TECNICATURA SUPERIOR EN

Ciencia de datos e Inteligencia Artificial

Módulo Programador – Ética y Deontología Profesional

Evidencia de Aprendizaje 3

Grupo de trabajo:

Avila, Daniela Carolina: 36706615

Fava Perez, Maria Pia: 30722626

Rivas, Mariela Yanina: 34677549

Raspanti, Gerardo: 35524770

Entregables: LINK

1. **Explicar brevemente y de manera general, como implementarían la Ley 11.723 - Régimen Legal de la Propiedad Intelectual en el código que han desarrollado.**

Para aplicar la Ley 11.723 – Régimen Legal de la Propiedad Intelectual en el código desarrollado, es importante reconocer que los programas de computación están protegidos como las obras científicas, artísticas y literarias. Esto incluye tanto el código fuente como el ejecutable, y cualquier contenido generado o utilizado, como bases de datos, textos o interfaces gráficas.

En nuestro proyecto, esto se refleja en la inclusión de avisos de copyright dentro del código y en la documentación, aclarando la autoría y los derechos sobre el desarrollo. Además, si utilizamos librerías o módulos de terceros, es fundamental respetar sus licencias para evitar infracciones.

También se debe tener en cuenta que si el software en un futuro permitiera la carga de contenidos por parte de los usuarios, sería necesario implementar políticas claras sobre el uso de materiales protegidos, así como sistemas para reportar y eliminar contenido que viole derechos de autor.

Finalmente, si se desea proteger legalmente el desarrollo, se puede registrar el programa en la Dirección Nacional del Derecho de Autor. Esto brinda respaldo legal ante cualquier conflicto sobre la autoría o el uso del software.

2. **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.**

Para aplicar la Ley 25.326 de Protección de los Datos Personales en la base de datos diseñada para nuestro proyecto, es importante tener en cuenta principios como la legalidad, el consentimiento, la finalidad específica, la calidad de los datos, y la seguridad de la información.

En primer lugar, los datos que se recolectan (como nombre, CUIT o mail) deben ser estrictamente necesarios para la gestión del sistema, y su uso debe estar justificado y claramente informado al usuario. De manera ideal, debería existir un aviso de privacidad que explique qué datos se recopilan, para qué se usan y cómo serán protegidos. Ya que el consentimiento informado debe ser la base para cualquier tratamiento de datos personales.

También es importante permitir que los usuarios puedan acceder, modificar o eliminar su información si lo desean (derechos ARCO). Por eso, se deben diseñar formularios y funcionalidades que faciliten la actualización de los datos, y que la base esté preparada para esos cambios sin perder consistencia.

En cuanto a la seguridad, se deben tomar medidas como limitar el acceso a los datos solo al personal autorizado, hacer copias de seguridad periódicas, y evitar el almacenamiento de información sensible sin protección. En caso de que en el futuro se tratara con datos más delicados, se podría implementar encriptación, control de

acceso, registros de actividad o técnicas como la seudonimización para reducir riesgos.

El cumplimiento de la Ley 25.326 no solo es una obligación legal, sino también una práctica que genera confianza en los usuarios y proteger su privacidad.

3. **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, ¿cómo se implementaría?**

El Convenio Internacional sobre Cibercriminalidad, o Convenio de Budapest, es un tratado internacional que sirve para abordar los delitos informáticos y facilitar la cooperación transfronteriza.

Si SkyRoute S.R.L. implementa el sistema en una sucursal de España y un cliente argentino presenta una denuncia por un problema de seguridad, se puede aplicar el Convenio Internacional sobre Cibercriminalidad, ya que tanto Argentina como España son países participantes.

Este tratado facilita la cooperación internacional en casos de delitos informáticos. Por ejemplo, las autoridades argentinas podrían pedir colaboración a las autoridades españolas para obtener pruebas digitales, investigar el incidente y localizar a los posibles responsables, incluso si los datos están alojados en servidores fuera del país.

