estudiar si los datos no estructurados, como complemento de los estructurados, permiten la detección del fraude. Se ha comentado en diferentes secciones de este escrito, que los datos no estructurados tienen información valiosa para cumplir este fin. Pero, en el caso de los estructurados la situación es diferente. Los autores Dong, Liao y Zhang (2018) sostienen que, para identificar los hechos delictivos, la mayoría de las compañías optan por contratar a auditores contables o reguladores, quienes

analizan registros financieros, estados contables y otros documentos que genera la organización (como facturas y órdenes de pago). El problema que presenta esta metodología es que esta información puede tener errores o ser ficticia, lo que entorpece la investigación (p. 3).

Otro beneficio, en concordancia con lo explicado por el Ingeniero Ponzoni, es que esta rama de la inteligencia artificial permite la detección en tiempo real de un posible caso de fraude, porque procesa los datos de manera inmediata. Una vez que el algoritmo está programado, este construye, por sí solo, nuevas conexiones neuronales y busca anomalías u otros elementos (dependiendo de cómo esté programado) sin la presencia de un humano. Es por esto que puede funcionar como una alarma para las compañías ya que, en caso de detectarse algún elemento que se distancia de la norma, puede enviar una notificación manifestando la situación, para que luego el posible fraude pueda ser comprobado.

En línea con esta idea, recordemos que el *deep learning* tiene la capacidad de aprender sin la presencia de un humano. Esta funcionalidad es particularmente importante para la detección del fraude porque esta práctica se orquesta de diferentes maneras y, en consecuencia, contar con una herramienta que pueda identificar patrones inusuales sin supervisión y en tiempo real resulta muy relevante. Este fue el motivo principal por el que el Ingeniero Ponzoni optó por el aprendizaje profundo para su trabajo.

Como se explica en *Report to the Nations* (2022), las organizaciones no pueden prevenir todos los casos de fraude, eventualmente un empleado cometerá algún hecho delictivo. Es por este motivo que la habilidad de detectarlo de manera rápida es crucial. Hoy en día, sus estudios indican que el tiempo medio en que se demora en identificarlo es de doce meses, generando una pérdida promedio de 100.000 USD. Pero no solo esto, sino que a medida que pasa el tiempo, las pérdidas financieras son cada vez mayores. Por ejemplo, si transcurren más de sesenta meses, en promedio es de 800.000 USD (p.13).

Además, comentan que hay algunos tipos de fraude que generan daño con mayor velocidad e impacto que otros. Por ejemplo, el fraude en los estados financieros es el que tiene mayor velocidad, generando pérdidas de 32.000 USD por mes, seguido por la corrupción, con 12.000 USD[10] (p.15). Incluso, este resultado puede triplicarse en los casos donde grupos de personas se colisionan para cometer el hecho, y aún más cuando ocupan cargos de poder (p.16).

El *deep learning*, por su capacidad de detección en tiempo real, se puede convertir en un activo muy valioso para las compañías. Pero aún más, no solo es importante el tiempo en que se demora en identificarlo, sino que también la forma en que se hace, porque ambas variables impactan en la empresa (p.21). Con esta tecnología puede hacerse de una manera muy sofisticada, informando a personas claves del gobierno corporativo para que ellas puedan pensar en la mejor manera de investigarlo y tomar las medidas necesarias. Todo esto con el objetivo de generar una cultura organizacional en la cual el fraude no es aceptable.

Por todos estos motivos, es que podemos afirmar que el *deep learning* es una tecnología eficiente para la detección del fraude. Por eficiente se entiende a la capacidad de alcanzar las metas establecidas. En este caso, por la posibilidad de trabajar con *big data* y con datos no estructurados, por permitir la identificación del hecho en tiempo real y por reconocer patrones sin la presencia de un humano, es que aseguramos que es una metodología que logra reconocer los hechos delictivos. Aún más, estas características demuestran que puede hacerlo de una manera más eficiente que las otras herramientas utilizadas en la actualidad.

[10] Para determinar la velocidad de los diferentes tipos de fraude se dividió el monto total de la pérdida por la cantidad de meses en que demora en ser detectado.

