Tecnicatura Superior en Ciencia de datos e Inteligencia Artificial

PROYECTO FINAL

Integrantes del Grupo

- Calero, Juan
- Fischer, Rocío Ayelén
- Maldonado, Sabrina
- Ponce, Oscar
- Strada, Julieta

Ética y Ejercicio Profesional

- Implementación del Botón de Arrepentimiento a nivel programación y base de datos, pudiendo llevar a la práctica reemplazando días por minutos, cada grupo puede sugerir la escala.
- Explicar brevemente y de manera general, como implementarían la Ley 11.723 - Régimen Legal de la Propiedad Intelectual en el código que han desarrollado.
- Explicar brevemente y de manera general, como implementarían la Ley 25.326 Protección de los Datos Personales en la base de datos que han diseñado e implementado para el presente proyecto.
- Si SkyRoute S.R.L. implementa el desarrollo en su sucursal de España y un cliente Argentino presenta un inconveniente de seguridad que denuncia. El Convenio Internacional sobre Cibercriminalidad o convenio de Budapest, como se implementaría?
- Si se implementara Inteligencia Artificial para éste proyecto, bajo que legislación debería estar regulado y que buenas prácticas deberían implementar?

- La Ley 11.723 Régimen Legal de la Propiedad Intelectual se implementa en el proyecto desarrollado principalmente en el área de programación, es decir en el desarrollo del

código que empleamos para llevar a cabo el ABP. Es importante su aplicación ya que la misma ofrece diferentes formas de protección legal al código creado, tales como:

1. **Derechos de autor**: Protegen el código fuente como una obra intelectual, sin necesidad de registro formal.
2. **Patentes**: Aplicables a innovaciones técnicas dentro del software.
3. **Licencias**: Definen cómo terceros pueden usar el código (ejemplo: MIT, GPL, Apache).

Se puede implementar mediante **Registro de software**: Aunque no es obligatorio, registrar el código puede servir como prueba en caso de disputas. **Contratos de confidencialidad**: Evitan el uso no autorizado del código por empleados o colaboradores. **Cifrado y control de acceso**: Protege el código contra copias no autorizadas. En nuestro proyecto establecimos una Licencia de Uso del código creado, lo que permite la continuidad del servicio por parte de SkyRoute S.R.L. sin transferir la propiedad, impidiendo modificaciones y distribución sin autorización.

- La Ley 25.326 Protección de los Datos Personales se implementa en el proyecto llevado a cabo en el área y desarrollo de Base de Datos, ya que se utilizan gran cantidad de datos por los cuales se debe seguir ciertos principios y medidas de seguridad para garantizar la protección legal tales como:

1. **Diseño Seguro de la Base de Datos:** Definir tablas que almacenen datos personales de manera organizada y con restricciones adecuadas (no almacenas información sensible sin justificación). No almacenar mas datos de los necesarios para la operación del sistema.
2. **Seguridad en el Almacenamiento:** Encriptación: Usa algoritmos de cifrado para proteger datos sensibles. Control de acceso: Implementa autenticación y permisos para restringir el acceso a la información. Registro de actividad: Mantén logs de acceso y modificaciones para detectar posibles vulnerabilidades.
3. **Regirse bajo los principios que estable la ley:** *Consentimiento informado:* Solo puedes almacenar datos personales con el consentimiento del titular. *Finalidad específica:* Los datos deben ser utilizados únicamente para el propósito declarado. *Calidad de los datos:* Deben ser exactos, actualizados y pertinentes.
   Seguridad: se debe implementar medidas para evitar accesos no autorizados, pérdidas o alteraciones.
4. **Derechos de los Titulares de Datos:** *Acceso:* Permitir que los usuarios consulten qué datos se almacenan sobre ellos. *Rectificación:* Facilitar la actualización o corrección de datos incorrectos. *Supresión:* Garantizar que los usuarios puedan solicitar la eliminación de sus datos cuando corresponda.

- En el caso que la Empresa SkyRoute S.R.L. implementa el desarrollo en su sucursal de España y un cliente Argentino presenta un inconveniente de seguridad que denuncia. Se aplica el **Convenio de Budapest** que es el principal tratado internacional sobre ciberdelincuencia y cooperación en investigaciones digitales. Para su aplicación se tendrá en cuenta lo siguiente:

1. **Jurisdicción y Aplicabilidad.** Argentina y España son países adheridos al Convenio de Budapest, lo que facilita la cooperación internacional en casos de ciberdelincuencia. La denuncia del cliente argentino podría ser investigada

bajo la legislación argentina, pero si el problema se origina en la sucursal española, España también tendría competencia.

