**Ecosistema de la IA. Conceptualización, desafíos y problemáticas del Tratamiento automatizado de datos personales**

**Datos personales:** es información sobre personas físicas o jurídicas de cualquier tipo. Por ejemplo, un DNI un domicilio, la situación crediticia, etc.

**Datos sensibles:** Son aquellos datos personales que son susceptibles de generar situaciones de segregación o discriminación de la persona que los tenga. Aquí hablamos de datos referidos al origen étnico, opiniones políticas, afiliación sindical, etc.

No es obligatorio darlos, no son de índole pública y no se pueden almacenar.

Luego, los datos biométricos que identifican a la persona son datos sensibles solo cuando pueden revelar otros datos y pueden provocar discriminación. Por ejemplo, cuando los datos dan información sobre la etnicidad de la persona. Además, los registros sobre antecedentes penales o contravencionales pueden existir, pero solo pueden tenerlos las autoridades públicas competentes.

**Perfiles:** Las grandes empresas de tecnología en general generan perfiles de las personas en base a sus interacciones con el entorno digital, con esto pueden inferir aspectos de nuestra persona.

La unión europea ha definido la elaboración de un perfil como toda forma de tratamiento automatizado consistente en utilizar datos personales para evaluar determinados aspectos de un individuo. Los perfiles digitales se elaboran por medio de algoritmos para predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, ubicación o movimientos.

El tratamiento automatizado posibilita una actualización constante de nuestros perfiles digitales. Es decir, ya no se espera que los datos personales sean suministrados por el usuario, sino que son recolectados, almacenados y tratados sin intervención humana. Esto hace que nuestros perfiles digitales sean dinámicos y que en ocasiones hasta puedan inferir situaciones de nuestra persona antes que nosotros mismos, por ejemplo, una variación en nuestros gustos.

Esto se puede potenciar más si se trabaja agrupando enormes cantidades de perfiles digitales y comparando los distintos comportamientos de cada uno, para, por ejemplo, analizar la evolución de las sociedades o agrupar a las personas por afinidad en redes sociales.

Todo lo anterior si bien trae grandes beneficios para las personas y empresas conlleva enormes riesgos.

1. El usuario muchas veces no puede dar un consentimiento válido de esto ya que en general no se lo informa correctamente o se lo pone difícil.
2. Se pueden vulnerar derechos al tomar decisiones a gran escala solo basándose en tratamientos automatizados y comparaciones.
3. El perfil digital en ocasiones puede sesgar o distorsionar los derechos de las personas sobre los cuales tiene influencia.
4. La IA y el tratamiento automatizado hace más frecuente el uso de scorings para clasificar a las personas según su nivel de ingresos. Un scoring mal implementado generará segregación a ciertos grupos sociales.
5. En el ámbito del sector público, es indispensable desarrollar un tratamiento automatizado estrictamente regulado para evitar darle al estado facultades de autoritarismo inauditas en donde se podrían limitar severamente las libertades y derechos de los ciudadanos.
6. Las plataformas que generan estos perfiles en general monetizan los datos transfiriéndolos a terceros. Aquí no existe una suerte de “cadena de custodia” que garantice hasta donde llegan esos datos.

**Subasta de perfiles digitales:** Las compañías que monetizan nuestros perfiles digitales en general los venden a empresas, dichas empresas pagan mucho dinero por ellos porque así se pueden crear ofertas de publicidad personalizadas para cada usuario, maximizando enormemente las ganancias.

El perfil digital en constante transformación, basado en datos y metadatos, sustenta predicciones sobre el consumo que se venden al mejor postor. Los porcentajes de acierto de las predicciones en cada persona son útiles para que las empresas inviertan y logren llegar con mensajes cada vez más personalizados. En la subasta de perfiles, suele darse la vulneración más notoria a los derechos de los titulares de los datos personales, ya que, ni siquiera se solicita su consentimiento o se les brinda información en este aspecto.

**Consentimiento:** De todo lo anterior surge la pregunta de si es siempre necesario el consentimiento de la persona para adquirir sus datos, consideramos que siempre será necesario el consentimiento salvo los casos donde:

* Los datos fueron obtenidos de fuentes de acceso público, por ejemplo, la central de deudores.
* Los datos están en listados que se limitan a nombres, documento de identidad identificación tributaria y domicilio.
* Los datos fueron tomados para el ejercicio de funciones propias de los poderes del estado o por una obligación legal.