7. Conclusiones

A lo largo del presente trabajo de investigación, se ha abordado la temática del *fraude corporativo* desde múltiples perspectivas. Hemos recorrido su definición junto con la teoría que explica por qué un sujeto comete un hecho delictivo, denominada el triángulo del fraude. Además, nos apoyamos en diferentes autores para comprender cuáles son las consecuencias negativas de esta práctica, desde pérdidas económicas, de legitimación empresarial, quiebra de la compañía y hasta incluso repercusiones en la sociedad.

También, analizamos cuáles son las responsabilidades que tienen Auditoria Externa, Auditoría Interna y equipos especialistas en fraude respecto a esta problemática e indagamos sobre los mecanismos que utilizan para detectarlo.

En este punto, reconocimos algunas limitaciones en cada especialidad. En el caso de Auditoría Externa, argumentamos que los procedimientos sustantivos y analíticos no son suficientes para la identificación de un fraude, por el contrario, son necesarias herramientas de análisis de datos para poder hacer frente a este problema. Aunque el *Audit Analytics* es una tendencia creciente, no se aplica en la práctica por diferentes motivos: económicos, legales, reticencia por parte del Directorio para brindar los datos, entre otros.

Auditoría Interna, por su parte, se enfoca más en cerrar las oportunidades para la concreción de los hechos delictivos, antes que en la detección propiamente dicha. Adicionalmente, la falta de inversión en nuevas tecnologías para aplicar en los controles también se constituye como un limitante.

Finalmente, en lo que respecta a los equipos de detección del fraude, vemos que hacen más uso de las herramientas de análisis de datos pero ninguna de ellas es predictiva, solo hacen uso de los datos históricos. Además, aún no lograron la integración de sus sistemas, lo que tal vez permitiría una detección

más eficiente. Otra limitación es que comienzan sus investigaciones tiempo después del perfeccionamiento del hecho, lo que aumenta las pérdidas para la compañía.

Claro está que la detección del fraude es aún un campo de estudio que requiere de atención. Todavía no se ha logrado implementar un mecanismo que disminuya a casi cero esta problemática. Sin embargo, el surgimiento de nuevas tecnologías puede colaborar con ese objetivo. El *deep learning* es una de ellas.

Durante el estudio de esta rama de la inteligencia artificial, reconocimos su enorme abanico de funcionalidades, respectivas al análisis de texto, video, imágenes y sentimientos. Con la ayuda del Ingeniero Ponzoni, descubrimos que la forma en que se estructuran las redes neuronales y su mecanismo de aprendizaje, posibilitan identificar elementos en los datos que ingresan como *input,* los cuales denotan la existencia de fraude. Además, otras características de esta tecnología permiten confirmar la hipótesis de este trabajo de investigación. Una de ellas, es la posibilidad de trabajar con *big data*, es decir, con datos no estructurados y así sumergirse en aquellos, generados por la organización o sus miembros, que no son tenidos en cuenta por otras especialidades que se ocupan de la detección del fraude. También, por su forma de trabajar, es posible identificar el hecho en tiempo real, lo que es fundamental porque entre mayor es el tiempo en que se demora en detectarlo, mayores son las pérdidas económicas. Adicionalmente, como fue comentado, el perfil del defraudador es un objeto que ha sido extensamente estudiado por diversas instituciones, como KPMG y ACFE. Esta descripción incluye desde características físicas (como edad y género), hasta características de la personalidad (lo que denominamos *red flags*), todas ellas identificables por medio del *deep learning*. Es por estos motivos que concluimos que es una herramienta eficiente para la detección del fraude.

Sin embargo, quedan aún aspectos por investigar. Explica el ingeniero Ponzoni que, en la actualidad, no es posible la integración de diferentes redes

neuronales. Esto quiere decir que un mismo algoritmo no tiene la capacidad de incluir todas las funcionalidades del aprendizaje profundo. Además, como se explica en *Global profiles of the fraudster: technology enables and weak controls fuel the fraud* (2016), la tecnología es un arma de doble filo, porque sus avances generan herramientas más poderosas para la detección del fraude, al mismo tiempo que colaboran para que los criminales encuentren áreas vulnerables en la compañía para atacar. En consecuencia, el *deep learning* se presenta como una alternativa innovadora en este momento, pero tal vez, en un par de años, se deba direccionar la mirada hacia otras tecnologías. Entonces, combatir el fraude debe convertirse en una práctica continua.

