

TP Inicial - Aplicación de la Inteligencia Artificial

Investigación Inicial

Juan Bautista Dalmasso, Máximo De Michieli, Paulina Paniagua

Las inteligencias artificiales son una tecnología en auge, que permite encontrar soluciones a problemas de una manera que la programación tradicional nunca alcanzó. Más allá de los cuestionamientos éticos del uso y entrenamiento de ciertas IAs, es indiscutible que éstas son una herramienta muy poderosa cuando son utilizadas con conciencia.

De especial interés para nosotros es el uso de estas tecnologías en la etapa de onboarding de nuevos clientes de manera automatizada. A su vez, este proceso requiere la recopilación, análisis y verificación de datos de dichos clientes, por lo cual también nos interesa el área de biometría y análisis de documentos de identidad.

Por eso, en este documento compartimos nuestra investigación sobre los temas de interés. Además, detallamos las herramientas que utilizaremos para el desarrollo de un proyecto que busca demostrar el conocimiento recopilado y su aplicación. Para este proyecto hemos ideado el siguiente escenario:

“Se solicita la realización de una aplicación móvil para la Biblioteca Skynet, la cuál busca acercar libros a su comunidad de manera gratuita a la vez que encuentra formas de mantenerse financiada.

Se deberá realizar un software que demuestre lo “moderna” que es la biblioteca. Con una inteligencia artificial que conteste preguntas sobre el funcionamiento de la misma y ayude a tramitar un carnet de biblioteca, así como solicitar autenticación mediante huellas digitales.”

Aplicaciones IA en el onboarding

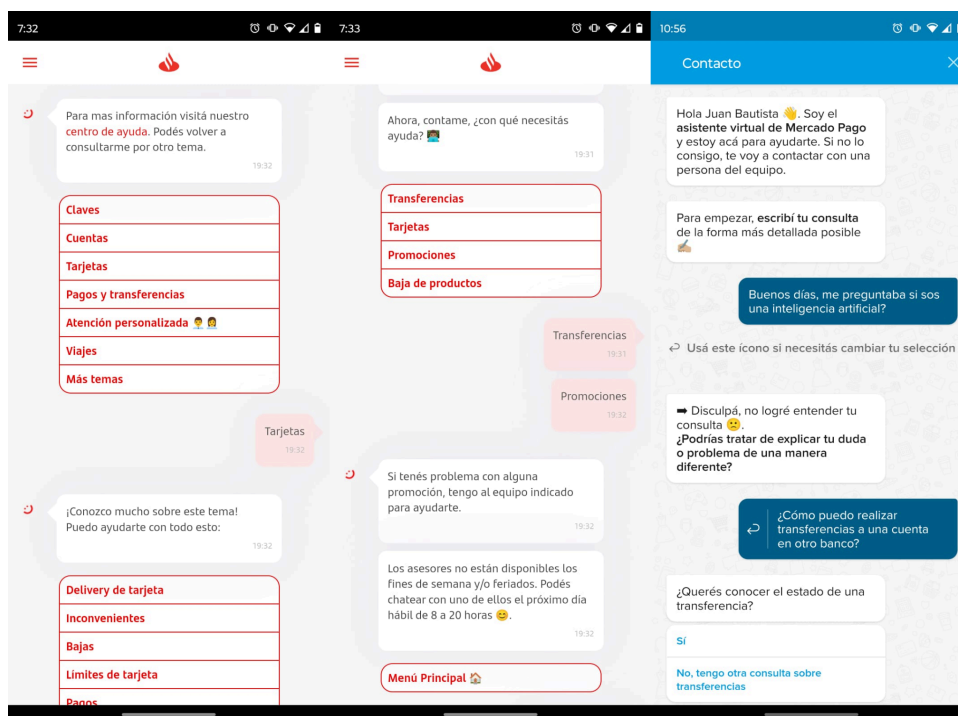
El proceso de **client onboarding** consiste en **introducir a nuevos clientes** a la funcionalidad de tu negocio. Además, durante esta etapa se debe **obtener la información necesaria** para que el cliente opere dentro de dicho negocio. Por ejemplo, un servicio de streaming on demand podría pedir los datos de tu tarjeta de crédito para cobrar la suscripción, un servicio de turnos médicos podría pedir tu dni y obra social o prepaga y, en general, plataformas online suelen requerir que los clientes se registren con un usuario y contraseña.