**Anonimización de los Datos:** Es el proceso de convertir los datos personales de un individuo a una forma en la que no se pueda identificar a los individuos, de este modo se conforma una herramienta para mitigar los riesgos que presenta la obtención masiva de datos personales.

**Orientaciones acerca de los procedimientos de anonimización de datos:** En el proceso de anonimización se deberá producir la ruptura de la cadena de identificación de las personas. Esta cadena se compone de microdatos o datos de identificación directa y de datos de identificación indirecta. Será necesario prever las consecuencias de una eventual re-identificación de las personas que pudiera generar un perjuicio o merma de sus derechos. Igualmente será necesario prever una hipotética pérdida de información por negligencia del personal implicado, por falta de una política de anonimización adecuada o por una revelación de secreto intencionada que diera lugar a la pérdida de las variables de identificación o claves de identificación de las personas.

Luego, es interesante seguir una serie de principios orientativos al realizar este proceso:

1. El proceso de anonimización debe siempre ser proactivo y no reactivo. Es decir, debemos trabajar sobre lo que podría pasar y no simplemente reaccionar sobre las vulneraciones que hayan pasado.
2. Privacidad por defecto. El primer requisito conceptual en el diseño de un sistema de información será garantizar la confidencialidad de los interesados. Por lo tanto, conviene que desde el inicio se salvaguarde su privacidad.
3. Principio de plena funcionalidad. Desde el inicio del diseño del sistema de información se tendrá en cuenta la utilidad final de los datos anonimizados, garantizando así en la medida de lo posible que los datos finales sean útiles a la labor.
4. Principio de privacidad en el ciclo de vida de la información. Las medidas que garantizan la privacidad de los interesados son aplicables durante el ciclo completo de la vida de la información partiendo de la información sin anonimizar.
5. Informar y formar. Durante el ciclo de vida de la información, todo el personal con acceso a los datos anonimizados o no anonimizados será convenientemente formado e informado acerca de sus obligaciones.

Conviene además que en los procesos de anonimización sean definidas las funciones necesarias y el detalle del alcance de cada uno de los perfiles que pudieran finalmente designarse con relación a las mismas. Es recomendable que se garantice, en la medida posible, que cada uno de los actores obre en el ámbito de su competencia con independencia del resto de los actores. Luego, siempre que sea posible, se tratara d evitar que la misma persona pueda implicarse en varios perfiles o funciones diferentes.

Al finalizar la anonimización, conviene realizar un análisis de riesgos del proceso de anonimización para posteriormente gestionar los riesgos resultantes con medidas técnicas, organizativas o de cualquier otra índole.

**Profundizando conceptos y técnicas de la IA. Vinculación con los datos**

**¿Qué es un Algoritmo?** Es un conjunto de instrucciones y reglas definidas, las cuales deben ser, no ambiguas, ordenadas y finitas; que permite típicamente ejecutar una tarea. Dando un estado inicial y una entrada, y siguiendo los pasos sucesivos, se llega a un estado final y se obtiene una solución.

Un algoritmo tiene que ser preciso y debe definir tres partes: entrada, proceso y salida. Algunos ejemplos de algoritmos cotidianos son los de reconocimiento facial en los teléfonos móviles, los detectores de patentes, los algoritmos de los cajeros automáticos y otros más.

**Técnicas actuales de IA:** La IA actual es una aplicación de diversas teorías matemáticas, lingüísticas, psicológicas, filosóficas, de la física y la ingeniería. Su núcleo es tanto la ciencia computacional y el procesamiento digital de señales, como la estadística, el cálculo, la teoría de la probabilidad y el álgebra lineal.

Las ramas de la IA no están claramente delimitadas y se cruzan en muchas áreas. Las cuatro más comunes son el aprendizaje automático, la visión computacional, el procesamiento del lenguaje natural y la robótica. Todas ellas se encargan de tareas de percepción, es decir, de la clasificación de entidades observables (ya sea concreta o simbólicamente) en una categoría. Asimismo, se ocupan de tareas de regresión, consistentes en predecir un valor numérico que representa algo, pero en un rango infinito (precios, frecuencias, tamaños, fechas, coordenadas, etc.). Así mismo, las cuatro ramas, especialmente la robótica, se encargan de tareas de control, que es la toma de decisiones óptimas sobre acciones posibles.