Llegado a este punto, muchos lectores se preguntarán por qué el *deep learning* no tiene un uso extendido en las compañías, siendo que cuenta con tantos beneficios. Proponemos dividir a las barreras para su adopción en tres:

1. Conocimiento del área. Durante la recolección de información, se identificó que no existe gran cantidad de escritos que hagan referencia a la utilización del *deep learning* en áreas de la compañía, menos aún para el fraude. Solo se observa un uso extendido para los casos de fraude en tarjetas de crédito y débito. Tal vez, esta barrera se vincula al hecho de que todavía falta una comprensión profunda de cómo adaptar esta nueva tecnología a los negocios. El autor Sosa Escudero define a esto como una falta de “cultura algorítmica” que hace que se desconfíe de los resultados de los algoritmos complejos y que, en consecuencia, no se tengan en cuenta las grandes oportunidades que ofrecen (2019, p.167).
2. Recursos capacitados. Otra de las limitaciones es la falta de personas especializadas en estas temáticas. Un estudio de *Statista* (2022) muestra la penetración de habilidades de Inteligencia Artificial (IA) por país en todo el mundo en 2018. Estados Unidos tuvo la mayor penetración de habilidades de IA entre su fuerza laboral, mientras que en Argentina solo representa un 3 % (ver anexo 3).

3. Carencia de datos de calidad. Muchas veces sucede que los datos generados por las organizaciones no son de calidad y, en consecuencia, los algoritmos funcionan mal. Esto genera grandes pérdidas en las organizaciones no solo por la posibilidad de tomar malas decisiones, sino también por el tiempo consumido en “arreglar” dichos datos (Redman, 2016). Para esto, el autor Redman explica que es importante que quienes recolectan los datos sepan con exactitud qué es lo que quiere o necesita el área que los utilizará (también denominado cliente) (2020). Además, son necesarias buenas bases de datos que logren almacenarlos de una manera correcta y confiable.

Adicionalmente, Walter Sosa Escudero, en su libro *Big Data* (2019), comenta otras limitaciones vinculadas a la utilización de los datos y algoritmos que nos parecen interesantes de mencionar. Una de ellas se relaciona con el uso inescrupuloso de los datos. Comenta la importancia de pensar en límites éticos que frenen el impulso de comunicar cualquier cosa, máxime ante la posibilidad de error (p.143-144). Por ejemplo, si a partir del uso del *deep learning* se observan tendencias que incriminan a un empleado de la compañía, es importante que esta información se maneje con confidencialidad hasta que se pruebe el hecho, de lo contrario se podría afectar enormemente a esa persona.

Otra cuestión que menciona se denomina “la falacia de la correlación” (p.160). Esto refiere a que “la alta relación entre dos variables ni valida ni refuta el hecho de que una cause la otra” (p.160). Esto es particularmente importante para los casos de fraude. Por ejemplo, si nuestro algoritmo identifica que una persona entra a un área de la compañía sin autorización, no necesariamente implica que está cometiendo un hecho delictivo. Recordemos que el margen de error está siempre presente. Es por esto que Sosa Escudero explica que existe una gran diferencia entre predecir correctamente y explicar los resultados del algoritmo con coherencia (p. 162).

De todas maneras, estas no son barreras que no se puedan superar. Será necesario que los profesionales del futuro aprendan sobre estas nuevas

tecnologías y sean disruptivos, es decir, que se animen a implementarlas en las áreas donde trabajen. Particularmente, el Contador Público y el Licenciado en Administración de Empresas tendrá un rol fundamental en el liderazgo de equipos que se ocupen de la detección del fraude. Esto es así porque durante su formación académica adquieren distintas habilidades que son comentadas por Dores y Pacheco:

1. Tienen una visión integral de las actividades del negocio y de los riesgos relevantes.
2. Conocen las fuentes de información y flujos de transacciones.
3. Saben identificar tendencias y patrones inusuales en los procesos y controles asociados.
4. Poseen conocimientos generales en materia de regulaciones y contratos.
5. Cuentan con los conocimientos para ser nexos e interlocutores en equipos interdisciplinarios.