Utilizar estrategias de onboarding automatizado proveen la ventaja de ofrecer **atención inmediata a cualquier horario**. Sin embargo, ante ciertas dudas o consultas específicas de los clientes estos pueden no tener las respuestas buscadas y causarle frustración al cliente. Esto se debe a que el acto de hablar con una “máquina” la cuál está limitada en el rango de sus respuestas puede provocar que el cliente sienta que el negocio no lo valora lo suficiente como para proveer un ayudante humano.

Dentro de las estrategias de onboarding automatizado nos centraremos en los **chatbots**. Estos son sistemas que buscan entablar un símil de conversación con el cliente, respondiendo dudas y consultando datos.

Se pueden identificar varios tipos distintos de chatbots. Los más comunes son los que buscan funcionar como contestadores de **FAQ** (preguntas frecuentes). Pueden ser un simple menú con opciones de conversación o incorporar IA para simular una conversación más natural.

A continuación mostramos un ejemplo de dos asistentes virtuales que nos podrían resultar cotidianos, el de Santander y el de Mercado Pago.



En este caso podemos ver que el asistente de Santander utiliza un “dumb chatbot”, este ofrece una lista de opciones de diálogo fijas y el usuario no tiene la oportunidad de ingresar una pregunta personalizada. Además, llegado a cierto punto de la conversación el chatbot concluye que es mejor transferir al usuario a una conversación con un asesor humano. Sin embargo, en este caso la consulta fue realizada durante un fin de semana cuando los asesores humanos no estaban disponibles. Podríamos considerar que se desperdició una de las ventajas de la atención automatizada, la disponibilidad horaria completa.

En contraste, el asistente de Mercado Pago parece estar utilizando o una Inteligencia Artificial o un mecanismo de “word-spotting”, que en este caso detectó la palabra clave “transferencia”. Sin embargo, podemos ver que si bien la consulta estaba relacionada con “transferencias”, la duda precisa era otra. Además, llegado a cierto punto de la conversación, el chatbot de Mercado Pago decide limitar el rango de consultas del usuario, convirtiéndose en un dumb chatbot similar al de Santander.

Ahora, teniendo en cuenta que la inteligencia artificial está en auge, ¿Por qué estas dos grandes empresas no la aplican a sus chatbots? Analicemos cómo funcionan las IAs para luego entender sus ventajas y desventajas.

Funcionamiento (básico) de las IA

En la actualidad, con el auge de aplicaciones como ChatGPT, solemos pensar en sistemas que utilizan Machine Learning o Deep Learning, especialmente este último con su uso de “redes neuronales”.

La programación tradicional requiere que el programador defina los mecanismos precisos por los cuales se operará sobre los inputs para producir ciertos outputs. En cambio, las IA requieren un proceso de entrenamiento. Durante esta etapa se les provee un subconjunto de pares input/output (en el caso del entrenamiento supervisado). De esta manera, el sistema ajusta valores internos ocultos que les permiten relacionar futuros inputs a sus outputs esperados.

Ventajas y desventajas de las IA

El caso de uso ideal de una IA es aquel en el cual su entrenamiento les permite responder de manera precisa a un gran rango de inputs futuros que no estaban presentes durante el entrenamiento inicial.

Sin embargo, aquí también aparece nuestra primera desventaja. Para entrenar una inteligencia artificial se requiere una gran cantidad de información de calidad. Es decir, pares input/output que se consideren válidos. ¿Qué significa esto para una empresa que busca instalar un chatbot de IA en su negocio? Tengamos en cuenta que cada negocio tiene su propia *business logic* única. Por lo tanto, no es posible “empaquetar” una IA que le sirva a todos los negocios. Cada uno tendrá que recopilar una gran cantidad de datos específicos a sus casos de uso para poder entrenar una inteligencia que le sea útil.