En un programa tradicional, ya se conoce el proceso o algoritmo para calcular variables dependientes a partir de variables independientes. En la IA, los problemas son tan complejos y ambiguos que se sabe que debe haber una función matemática que lo pueda modelar, pero no se conoce a ciencia cierta cuál (por ejemplo, para identificar la cara de una persona). Por ende, se crea un programa genérico cuya misión es «aprender» dicha función.

**Aprendizaje Automático:** Aprender es una metáfora antropomórfica que se usa para comunicar de manera más intuitiva lo que el programa hace, pero es quizás esta palabra la que haya originado la ilusión de que este tiene una conciencia y voluntad propias.

Lo que en realidad sucede es que dado un banco de datos se aplica algún método numérico como la regresión lineal o la regresión logística para que el programa pueda aproximar una función compleja que describa un fenómeno. En el caso de la regresión logística cada unidad de trabajo se la conoce como una neurona artificial, cuando se usa más de una capa de regresión logística decimos que estamos ante una red neuronal. Si nos encontramos con más de tres capas estamos hablando de una red neuronal profunda (deep learning).

Existen varios tipos de redes neuronales, cuando el resultado de todas las regresiones logísticas de una capa, entran en la siguiente capa, hablamos de una red neuronal simple o completa. Si los resultados se agrupan tras cada capa en un numero menor de neuronas estamos ante una red neuronal convolucional. Las redes neuronales convolucionales se consideran muy útiles por su capacidad de comprimir información, no obstante entrenar la red requiere mucha información.

**Visión Computacional:** Esta rama de la IA se centra en la percepción del especto electromagnético (luz visible, ondas de radio, radar, etc). Aquí las redes neuronales tienen diversas arquitecturas y número de neuronas que les permiten ser optimizadas para distintos tipos de tareas. A dichas características se las conoce como hiperparámetros.

Algunas de las tareas que realiza esta área de la IA son las siguientes:

* Reconocimiento facial.
* Detección de objetos.
* Clasificación de imágenes.
* Búsqueda por imagen.
* Etc.

Otra arquitectura que vale la pena mencionar son las redes siamesas las cuales funcionan cuando no es posible entrenar a una red neuronal ajustando en función de las salidas correspondientes, como puede ser en el caso del reconocimiento facial, donde no podemos saber de antemano el valor de la variable dependiente (a menos que tengamos un campo de datos enorme).

Aquí las redes neuronales siamesas toman dos entradas que se quieran comparar y aprenden una función de similitud generalizada, que puede ser utilizada para comparar objetos o personas no vistos anteriormente con un sólo ejemplo.

**Procesamiento de lenguaje Natural:** También nos encontramos en este universo de la IA con el procesamiento de lenguaje natural, un área en la que se busca el entendimiento, clasificación y escritura de lenguajes humanos. Esto es especialmente útil en herramientas de traducción automática, clasificación y generación de texto, resúmenes de texto, etc.

Aquí son populares los modelos secuencia a secuencia (seq2seq), que son esencialmente autocodificadores que codifican el idioma original a un vector intermedio y luego lo decodifican a un idioma objetivo.

**Robótica:** Por último, el aprendizaje por refuerzo es la técnica que ha dado los resultados más alucinantes de la IA, particularmente por las posibilidades que la robótica ofrece.

A diferencia del aprendizaje supervisado y no supervisado, el aprendizaje por refuerzo no se basa en un conjunto de datos predefinido. Sino que se funda en la interacción del algoritmo con un contexto. Este último puede ser virtual o natural y se le llama ambiente (environment).

El algoritmo, en este caso llamado agente (agent), observa el entorno mediante, por ejemplo, un extractor de características convolucional. En cada momento, se encuentra en un estado determinado (número de vidas, posición en el ambiente, puntuación) y debe llegar a otro. Para ello, puede ejecutar un conjunto de acciones (moverse, recoger algo, disparar, saltar). El entrenamiento consiste en pasar por diferentes «episodios», en los que comienza en un estado inicial y busca llegar a un estado final, siguiendo la secuencia de acciones que maximice o minimice una penalización o recompensa (el equivalente a la función de costo). La estrategia para lograrlo se llama política (policy).

Otra diferencia es que el supervisado y no supervisado dependen fuertemente de un historial de observaciones, mientras que el aprendizaje por refuerzo se ocupa de procesos “macrobianos”. En estos, solo se toma en cuenta el momento presente y lo que la política indique que es la opción que más probablemente acercará al agente al estado final. Por ello, puede abordar situaciones sui generis con más éxito que los otros.