Igualmente, reconocemos que para que los Contadores y Administradores lleven adelante la evolución de la detección del fraude hacia la inteligencia artificial, es importante incorporar materias de tecnología a estas carreras. Principalmente, para que estas profesiones acompañen la acelerada evolución tecnológica. No con el objetivo de ser expertos programadores, sino para conocer su existencia y liderar equipos que tengan como objetivo su implementación. Esperamos que este trabajo de investigación sea útil para este fin.

Finalmente, concluimos este trabajo destacando que el *deep learning*, por sí solo, no erradicará el fraude en las organizaciones. Por el contrario, es necesaria una cultura donde la honestidad sea el mensaje principal, donde las condiciones laborales sean óptimas para todos y en donde sus líderes demuestren, con el ejemplo, que las prácticas delictivas no son el *modus operandis* de la firma. Estas son las compañías que tenemos la responsabilidad

de construir como futuros profesionales egresados de la Universidad de San Andrés.

8. Bibliografía

- ACFE. (2022). Occupational Fraud 2022: A Report to The Nations. Recuperado de:

  https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

- Ajayi D. & Sodha S. (2020). Solving common challenges in sentiment analysis with help from Project Debater. *IBM Watson Blog*. Recuperado el 10 de octubre de 2022 de:

  https://www.ibm.com/blogs/watson/2020/08/solving-common-challenges-in-sentiment-analysis-with-help-from-project-debater/

- Arthur Meng, Ting-Fang Yen (2017). Deep Learning for Large Scale Online Fraud Detection. Fighting Fraudsters among Billions of Users. Recuperado de:

  https://www.databricks.com/session/deep-learning-for-large-scale-online-fraud-detection-fighting-fraudsters-among-billions-of-users

- Bergur Thormundsson. (17 de marzo de 2022). AI skill penetration by country worldwide 2018. *Statista*. Recuperado de:

  https://www-statista-com.eza.udesa.edu.ar/statistics/947911/ai-skill-penetration-by-country/

- Blackburn, Robin. (2002). La debacle de Enron y la crisis de los fondos de pensiones. New left review (14), 25-50. Recuperado de: https://newleftreview.es/issues/14/articles/robin-blackburn-la-debacle-de-enron-y-la-crisis-de-los-fondos-de-pensiones.pdf

- Bravo, Rodrigo Monge. (2015) Contabilidad Creativa y Estafa: Análisis del Caso Enron [Tesis de grado, Universidad de Comillas]. http://hdl.handle.net/11531/4565

- Craja, P., Kim, A., & Lessmann, S. (2020). Deep learning for detecting financial statement fraud. *Decision Support Systems*, *139*.

- Dong, W., Liao, S., & Zhang, Z. (2018). Leveraging Financial Social Media Data for Corporate Fraud Detection. Journal of Management Information Systems, 35(2), 461–487.

- Hayes. (2010). More Red-Hot Tips on Fraud Hotlines. The Journal of Government Financial Management, 59(2), 66.
- IBM Technology. (15 de marzo de 2022). *What are Autoencoder?* [Video]. Youtube. Recuperado de:

  https://www.youtube.com/watch?v=qiUEgSCyY5o
- IBM Technology. (6 de octubre de 2021). *What are Convolutional Neural Networks (CNNs)?* [Video]. Youtube. Recuperado de:

  https://www.youtube.com/watch?v=QzY57FaENXg
- IBM Technology. (11 de noviembre de 2021). *What are GANs (Generative Adversarial Networks)?* [Video]. Youtube. Recuperado de:

  https://www.youtube.com/watch?v=TpMIssRdhco
- IBM Technology. (31 de marzo de 2022). *Machine Learning vs Deep Learning* [Video] Youtube. Recuperado de: https://www.youtube.com/watch?v=q6kJ71tEYqM
- Inmon & Lindstedt (2015). "Data Architecture: a primer for the data scientist"
- International Journal of Engineering Research & Technology (IJERT) (2020). A Depth of Deep Learning for Big Data and its Applications, 8(10), 20–23.
- Isoré Gutiérrez. (2020). El fraude corporativo y las buenas prácticas para su efectivo tratamiento. Derecho & Sociedad, 55, 491–502.
- Jost, Zak. [WelcomeAIOverlords]. (28 de octubre de 2019). *Simple Explanation of AutoEncoders* [Video]. Youtube. Recuperado de: https://www.youtube.com/watch?v=3jmcHZq3A5s
- Kaminski, K. A., Sterling Wetzel, T., & Guan, L. (2004). Can financial ratios detect fraudulent financial reporting? Managerial Auditing Journal, 19(1), 15–28.
- Karpoff, J. M., Lee, D. S., & Martin, G. S. (2008). The Cost to Firms of Cooking the Books. Journal of Financial and Quantitative Analysis, 43(3), 581–611.
- Klein Joanna. Santiago Ramón y Cajal, el hombre que dibujó los secretos del cerebro, (2017). Recuperado el 23 de noviembre de 2022 de:

https://www.nytimes.com/es/2017/02/21/espanol/cultura/santiago-ramon-y-cajal-el-hombre-que-dibujo-los-secretos-del-cerebro.html

- KPMG. (2016). Global profiles of the fraudster: Technology enables and weak controls fuel the fraud. Recuperado de: https://advisory.kpmg.us/content/dam/advisory/en/pdfs/profiles-of-the-fraudster.pdf

- Krohn Jon (2020). Deep Learning illustrated. A visual, interactive guide to artificial intelligence (1ra edición). Addison-Wesley Data & Analytics Series).

- Larcker, D. F., & Zakolyukina, A. A. (2012). Detecting Deceptive Discussions in Conference Calls. Journal of Accounting Research, 50(2), 495–540.

- Michael Schrage (2016). Sentiment Analysis Can Do More than Prevent Fraud and Turnover. Recuperado de: https://hbr.org/2016/01/sentiment-analysis-can-do-more-than-prevent-fraud-and-turnover

- Normas Internacionales de Auditoría (2019). NIA 240.

- Pang, Shen, C., Cao, L., & Van Den Hengel, A. (2022). Deep Learning for Anomaly Detection. ACM Computing Surveys, 54(2), 1–38.

- Pouyanfar, Sadiq, S., Yan, Y., Tian, H., Tao, Y., Reyes, M., Shyu, M.-L., Chen, S.-C., & Iyengar, S. S. (2019). A Survey on Deep Learning. ACM Computing Surveys, 51(5), 1–36. https://doi.org/10.1145/3234150

- Power Data (20 de agosto de 2013). Staging: la salvaguarda de los procesos ETL. Recuperado el 15 de octubre de: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/312643/staging-la-salvaguarda-de-los-procesos-etl

- Rouhiainen, Lasse (2018). Inteligencia Artificial: 101 cosas que debes saber hoy sobre nuestro futuro (1ra edición). Alienta Editorial.

- Russell, Stuart & Norving, Peter. (2008). Inteligencia artificial: un enfoque moderno (2a. ed.). Pearson.

  https://luismejias21.files.wordpress.com/2017/09/inteligencia-artificial-un-enfoque-moderno-stuart-j-russell.pdf

- Shaio Yan Huang, Chi-Chi Lin, An-An Chiu & David C. Yen (2016). Fraud detection using triangle risk factors. Springer, 1344–1356.

- Tang, & Karim, K. E. (2017). BIG DATA in Business Analytics: Implications for the Audit Profession. The CPA Journal (1975), 87(6), 34–39.

- Tang, J., & Karim, K. E. (2019). Financial fraud detection and big data analytics – implications on auditors' use of fraud brainstorming session. Managerial Auditing Journal, 34(3), 324–337.