¿Cómo puede recopilar un negocio toda esta información? Crearla manualmente mediante humanos puede ser un proceso tedioso, en el cual se tendría que tener en cuenta todos los tipos de consulta posible que un usuario podría tener y realizar varios casos distintos para cada una. Si la empresa ya tiene un chat de onboarding gestionado por humanos, se podrían tomar datos de este para entrenar a una IA, pero incluso este

acercamiento puede quedarse corto en el rango de consultas realizadas, además de ser potencialmente imposible por cuestiones legales.

¿Qué aprendimos de todo esto? Los mecanismos de entrenamiento de IAs pueden resultar inviables para empresas debido a la no disponibilidad de datos específicos a su *business logic*.

Pero las desventajas pueden ir más allá, las inteligencias artificiales supuestamente más avanzadas (como ChatGPT) son propensas a “alucinaciones”. En otras palabras, estas buscan imitar la manera en la que las conversaciones humanas se ven, sin llegar a entender el significado de estas. El problema sucede cuando en su intento de otorgar cualquier respuesta con tal de mantener la apariencia de una conversación normal, estas proveen información falsa o engañosa.

Un ejemplo de un chatbot potenciado por inteligencia artificial fallando y costando dinero a su empresa es el de AirCanada. En el 2022 Jake Moffat se contactó con el chatbot de la empresa para consultar por un “descuento por duelo” (bereavement fare), ya que requería un ticket de avión para asistir al funeral de un familiar. El chatbot le indicó que podía comprar un ticket y luego pedir una devolución dentro de los 90 días de realizada. Sin embargo, cuando Jake se contactó posteriormente con la empresa para solicitar su devolución, le informaron que esta debía ser realizada antes de comprar el ticket. El tribunal canadiense concluyó en que el chatbot de la empresa había proveído información engañosa y AirCanada se vió obligada a compensar a Moffat por el valor completo del ticket más los costos del juicio.

Aplicaciones de IA en la vida cotidiana

Cuando pensamos en la manera en la que las Inteligencias Artificiales afectan a nuestra vida cotidiana, quizás el ejemplo más obvio e influyente es el de los algoritmos de las redes sociales. Estos “algoritmos” son entrenados con la información de millones de usuarios, y buscan recomendar contenido personalizado a cada uno de ellos para generar la mayor cantidad de “engagement” posible. Es evidente que en la actualidad su accionar es central en la manera en la que nuestra sociedad y nuestra cultura opera.

De la mano con los algoritmos de recomendación de las RRSS, están los algoritmos de recomendación de anuncios. Los algoritmos de redes sociales buscan capturar la atención de los usuarios por la mayor cantidad de tiempo posible, a su vez recopilan información sobre los gustos de estos la cual puede ser usada para recomendar propagandas de manera “personalizada”. La tan conocida Big Data es un negocio billonario que se centra en recopilar información de nuestras vidas cotidianas, y las inteligencias artificiales resultan una herramienta ideal para procesarla.

Desde un punto de vista más positivo, tecnologías como ChatGPT con la capacidad de recopilar una muy vasta librería de conocimiento humano tienen la capacidad de identificar preguntas completamente nuevas y únicas y proveer respuestas a estas (cuando no sufren de las ya mencionadas alucinaciones).

Las inteligencias artificiales también pueden ser utilizadas para aplicaciones médicas. Estas pueden ser entrenadas con vastos repositorios de registros médicos lo cual les permite identificar enfermedades e incluso predecir la probabilidad de contraerlas basándose en patrones genéticos.

Por supuesto, las IA son una tecnología en auge y las empresas las ponen en uso cada vez más en todos los rincones de nuestra vida cotidiana posible. Un ejemplo común es su uso en el filtrado de correo basura o “spam”. Las Inteligencias Artificiales resultan

perfectas para este trabajo, por su capacidad para entrenarse con grandes cantidades de estos correos y encontrar patrones únicos que los identifican.