**Relación entre Data Science y Machine Learning:** La “Data Science” es una disciplina que se encarga del trabajo y estandarización de grandes volúmenes de datos, mientras que el machine learning es una disciplina encargada de trabajar con algoritmos de análisis, los cuales en general se encargarán luego de analizar los datos en busca de patrones.

Es decir, mientras el primero se encarga del conjunto de los datos, el segundo se encarga del análisis de los mismos. El Machine Learning es utilizado en el Data Science para poder analizar datos de manera automatizada, detectar patrones y así generar perfiles digitales.

**La ética en el Ámbito de la IA:** Debido a los grandes alcances que el aprendizaje automático y los algoritmos “inteligentes” tienen, podemos generar una infinidad de redes neuronales que puedan responder de manera asertiva a infinidad de situaciones. Tanto así que en muchos casos las máquinasdemuestran sobrepasar a la capacidad humana en el reconocimiento de patrones o en la generación de perfiles.

Lo anterior genera una discusión ética acerca del alcance que estas inteligencias puedan tener y sobre todo actualmente está sentada socialmente la petición de que las empresas que las administran blanqueen los procesos computacionales que sus máquinas utilizan.

El problema aquí es que en una red neuronal no estamos programando las soluciones para implementarlas luego, sino que estamos dejando que la máquina ajuste los parámetros de salida a fuerza de ensayo y error hasta refinar el algoritmo. Por lo que la máquina en realidad no posee un algoritmo claro.

La situación se agrava mucho más cuando empleamos redes neuronales con muchas capas de abstracción (deep learning), ya que hasta para los ingenieros de software les resulta imposible seguir un patrón lógico y recrear el algoritmo que la máquina está generando. De hecho, el programa computacional es simplemente una secuencia de comandos que se refinan indefinidamente a fuerza de introducirle una ingente cantidad de datos. Por lo que ni siquiera tiene noción de si, o puede “aprender” realmente. La IA solo puede contestar asertivamente a las preguntas para las que se haya entrenado.

¿Queremos tener siempre una explicación exacta de que es lo que la máquina realiza, o queremos simplemente tener la certeza de que, para ciertas entradas, las respuestas serán asertivas? La máquina no tiene conciencia y trabaja de manera simbólica haciendo simples operaciones lógicas.

**Ciclo de vida de la IA:** El ciclo de vida de un sistema de inteligencia artificial, es similar al ciclo de vida de cualquier software en general. De este modo el mismo abarca las fases de *desarrollo* (incluidas las tareas de investigación, diseño, provisión de datos y realización de ensayos limitados), *despliegue* (incluida la aplicación) y al final la *utilización* de dicho sistema.

**Auditabilidad:** Es la capacidad de un sistema de IA de someterse a la evaluación de sus algoritmos, datos y procesos de diseño. Las auditorias pueden ser internas a la empresa que administra la IA, para corroborar detalles de diseño, rendimiento, fiabilidad del código, etc. Luego, también pueden existir auditores independientes, los cuales juegan un papel crucial en aplicaciones de IA en las que los derechos fundamentales se encuentran en juego.

La auditabilidad resulta tan importante hoy en día, que incluso la Comisión Europea habla de que los centros de ensayo deben facilitar la auditoría y evaluación independientes de los sistemas de IA, para promover la excelencia y la confianza en ellos. No obstante, lo anterior no implica necesariamente que deba disponerse siempre y de forma inmediata la información sobre los modelos de negocio y la propiedad intelectual de dicho sistema a cualquier persona.