El convenio permite acciones como la preservación y entrega de datos informáticos, la intervención de comunicaciones electrónicas o la confiscación de sistemas si es necesario para la investigación. Además, cuenta con una red internacional de contacto 24/7 para dar respuesta rápida entre países.

Esto asegura que, aunque el sistema funcione en otro país, el incidente pueda ser tratado de manera efectiva, respetando las leyes de ambos lugares y garantizando una respuesta coordinada frente a delitos informáticos.

Si se implementara Inteligencia Artificial para este proyecto, ¿bajo qué legislación debería estar regulado y que buenas prácticas deberían implementar?

Si en el futuro SkyRoute S.R.L. decide implementar Inteligencia Artificial para optimizar la gestión de clientes, destinos o ventas, el sistema debería estar regulado por varias normativas, tanto nacionales como internacionales, debido a su presencia en Argentina y España.

Legislación que regularía el negocio:

- EU AI Act (Reglamento de Inteligencia Artificial de la Unión Europea): al tener operaciones en España, el proyecto podría quedar alcanzado por esta ley, que regula el uso de IA según su nivel de riesgo. Un sistema que toma decisiones automatizadas sobre clientes (como recomendaciones de viajes o segmentación) podría ser considerado de alto riesgo, por lo que debe cumplir

con requisitos de transparencia, seguridad, supervisión humana y gestión de riesgos.

- Ley 25.326 (Protección de los Datos Personales - Argentina): regula la recolección y tratamiento de datos personales. Cualquier sistema de IA que use datos de clientes deberá garantizar el consentimiento informado, la posibilidad de acceder, modificar o eliminar los datos, y asegurar su confidencialidad y protección.
- Ley 24.240 (Defensa del Consumidor - Argentina): si la IA interactúa con usuarios (por ejemplo, a través de chatbots o recomendaciones automáticas), debe cumplir con esta ley, respetando el derecho a la información clara y la posibilidad de revisión humana de decisiones automatizadas.

Buenas prácticas recomendadas:

- Transparencia y explicabilidad: informar claramenteal usuario o cliente cuándo se está interactuando con IA y cómo se toman las decisiones.
- Privacidad desde el diseño: minimizar los datos recopilados, usar anonimización o cifrado, y cumplir con los principios de protección de datos desde el inicio del desarrollo.
- Supervisión humana: las decisiones críticas deben ser revisables o reversibles por una persona.
- Equidad: evitar sesgos que puedan generar discriminación (por ejemplo, en precios o recomendaciones basadas en características protegidas de los usuarios).
- Robustez: asegurar que el sistema de IA sea resistente a errores o ataques.
- Gobernanza del sistema: políticas claras para la gestión del ciclo de vida de los datos utilizados por la IA. Mantener trazabilidad de los datos y modelos utilizados, con documentación clara y políticas de control.

El uso de IA debe ser ético, seguro y transparente, cumpliendo con las normativas vigentes en cada región donde opera la empresa y respetando siempre los derechos de los usuarios.

4. Conclusiones

A lo largo del desarrollo del proyecto, no solo aplicamos conocimientos técnicos sobre programación, bases de datos y estructuras de software, sino que también comprendimos la importancia de considerar el marco legal y ético en el desarrollo de sistemas. Incorporar normativas como la Ley 11.723 de Régimen Legal de la Propiedad Intelectual y la Ley 25.326 de Protección de los Datos Personales nos permitió tomar

conciencia de la responsabilidad que implica trabajar con información y propiedad intelectual en entornos digitales.

Además, explorar escenarios reales como la implementación internacional del sistema o el uso de inteligencia artificial nos ayudó a entender que la tecnología debe diseñarse con criterios de seguridad, equidad y transparencia, respetando siempre los derechos de los usuarios. Estas reflexiones nos brindan una base para futuros desarrollos, en los que la ética profesional y la normativa vigente deben ir de la mano con la innovación tecnológica.