Aplicaciones de IA en las empresas

Más allá del uso de chatbots de cara al público, las IA pueden instalarse en un gran rango de los procesos internos de las empresas. Un ejemplo de esto es el de **Edenor**, mediante el uso de inteligencias artificiales la empresa de electricidad argentina puede detectar fallos en su red, previniendo y aliviando cortes de luz.

También la empresa **Prosegur Alarms Argentina** implementó en 2021 el uso de IAs a su servicio de vigilancia remota. Esto les permite analizar datos de un gran número de cámaras simultáneamente y en tiempo real para detectar “situaciones anómalas”.

El banco **BBVA** también ha incorporado las capacidades de la inteligencia artificial en su sistema de detección de fraudes y de análisis de incidentes.

Análisis de un Documento de Identidad

El análisis de un documento de identidad es un componente esencial del proceso de onboarding digital. Este proceso implica la verificación y autenticación de la identidad del usuario a través de la inspección de documentos emitidos por autoridades gubernamentales, como pasaportes, tarjetas de identificación nacionales o licencias de conducir.

El análisis de un documento de identidad implica varios pasos:

1. **Captura de Imágenes:** El usuario proporciona imágenes del documento de identidad mediante la cámara de su dispositivo o carga imágenes escaneadas.
2. **Extracción de Datos:** Se utilizan algoritmos de reconocimiento óptico de caracteres (OCR) para extraer información relevante del documento, como el nombre, la fecha de nacimiento, el número de identificación y la fecha de vencimiento.
3. **Validación de la autenticidad:** Se aplican técnicas de verificación para determinar la autenticidad del documento. Esto puede incluir la detección de marcas de agua, hologramas, características de seguridad específicas del documento y comparación con bases de datos gubernamentales.
4. **Comprobación de integridad:** Se analizan la calidad de la imagen y la integridad del documento para detectar posibles signos de manipulación o falsificación.
5. **Comparación Facial:** En algunos casos, se puede requerir que el usuario proporcione una selfie para compararla con la fotografía presente en el documento de identidad. Esto ayuda a garantizar que la persona que está solicitando el servicio sea la misma que aparece en el documento.

En resumen, el análisis de un documento de identidad durante el proceso de onboarding digital es fundamental para verificar la identidad del usuario de manera segura y confiable.

Biometría

La biometría es una tecnología que utiliza características físicas o comportamentales únicas de un individuo para verificar su identidad. En el contexto del onboarding digital, la biometría

desempeña un papel crucial en la autenticación y verificación de la identidad de los usuarios.

Existen varios tipos de biometría utilizados en el proceso de onboarding digital:

- **Reconocimiento facial:** Esta técnica utiliza características faciales únicas, como la forma de la cara, el tamaño de los ojos y la distancia entre ellos, para identificar a un individuo. Se capturan imágenes faciales durante el proceso de registro y se comparan con imágenes previamente almacenadas o con una selfie proporcionada por el usuario en tiempo real.
- **Reconocimiento de huellas dactilares:** Las huellas dactilares son únicas para cada individuo y se utilizan ampliamente en aplicaciones de autenticación biométrica. Durante el proceso de onboarding, se capturan imágenes de las huellas dactilares del usuario y se comparan con las huellas almacenadas en una base de datos para verificar su identidad.
- **Reconocimiento de iris:** El iris del ojo tiene patrones únicos que se pueden utilizar para la identificación biométrica. Se capturan imágenes del iris durante el proceso de registro y se comparan con imágenes previamente almacenadas para verificar la identidad del usuario.
- **Reconocimiento de voz:** La voz de una persona también puede ser única y se puede utilizar para la autenticación biométrica. Durante el proceso de onboarding, se capturan muestras de la voz del usuario y se comparan con grabaciones de voz previamente almacenadas para verificar su identidad.

La biometría proporciona un nivel adicional de seguridad y precisión en el proceso de onboarding digital al garantizar que solo los usuarios autorizados puedan acceder a los servicios. Sin embargo, es importante abordar preocupaciones relacionadas con la privacidad y la protección de datos al implementar estas tecnologías.