**Conceptos de IA:**

* **Sesgo:** Es cualquier inclinación del algoritmo que favorezca o perjudica a una persona, objeto, posición o resultado. Es importante trabajar sobre estos sesgos ya que en algunos casos pueden dar lugar a resultados injustos. Los sesgos pueden surgir de la recogida de datos o provenir de la lógica del programa como consecuencia de la propia visión del programador.
* **Ética:** Es una disciplina académica que constituye un subcampo de la filosofía. En aplicaciones de la IA donde trabajamos con datos personales se torna importante analizar esta área. Luego, una IA Ética, será aquel sistema cuyo desarrollo, despliegue y uso garantice el cumplimiento de las normas éticas y los derechos fundamentales, así como aquellos específicos del contexto asociado.
* **Reproducibilidad:** Es un concepto que describe si un experimento con IA muestra el mismo comportamiento cuando se repite varias veces en las mismas condiciones. También hace referencia a la existencia de información necesaria y acceso a datos para reproducir un comportamiento.
* **IA Robusta:** La solidez de un sistema abarca tanto su solidez técnica, así como el punto de vista social (que la IA tenga debidamente en cuenta el contexto y entorno en el que opera). Esto es muy importante porque garantiza que el sistema no provoque daños involuntarios.
* **Trazabilidad:** Se refiere a la capacidad de un sistema de llevar a cabo un seguimiento de los datos, el desarrollo y el proceso de despliegue del sistema, en general mediante identificaciones, ficheros y registros. Además, este concepto habla de trazar de forma específica lo que el sistema debe hacer, y bajo que criterios, de modo que la máquina pueda dar resultados asertivos y nosotros, los programadores, podamos explicar de alguna forma, porque la máquina infiere un resultado (para esto último debemos recordar que la máquina simplemente se dedica a correlacionar, no entiende que es lo que está correlacionando).
* **Confianza:** Cuando hablamos de confianza hablamos de benevolencia, competencia profesional, credibilidad, integridad, previsibilidad, etc. En el ámbito de la IA se enfatiza en la importancia de confiar no solo en que los sistemas sean sólidos, robustos y cumplan los principios éticos. Sino también se habla de que todas las personas involucradas en los procesos de lA sean confiables.

**IA Fiable:** Luego, una IA que sea fiable debe cumplir con tres puntos principales, el sistema debe ser lícito (debe respetar las leyes), debe ser ético, y debe ser robusto. Asimismo, los desarrolladores tendrán que esforzarse principalmente por reducir en la medida de lo posible todos los sesgos que existan en su sistema de IA.

**Cajas Negras:** Se llama caja negra a la forma de ver un sistema únicamente en función de sus entradas y salidas, sin hurgar en el funcionamiento interno del mismo. Esto no quiere decir que necesariamente los contenidos del sistema no sean accesibles, aunque el concepto se relaciona generalmente con esta idea.

**Cajas Blancas:** Es la contraparte de la anterior, es la vista de un sistema que nos da acceso total a su funcionamiento, claro está que, aunque el sistema esté abierto para todos, no necesariamente todas las personas comprenderán de buenas a primeras el funcionamiento del mismo.



**https://www.youtube.com/watch?v=PPLop4L2eGk&list=PLLssT5z\_DsK-h9vYZkQkYNWcItqhlRJLN**

**Ejemplos de Machine Learning:** <https://www.tensorflow.org/js/models>

Proyectos de Software y su Documentación:

Un proyecto de software es una secuencia de actividades únicas, complejas e interconectadas que tienen una meta o propósito y que deben completarse dentro de un tiempo y presupuesto estipulado conforme a una especificación.

¿Por qué documentar?

* La documentación es ampliamente reconocida como una componente fundamental de procesos maduros de desarrollo de todo tipo de software.
* Los proyectos de inteligencia artificial/ aprendizaje automático y ciencia de datos son casos particulares de proyectos de software.

Existe una normativa que regula las bases de calidad de un proyecto de software y es la norma ISO 9216: “Modelo de calidad de productos”.

Entre las cosas que esta norma aclara podemos resaltar:

* Es una norma de calidad internacional que se desarrollo para sentar las bases de una evaluación integral de los diversos aspectos que hacen a la calidad de productos.
* Esta informada por modelos desarrollados en los años 70’s.
* Fue aprobada en 1991, actualmente due reemplazada por la ISO/IEC25010.

Veremos ambas normas:

ISO 9126:

Calidad del software: Es el conjunto de características de un software que le confieren su aptitud para satisfacer las necesidades expresadas y las implícitas. Es decir todo producto informático debería cumplir con lo siguiente:

* Estar bien construido (buenas prácticas).
* Responder a los requerimientos del cliente, tantos explícitos e implícitos.
* Funciona de acuerdo a lo esperado.

La calidad puede analizarse en diferentes perspectivas:

* Interna: Medible a partir de las características intrínsecas, como el código fuente.
* Externa: Medible en el comportamiento del producto, como en una prueba.
* En uso: Durante la utilización efectiva por parte del usuario.