- Thomas C. Redman. (22 de septiembre de 2016). *Bad Data Cost the USD $3 Trillion Per Year.* Harvard Business Review. Recuperado el 20 de noviembre de 2022 de:

  https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year

- Thomas C. Redman. (10 de febrero de 2020). *To Improve Data Quality, Start at the Source.* Harvard Business Review. Recuperado el 20 de noviembre de 2022 de:

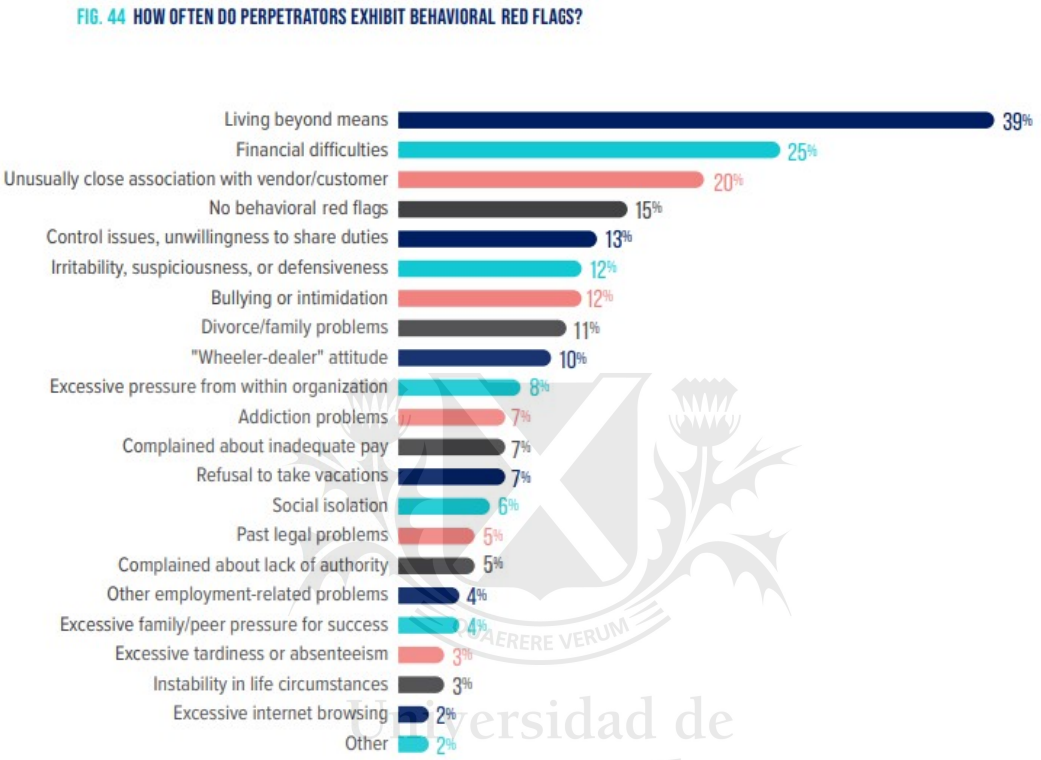
  https://hbr.org/2020/02/to-improve-data-quality-start-at-the-source

- Voican. (2021). Credit Card Fraud Detection using Deep Learning Techniques. Informatica Economica, 25(1/2021), 70–85. https://doi.org/10.24818/issn14531305/25.1.2021.06

- Yoon, Hoogduin, L., & Zhang, L. (2015). Big Data as Complementary Audit Evidence. Accounting Horizons, 29(2), 431–438. https://doi.org/10.2308/acch-51076