Listas AML (Anti Money Laundering)

El proceso de Onboarding Digital implica la verificación de la identidad de los clientes de manera remota, y una de las medidas utilizadas es la consulta de listas AML (Anti Money Laundering), herramientas fundamentales para prevenir el lavado de dinero y otras actividades financieras ilícitas.

Estas listas contienen información sobre individuos o entidades relacionadas con actividades sospechosas, como fraude, blanqueo de capitales, financiación del terrorismo, entre otros.

Las Listas AML generalmente incluyen la siguiente información:

- **Nombre completo:** De la persona o entidad.
- **Alias:** Si la persona o entidad tiene otros nombres conocidos.
- **Fecha de nacimiento:** Si se conoce, para las personas.
- **Nacionalidad:** De la persona o entidad.
- **Ubicación:** Donde se encuentra la persona o entidad.
- **Razón de la inclusión:** Por qué la persona o entidad fue incluida en la lista.
- **Fecha de inclusión:** Fecha en la que la persona o entidad fue incluida en la lista.

- **Información adicional:** Puede incluir detalles sobre las actividades delictivas de la persona o entidad, sus asociados y sus redes.

Las Listas AML pueden ser nacionales, las cuales son elaboradas por cada país y contienen información sobre personas y entidades nacionales o Listas internacionales, aquellas que son elaboradas por organismos internacionales como el Grupo de Acción Financiera Internacional (GAFI) y contienen información sobre personas y entidades de todo el mundo.

Al contrastar la identidad extraída durante el proceso de Onboarding Digital con estas listas, las empresas pueden asegurarse de no involucrarse con clientes o transacciones fraudulentas. La integración de esta verificación en el proceso digital permite cumplir con regulaciones financieras y garantizar la seguridad en las operaciones comerciales.

En el Onboarding Digital las listas AML funcionan a través de la recopilación de datos, verificación de la identidad, Comprobación de listas AML y toma de decisiones. Durante el proceso de Onboarding Digital, se recopilan datos del cliente, como su nombre completo, dirección, número de identificación y datos bancarios. Los datos del cliente se verifican con una base de datos de identidad confiable, como una base de datos gubernamental o un proveedor de servicios de verificación de identidad. Luego esos datos se comparan con las listas AML para determinar si existe alguna coincidencia.

Si el cliente coincide con una lista AML, la empresa puede tomar medidas adicionales, como solicitar información adicional, realizar una investigación más profunda o incluso rechazar la solicitud del cliente.

Utilizar las listas AML en el Onboarding Digital brindan mayor seguridad, ya que ayudan a proteger a las empresas del riesgo de ser utilizadas para el lavado de dinero o el financiamiento del terrorismo, ayuda a las empresas a cumplir con las regulaciones AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism), promueve la eficiencia al automatizar el proceso de verificación de riesgos, por lo que puede ahorrar tiempo y dinero a las empresas y, además, mejora la experiencia de los clientes ya que pueden ayudar a las empresas a ofrecer una experiencia de Onboarding Digital más rápida y eficiente para los clientes de bajo riesgo.

Sin embargo, la utilización de listas de AML puede plantear desafíos significativos. Los falsos positivos, por ejemplo, pueden llevar a la exclusión de individuos legítimos de los servicios financieros debido a coincidencias erróneas. Además, la falta de precisión en estas listas y los costos asociados con su implementación y mantenimiento también representan obstáculos importantes.

Los proveedores de listas AML (Anti Money Laundering) pueden ser entidades públicas o privadas que ofrecen información crucial para prevenir actividades financieras ilícitas. Algunos de los proveedores más reconocidos son: OFAC (Office of Foreign Assets Control), Europol, World-Check, entre otros.

Si bien Argentina no tiene proveedores directos de listas AML, la Unidad de Información Financiera (UIF) es el organismo encargado de recibir, analizar y difundir la información proveniente de las listas internacionales emitidas por el Grupo de Acción Financiera Internacional (GAFI) y elaborar y mantener Listas Nacionales de Personas y Entidades Vinculadas a Actividades de Lavado de Activos y Financiamiento del Terrorismo.