El estándar ISO 9126 está compuesto por cuatro partes:

Modelo de Calidad: La norma ISO/IEC 9126 define un modelo de calidad de software con seis áreas principales a abarcar. Las cuales serían:

* Funcionalidad: Se define la funcionalidad de un producto informático como el conjunto de atributos que se relacionan con la existencia de un conjunto de funciones y sus propiedades específicas. Las funciones son aquellas que satisfacen las necesidades implícitas o explícitas.
* Fiabilidad “Un conjunto de atributos relacionados con la capacidad del software de mantener su nivel de prestación bajo condiciones establecidas durante un período establecido.”
* Usabilidad “Un conjunto de atributos relacionados con el esfuerzo necesitado para el uso, y en la valoración individual de tal uso, por un establecido o implicado conjunto de usuarios.”
* Mantenibilidad “Conjunto de atributos relacionados con la facilidad de extender, modificar o corregir errores en un sistema software.”
* Portabilidad “Conjunto de atributos relacionados con la capacidad de un sistema software para ser transferido desde una plataforma a otra.”
  + Mantenible: Todo proyecto de software cambia constantemente para mantenerse actualizado o para solucionar algún problema “bug” que surja de su uso. Es por ello que resulta muy importante que antes que nada nuestro código debe sea de fácil mantención. Luego, un parámetro para medir esto sería ver cuanto trabajo nos implica realizar una modificación en él. Aquí también es importante recordar que es fundamental que nuestro software pueda evitar efectos inesperados debido a modificaciones sufridas Es decir: “Que si cambio algo no termine por romper todo”.

https://cs.uns.edu.ar/~virginia.cuomo/calidad-2016/downloads/CalidadSW-2016-Teoria06-ISO%209126.pdf

* Modelo de Calidad:
  + Mantenibilidad: Capacidad del producto para poder ser modificado ya sea para mantenerse actualizado como para poder modificar ciertas excepciones o “bugs”. Estabilidad: Capacidad del software para evitar efectos inesperados debido a modificaciones sufridas (si cambio algo no rompo todo). Pruebabilidad: Capacidad del producto de ser probado (testing). Aquí la documentación es muuuy importante.

Elementos esenciales de una buena documentación:

* Una breve descripción.
* Una guía de inicio para inciar el uso de la biblioteca.
* Tutoriales
* Proyectos de Muestra.
* Documentación API.
* Documentación de Arquitectura (descripción arquitectónica). Es una vista de alto nivel que nos describe como esta organizado el código en vez de como utilizarlo. Puede tener varias vistas:
  + Organización modular (vista lógica, o componentes y conectores).
  + Deployment (implementación o vista física).
  + Vistas de desarrollo (paquetes, componentes para usuarios finales).
* La documentación son realmente los planos de nuestro proyecto de software y son tan fundamentales como los planos para cualquier construcción.

¿Cómo saber si su documentación es buena? En general podemos saber si la documentación de un proyecto es buena mediante medidas objetivas: basados en tamaños, densidades, cobertura, etc. Médidas subjetivas: el feedback de los usuarios del proyecto con sus comentarios.

Hay una grave confusión que usa el manifiesto ágil para justificar la falta de documentación.

* Es decir no documentar como una forma de agilizar los procesos.
* El manifiesto ágil realmente dice que la documentacion no garantiza el éxito de un proyecto y se debe minimizar el desperdicio en documentar de más, no dice que no hay que documentar.

<https://www.sohamkamani.com/blog/how-to-write-good-documentation/>

Organización y documentación de proyectos de Machine Learning:

Usos y ejemplos de API:

API: Es una interfaz de comandos con las que me comunico con un sistema de software. Las API son mecanismos que permiten a dos componentes de software comunicarse entre sí mediante un conjunto de definiciones y protocolos.

Aprendizaje Automatizado o Machine Learning

Dentro de la Inteligencia Artificial (IA), uno de los campos más destacados es el del Aprendizaje Automático, más conocido como “Machine Learning”.

En su libro Sobre la inteligencia, publicado en 2004, Jeff Hawkins definía la inteligencia como la capacidad de predecir el futuro, por ejemplo, el peso de un vaso que vamos a levantar o la reacción de los demás a nuestros actos, en base a los patrones almacenados en la memoria (el marco memoria-predicción). Ese mismo principio está detrás del Machine Learning (ML), también conocido como aprendizaje automático.