2. **<u>Procedimiento de Denuncia y Cooperación Internacional</u>.** El cliente argentino puede presentar la denuncia ante la Unidad Fiscal Especializada en Ciberdelitos en Argentina. Argentina puede solicitar asistencia a España para investigar el incidente, utilizando los mecanismos del convenio para el intercambio de información y evidencia digital. Si el caso requiere acceso a datos almacenados en servidores españoles, se puede solicitar cooperación bajo el Segundo Protocolo Adicional del Convenio de Budapest, que facilita la obtención de evidencia electrónica.
3. **<u>Responsabilidad de SkyRoute S.R.L.</u>** La empresa debe cumplir con las normativas de protección de datos y ciberseguridad en ambos países. Si se determina que hubo negligencia en la seguridad del software, podría enfrentar sanciones legales en Argentina y España.

La cooperación entre Argentina y España bajo el convenio permitiría una investigación eficiente y el acceso a pruebas digitales necesarias para esclarecer el caso.

- Aunque el proyecto actual es una aplicación de consola con base de datos relacional y no menciona IA explícitamente, si en un futuro se decidiera incorporar funcionalidades de IA (por ejemplo, para recomendaciones de destinos, optimización de precios, o detección de fraudes) se debería considerar que en Argentina, la legislación sobre IA aún está en desarrollo. Sin embargo, cualquier implementación de IA estaría sujeta a marcos legales existentes y principios éticos que están emergiendo a nivel global.

    1. **<u>Marcos legales existentes</u>**: *Ley de Protección de Datos Personales* (Ley 25.326 y su Decreto Reglamentario 1558/01): Esta es la legislación más relevante y de aplicación inmediata. Si la IA procesa datos personales (nombres, CUIT, correos electrónicos de clientes, historial de compras, etc.), debe cumplir estrictamente con los principios que consagra (licitud, seguridad, información, etc*). Código Civil y Comercial de la Nación (Ley 26.994):* Podría ser aplicable en aspectos relacionados con la responsabilidad civil por daños causados por decisiones de la IA, si estas afectaran a los usuarios. *Ley de Defensa del Consumidor (Ley 24.240)*: Si la IA interactúa directamente con los consumidores, especialmente en decisiones que afectan sus derechos (como precios, disponibilidad de vuelos o decisiones de "arrepentimiento"), deberá garantizarse la transparencia, la no discriminación y la protección contra prácticas abusivas. El "botón de arrepentimiento" es un claro ejemplo de derecho del consumidor que la IA no debería socavar.

    2. **<u>Marcos Regulatorios Globales en Desarrollo (Referencia):</u>** Aunque no son ley en Argentina, son importantes puntos de referencia y es probable que influencien futuras normativas locales como *Reglamento General de Protección de Datos (RGPD) de la Unión Europea*: Ha sentado un precedente global en protección de datos y sus principios de "privacidad por diseño" y "explicabilidad" son relevantes para la IA.

3. **Las Buenas Prácticas al Implementar IA:** *Transparencia y Explicabilidad*, los usuarios deben saber cuándo están interactuando con un sistema de IA y cómo se toman las decisiones que los afectan. *Equidad y No Discriminación*: los datos utilizados para entrenar la IA deben ser representativos y no llevar a decisiones discriminatorias. *Privacidad y Seguridad de Datos*: Recopilar solo los datos estrictamente necesarios para el funcionamiento de la IA. Implementar medidas de seguridad cibernética de primer nivel para proteger los modelos de IA y los datos que procesan de accesos no autorizados o ataques. *Responsabilidad y Supervisión Humana:* Siempre debe haber un mecanismo para que un humano revise y anule las decisiones críticas de la IA, especialmente en casos que afecten derechos o bienestar del cliente. *Fiabilidad:* Probar rigurosamente los sistemas de IA en diversas condiciones para asegurar que funcionen de manera fiable y predecible. Implementar mecanismos para manejar errores. *Comité ético:* Considerar la creación de un comité o grupo de trabajo para revisar el diseño, desarrollo y despliegue de sistemas de IA, asegurando que se adhieran a los principios éticos y legales. *Sostenibilidad Ambiental:* Considerar el impacto energético del entrenamiento y la ejecución de modelos de IA, buscando soluciones más eficientes si es posible.

En resumen, si bien el proyecto actual de SkyRoute no integra IA, es fundamental estar preparados para las implicaciones legales y éticas si se decidiera hacerlo en el futuro. La protección de datos personales, la transparencia, la equidad y la supervisión humana serían los pilares de cualquier implementación de IA responsable en un sistema como este.