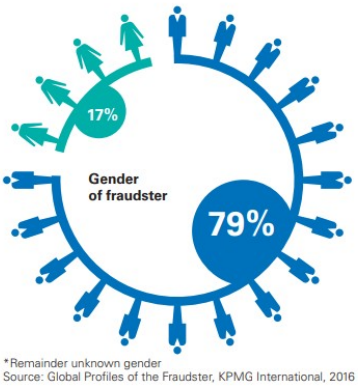
9. Anexos

ANEXO 1



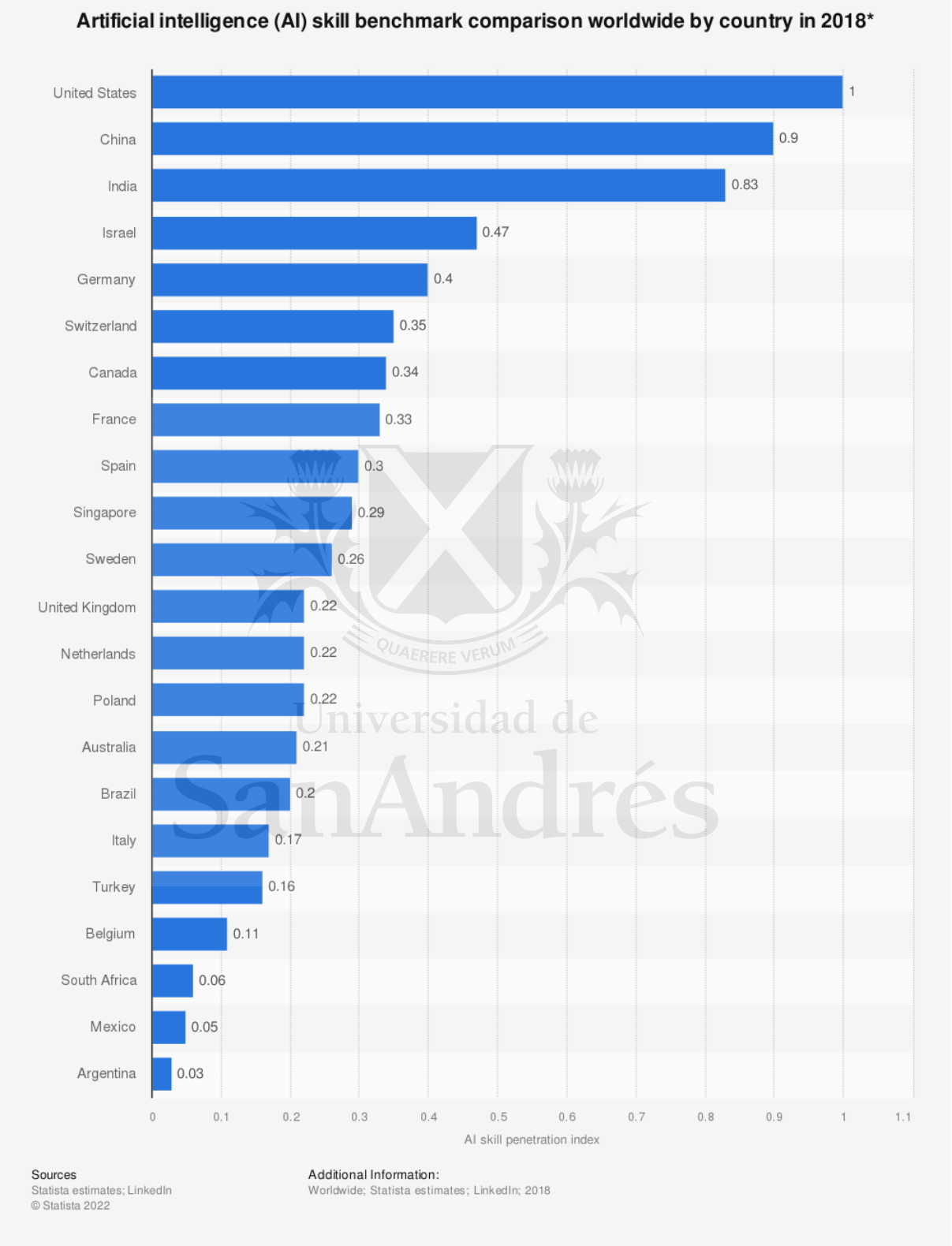
ACFE, 2022, p. 58

ANEXO 2



KPMG, 2016, p. 7

ANEXO 3



Statista, 2022