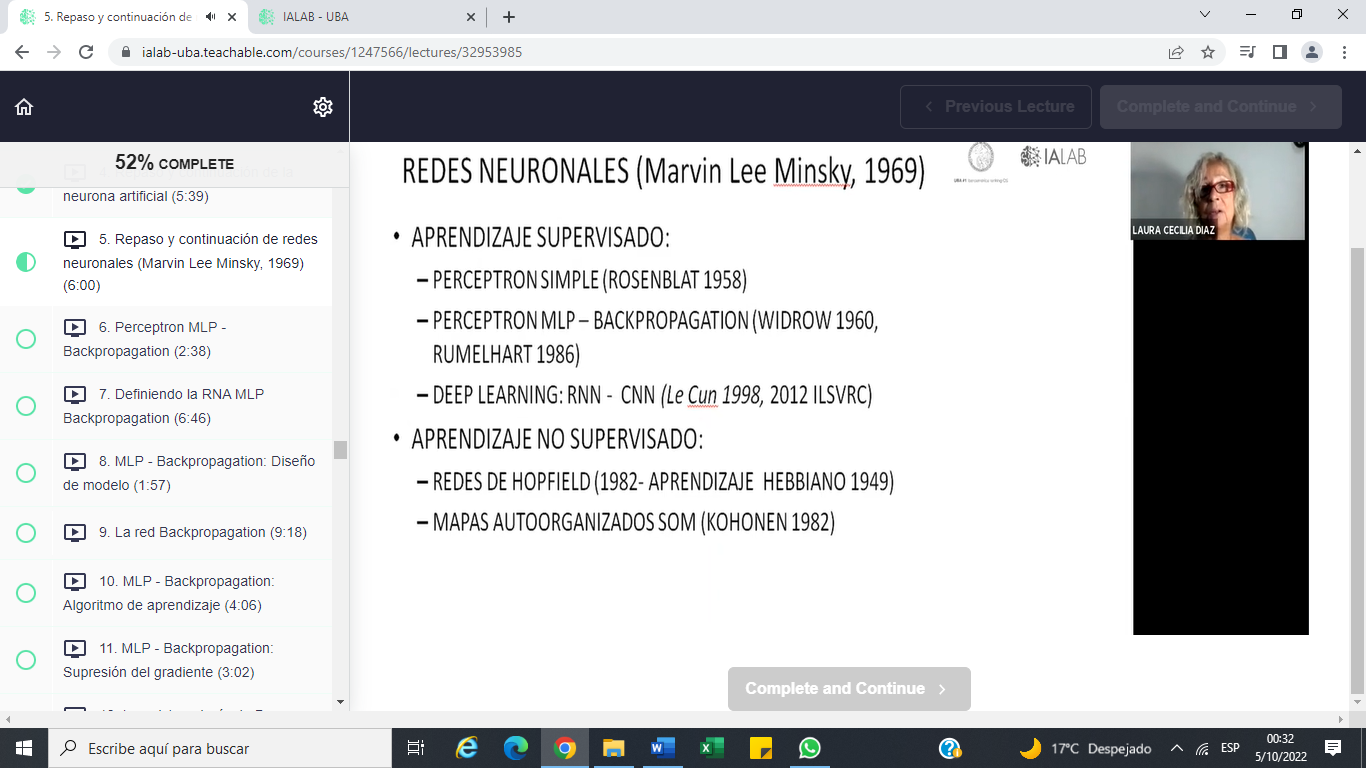
¿QUÉ ES EL 'MACHINE LEARNING' Y PARA QUÉ SIRVE?

El Machine Learning es una disciplina del campo de la Inteligencia Artificial que, a través de algoritmos, dota a los ordenadores de la capacidad de identificar patrones en datos masivos y elaborar predicciones (análisis predictivo). Este aprendizaje permite a los computadores realizar tareas específicas de forma autónoma.

El término se utilizó por primera vez en 1959. Sin embargo, ha ganado relevancia en los últimos años debido al aumento de la capacidad de computación y al boom de los datos. Las técnicas de aprendizaje automático son, de hecho, una parte fundamental del Big Data.