Las entidades que generalmente se ven obligadas a utilizar las Listas AML (Anti Money Laundering) en el proceso de Onboarding Digital son:

- **Entidades Financieras:** Bancos, casas de cambio, compañías financieras, etc.
- **Casinos y bingos:** Estos establecimientos deben verificar que sus clientes no figuren en las Listas AML antes de permitirles jugar.
- **Profesionales no financieros:** Abogados, contadores, inmobiliarias, etc.
- **Compañías de seguros:** Deben verificar que sus clientes no figuren en las Listas AML antes de contratar un seguro.
- **Empresas que operan con criptomonedas:** Estas empresas también deben verificar que sus clientes no figuren en las Listas AML.

La relación entre las Listas de Control Anti Money Laundering (AML) y los Chatbots se centra en la facilitación del cumplimiento normativo y la detección de actividades sospechosas.

Los Chatbots desempeñan un papel crucial en el proceso de AML al generar informes sobre la información de los clientes y guardar el comportamiento digital del usuario para recopilar evidencias. Además, los Chatbots pueden ser utilizados para la gestión de casos de alertas de blanqueo de capitales, lo que facilita la colaboración y la documentación de investigaciones.

La relación entre las Listas de Control AML y los Chatbots radica en su contribución al cumplimiento normativo y a la detección de actividades sospechosas mediante la automatización y la gestión eficiente de datos y alertas.

A través de un Chatbot, las Listas AML pueden utilizarse de varias maneras:

1. **Verificación de Clientes:** El Chatbot puede integrar las Listas AML para verificar la identidad de los clientes y asegurarse de que no estén en ninguna lista de sanciones o involucrados en actividades financieras ilícitas.
2. **Detección de Transacciones Sospechosas:** Las Listas AML pueden ayudar al Chatbot a monitorear las transacciones financieras y detectar patrones inusuales que podrían indicar actividades de lavado de dinero. Esto permite al Chatbot alertar sobre posibles transacciones sospechosas.
3. **Cumplimiento Normativo:** Al integrar las Listas AML en el Chatbot, se garantiza que la empresa cumpla con las regulaciones contra el Blanqueo de Capitales y la Financiación del Terrorismo, evitando así posibles sanciones legales y protegiendo la reputación de la empresa.

En resumen, al utilizar Listas de Control AML en un Chatbot, se garantiza la protección de datos sensibles, la autenticación segura de usuarios, el cumplimiento normativo, la detección de actividades sospechosas y la realización de pruebas de seguridad para mantener la integridad y seguridad de la interacción del chatbot con los usuarios.

Las listas de control AML pueden adaptarse a diferentes tipos de chatbots mediante la integración en plataformas específicas, la utilización de tecnologías como Machine Learning y PLN (Procesamiento de lenguajes naturales).

Normativas existentes

El marco regulatorio en el ámbito de la inteligencia artificial (IA) es crucial para asegurar un desarrollo y uso responsable de esta tecnología en la sociedad. Actualmente, existen diversas normativas técnicas y legales, así como políticas de privacidad y uso, que buscan abordar los diferentes aspectos relacionados con la IA.

En primer lugar, es importante distinguir entre las normativas técnicas y legales y las políticas de privacidad y uso de la IA. Las normativas técnicas y legales son de carácter general y obligatorio, aplicándose a todos los sistemas de IA independientemente de su aplicación específica. Estas normativas son establecidas por gobiernos u organismos internacionales y su incumplimiento puede acarrear sanciones. Por otro lado, las políticas de privacidad y uso son establecidas de manera específica y voluntaria por los desarrolladores o propietarios de sistemas de IA, y su cumplimiento generalmente no conlleva sanciones claras.

En términos generales, las normativas que una IA puede tener que cumplir pueden clasificarse en tres categorías principales:

Normativas generales: Incluyen leyes de protección de datos, responsabilidad civil y propiedad intelectual, las cuales establecen un marco legal para el tratamiento de datos personales, la responsabilidad por los daños causados por la IA y la protección de las creaciones intelectuales relacionadas con la IA, respectivamente.