**Tipos de Aprendizaje Automático:**

* Supervisado: Los datos de entrada vienen etiquetados con sus correspondientes salidas. Se llama supervisado porque simula que un tutor provee los resultados correctos. La meta es que el sistema pueda reproducir un modelo que produce salidas a través de entradas. Ej: Reconocimiento de fotos de animales.
* No Supervisado: Los datos de entrenamiento no vienen asociados con resultados y por ende los algoritmos deben encontrar por si solos la estructura subyacente en los datos de entrada. La meta puede ser encontrar esta estructura en si o como paso intermedio para otros procesos.
* Aprendizaje por Refuerzo: El software interactua con un entorno dinámico en el que debe desempeñarse para alcanzar una o más metas. Recibe retroalimentación en forma de recompensas o castigos a medida que navega el espacio del problema. Ej: Vehículo autónomo, Jugador de Ajedrez.
* Aprendizaje Representacional: Apunta a entender aspectos de alto nivel a partir de los datos de entrada. A menudo se usa como parte de un preprocesamiento de los datos para evitar pasos manuales. Puede ser supervisado o no. Un ejemplo muy conocido en estadística es el Análisis de Componentes Principales.
* Aprendizaje evolutivo: No se lo considera propiamente dentro del Machine Learning pero es muy cercano en sus métodos y metas. Aplica algoritmos inspirados en dinámica de poblaciones (evolución biológica). Se evaluan los individuos en cuanto a su desempeño y solo permanecen los más aptos. Se incorporan los conceptos de mutación y cruce. Al cabo de varias generaciones se alcanza un resultado que satisface los criterios buscados.



<https://aprendeia.com/aprender-matematicas-para-machine-learning/>

Perceptrón Simple o red neuronal monocapa.

Perceptron MLP o red neuronal multicapa:

MLP Backpropagation - La red neuronal [Backpropagation](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html" \l "backpropagation) es una red neuronal [feedforward](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html" \l "feedforward) de varias [capas](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#multi-layer%20Perceptron) y es, con diferencia, la más utilizada[ [6](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/References.html#6) ]. También se considera uno de los métodos más simples y generales utilizados para [el entrenamiento supervisado](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#supervised%20learning) de redes neuronales multicapa [ [6](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/References.html#6) ]. Backpropagation funciona aproximando la relación no lineal entre la [entrada](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#input) y la [salida](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#output) ajustando los valores de [peso](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#weight) internamente. Puede generalizarse aún más para la entrada que no está incluida en los [patrones de entrenamiento](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#training%20patterns) (habilidades predictivas).

Generalmente, la red Backpropagation tiene dos etapas, entrenamiento y [prueba](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#testing) . Durante la fase de entrenamiento, a la red se le "muestran" entradas de muestra y las clasificaciones correctas. Por ejemplo, la entrada podría ser una imagen codificada de una cara y la salida podría estar representada por un código que corresponde al nombre de la persona.

Una nota adicional sobre la codificación de información: una red neuronal, como la mayoría de [los algoritmos de aprendizaje](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#learning%20algorithm) , necesita tener las entradas y salidas codificadas de acuerdo con un esquema arbitrario definido por el usuario. El esquema definirá la arquitectura de la red de modo que una vez que se entrena una red, el esquema no se puede cambiar sin crear una red totalmente nueva. Del mismo modo, existen muchas formas de codificar la respuesta de la red.

La siguiente [figura](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/BackPropagation.html#Figure%205) muestra la [topología](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#topology) de la red neuronal Backpropagation que incluye una capa de [entrada](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#input%20layer) , una [capa oculta](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#hidden%20layer) y una [capa de salida](https://www.cse.unsw.edu.au/~cs9417ml/MLP2/Glossary.html#output%20layer) . Cabe señalar que las redes neuronales Backpropagation pueden tener más de una capa oculta.

<https://www.diegocalvo.es/funcion-de-activacion-redes-neuronales/>

<https://bootcampai.medium.com/redes-neuronales-13349dd1a5bb#:~:text=Funciones%20de%20activaci%C3%B3n,que%20permitir%C3%A1%20reconstruir%20o%20predecir>.

<https://es.acervolima.com/funciones-de-activacion-en-redes-neuronales/>

<https://www.ibm.com/cloud/learn/recurrent-neural-networks>

Regresión Lineal.

Regresion lineal multiple.

Regresión Polinomial.

Regresión logística.

Arboles de decisión.

Bosques aleatorios de decisión.

Aprendizaje Supervisado:

* Perceptrón Simple.
* Perceptrón Multicapa (MLP).
* Descenso por el gradiente.
* Backpropagation.
* Usos para Regresión y Clasificación.
* Redes Neuronales Convolucionales (CNN).
* Redes Neuronales Recurrentes (RNN).

Aprendizaje No Supervisado:

Redes de Hopfield.

Redes de Boltzmann (redes recurrentes).

Restricted Boltzmann machines.

SVM.

Sesgo, varianza, under & overfitting.

K-means, PCA, SOM & RBM.

Lasso y Ridge.

Lasso y Ridge en regresión lineal.

RNA 🡪 RBM

Clustering.

Clustering con K-Means.