Normativas específicas: Algunos países han promulgado leyes específicas sobre IA que establecen requisitos particulares para su desarrollo y uso, especialmente en sectores como la salud, las finanzas o el transporte.

Normativas técnicas: Estas consisten en estándares internacionales y nacionales para el desarrollo y uso de la IA, cubriendo aspectos como la seguridad, la ética y la calidad de la tecnología.

A nivel internacional, diversos países y organizaciones están trabajando en el desarrollo de normativas para la IA. Por ejemplo, la Unión Europea ha adoptado un Reglamento sobre la IA, mientras que la Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha establecido principios para el desarrollo responsable de la IA. En Estados Unidos y China también se están llevando a cabo iniciativas similares.

En el contexto específico de Argentina, el marco regulatorio de la IA está en evolución, actualmente solo se implementan normativas en base a la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO.

Según las “Recomendaciones para una Inteligencia Artificial Fiable” aprobada por La Subsecretaría de Tecnologías de la Información en junio de 2023, las inteligencias artificiales deben cumplir con una serie de normativas para garantizar su correcto

funcionamiento y su impacto positivo en la sociedad. Estas regulaciones abarcan varios aspectos fundamentales:

1. **Transparencia y explicabilidad:** Es crucial que la IA sea transparente en su funcionamiento y decisiones, permitiendo a los usuarios comprender su lógica y razón de ser. Si un sistema de IA causa daño, se debe poder determinar la razón de dicho fallo, promoviendo la transparencia en el uso de los datos y en las decisiones tomadas por la IA.
2. **Privacidad y seguridad de los usuarios:** La IA debe proteger los datos personales de los usuarios y ser resistente a posibles ataques cibernéticos.
3. **Equidad y no discriminación:** Los actores de la IA deben promover la diversidad, la inclusión y garantizar la justicia social, evitando la discriminación y asegurando la equidad a lo largo del ciclo de vida de los sistemas de IA.
4. **Robustez y confiabilidad:** La IA debe ser capaz de adaptarse a diferentes situaciones y entornos, así como detectar y corregir errores en su funcionamiento.
5. **Alineación con valores humanos fundamentales:** Es importante que la IA esté alineada con valores como la dignidad, la libertad y la justicia, utilizándose para promover el bien común y evitar cualquier forma de daño o discriminación.
6. **Sostenibilidad:** Es fundamental evaluar constantemente los efectos humanos, sociales, culturales, económicos y ambientales de las tecnologías de IA para garantizar su sostenibilidad a largo plazo.
7. **Supervisión y decisión humanas:** Aunque los sistemas de IA pueden ser utilizados para tomar decisiones eficientes, la responsabilidad final y la rendición de cuentas siguen recayendo en los seres humanos, quienes deben mantener el control en contextos críticos.

En Argentina, no existe una ley específica que regule la inteligencia artificial (IA) en su totalidad. Sin embargo, hay varias leyes y regulaciones que se aplican al desarrollo y uso de la IA en el país, algunas de las cuales restringen su uso:

1. Ley Nacional de Protección de Datos Personales (Ley 25.326)

Regula la recopilación, almacenamiento, tratamiento y uso de datos personales. Limita el uso de datos personales para la toma de decisiones automatizadas, especialmente aquellas que afecten los derechos de las personas. Además, exige el consentimiento de las personas para el uso de sus datos personales.

2. Ley de Defensa del Consumidor (Ley 24.240)

Protege a los consumidores de prácticas comerciales desleales, incluyendo aquellas relacionadas con la IA. Prohíbe la publicidad engañosa o discriminatoria que utilice IA. Exige que las empresas brinden información clara y precisa sobre los productos y servicios que ofrecen con IA.

3. Ley de Servicios de la Sociedad de la Información (Ley 25.506)

Regula la prestación de servicios online, incluyendo aquellos que utilizan IA. Establece responsabilidades para los proveedores de servicios de IA. Protege la privacidad y los derechos de los usuarios de servicios de IA.

4. Código Civil y Comercial de la Nación

Establece principios generales de responsabilidad civil que pueden ser aplicados a los daños causados por la IA. Regula la responsabilidad de las personas por los actos de sus

robots. Permite que las personas puedan reclamar daños y perjuicios por los daños causados por la IA.

También, existen otras leyes y regulaciones que pueden ser aplicadas a la IA de manera sectorial, como la Ley de Telecomunicaciones, la Ley de Bancos, la Ley de Mercado de Valores, etc.

Además, las IA deben cumplir con normativas específicas del sector en el que se utilizan. Por ejemplo, en el sector financiero, deben respetar las normas de la Comisión Nacional de Valores (CNV) y del Banco Central de la República Argentina (BCRA).

Es importante destacar que la interpretación y aplicación de estas leyes aún está en desarrollo. En general, las leyes argentinas que restringen a la IA también se aplican a los chatbots.

A continuación, se presentan algunos ejemplos de cómo las leyes argentinas pueden restringir a los chatbots:

- Los chatbots no pueden recopilar o procesar datos personales sin el consentimiento del usuario.
- Los chatbots no pueden utilizar datos personales para fines discriminatorios o para tomar decisiones automatizadas que afecten los derechos del usuario.
- Los chatbots no pueden brindar información falsa o engañosa a los usuarios.
- Los chatbots no pueden ser utilizados para realizar prácticas comerciales desleales.

Herramientas a utilizar

- FastAPI (Backend)
- TensorFlow (IA chatbot)
- React Native (Front end)

- **Inteligencia Artificial del Chatbot**

En este punto podemos observar dos alternativas principales. La primera es programar una IA “desde 0”, utilizando herramientas como **TensorFlow**. La segunda es aprovechar inteligencias artificiales ya existentes como **ChatGPT**.

Estas últimas ofrecen APIs que permiten la comunicación con sus chatbots preexistentes. También hay APIs de terceros que encapsulan la API original para proveer o facilitar ciertas funcionalidades. Las principales ventajas es que suelen ser “**low code**”, permitiéndonos otorgarle a la IA preexistente información de nuestro negocio en lenguaje natural. Además estos programas ya fueron entrenados con enormes datasets que les permiten imitar conversaciones humanas extremadamente bien. El problema de estas opciones es que suelen ser **pagas** o tener versiones “**freemium**” **muy limitadas**. Además, como se mencionó en el apartado anterior de ventajas y desventajas de las IA, estas pueden llegar a tener “**alucinaciones**” y proveer información errónea a los clientes.

Sobre programar y entrenar una IA de manera independiente, se nos presentan problemas diferentes. El primero es la programación en sí, herramientas como **TensorFlow** son **open source**, pero requieren un profundo entendimiento del campo de machine o deep learning. Además se nos presenta el problema de obtener un dataset capaz de entrenar a nuestra AI desde 0.

En resumen, las APIs de terceros no requieren un conocimiento profundo del campo de las IA y vienen con un cierto nivel de pre-entrenamiento, sin embargo pueden ser problemáticas en cuanto a nuestro presupuesto. Las IA programadas a mano requieren un

profundo conocimiento del campo y necesitan ser entrenadas desde 0, sin embargo, son completamente gratis al utilizar herramientas open source.

Teniendo en cuenta toda esta información, llegamos a una decisión sobre qué tipo de IA utilizar. Programaremos una IA muy simple con **TensorFlow** y Python. Esta será entrenada con diferentes frases y palabras posibles que un cliente podría utilizar, luego, podrá relacionar estas palabras clave con ciertos temas. Por ejemplo, si el usuario dice “¿Cómo puedo sacar un carnet para la biblioteca”, la IA relaciona esta consulta con el tema “Obtención de Carnet”. Una vez que sepamos sobre qué tema nos está consultando el cliente, podremos otorgar respuestas predefinidas.

Este acercamiento tiene las siguientes ventajas:

- Completamente gratis.
- Relativamente fácil de programar.
- No nos arriesgamos a que la IA otorgue respuestas falsas, ya que todas nuestras respuestas están predefinidas.
- Incluso con datasets “pequeños” podemos empezar a observar un correcto comportamiento de la IA, lo cual es ideal para una demo.