**PROYECTO (ABP)**

**Módulo: Programador**

**Evidencia de aprendizaje N°3**

**Estudiantes:**  
Luciana Goldraij

Luciano Castillo

Sol Milagros Baigorria

Emanuel Isaías Sudañez

### **Ética y Ejercicio Profesional**

**Implementación del Botón de Arrepentimiento:** El grupo incorporó dicha funcionalidad ya que la implementación del botón de arrepentimiento es un aspecto crucial en cualquier sistema de ventas que permita a los usuarios deshacer una transacción dentro de un período determinado. En definitiva, si lo pensamos desde la ética profesional, cumple con los principios rectores de la Ley de Defensa del Consumidor, como la transparencia, la protección de los derechos del usuario y la posibilidad de ejercer el derecho a desistir sin penalidades,

**Implementación de la Ley 11.723 en Hélice Tech:**

Para implementar la Ley 11.723 en Hélice Tech, tomamos las siguientes medidas:

* **Incluir información de derechos de autor:** Agregar campos en la base de datos para almacenar información sobre los derechos de autor y propiedad intelectual de los contenidos y datos almacenados.
* **Registrar la autoría:** Registrar la autoría de los contenidos y datos almacenados en la base de datos, para garantizar la protección de los derechos de autor.
* **Establecer permisos de acceso:** A la base de datos para garantizar que solo los usuarios autorizados puedan acceder y modificar los contenidos y datos protegidos por derechos de autor.

**Implementación de la Ley 25.326 de Protección de los Datos Personales en Hélice Tech, se pueden tomar las siguientes medidas:**

* **Cifrado de Datos:** Utilizar técnicas de cifrado para proteger los datos personales almacenados en la base de datos, como los nombres, apellidos y direcciones de correo electrónico de los clientes y empleados.
* **Autenticación y Autorización:** Implementar mecanismos de autenticación y autorización para controlar el acceso a los datos personales, asegurando que solo los usuarios autorizados puedan acceder y modificar los datos.
* **Registro de Accesos:** Mantener un registro de accesos a los datos personales para garantizar la transparencia y la seguridad.
* **Política de Privacidad:** Establecer una política de privacidad que informe a los titulares de los datos sobre la recopilación, almacenamiento y tratamiento de sus datos personales.

**Implementación del Convenio Internacional sobre Cibercriminalidad (Convenio de Budapest):**

El Convenio de Budapest es un tratado internacional que busca combatir la cibercriminalidad y proteger la seguridad en línea. Si SkyRoute S.R.L. implementa el desarrollo en su sucursal de España y un cliente argentino presenta un inconveniente de seguridad que denuncia, la implementación del Convenio de Budapest sería crucial para abordar el problema de manera efectiva.

Aspectos clave de la implementación:

* **Cooperación internacional:** España y Argentina, como signatarios del Convenio de Budapest, deben cooperar entre sí para investigar y perseguir los delitos cibernéticos.
* **Denuncia y notificación:** La denuncia del cliente argentino debe ser notificada a las autoridades españolas, que deberán investigar y tomar medidas para abordar el problema.
* **Investigación y persecución:** Las autoridades españolas y argentinas deben trabajar juntas para investigar y perseguir a los responsables del delito cibernético.
* **Protección de la evidencia:** La evidencia digital debe ser protegida y preservada para ser utilizada en la investigación y el proceso judicial.

**Implementación en la práctica:**

* **Punto de contacto:** España y Argentina deben designar un punto de contacto para recibir y responder a las solicitudes de asistencia en materia de cibercriminalidad.
* **Comunicación y coordinación:** Las autoridades de ambos países deben comunicarse y coordinar sus esfuerzos para investigar y perseguir el delito cibernético.
* **Capacitación y conciencia:** Los funcionarios de ambos países deben recibir capacitación y conciencia sobre la cibercriminalidad y el Convenio de Budapest.

**Beneficios de la implementación:**

* **Mejora de la seguridad:** La implementación del Convenio de Budapest puede mejorar la seguridad en línea y proteger a los ciudadanos y empresas de ambos países.
* **Cooperación efectiva:** La cooperación internacional puede ser efectiva para investigar y perseguir los delitos cibernéticos.
* **Protección de la evidencia:** La protección de la evidencia digital es crucial para garantizar la integridad de la investigación y el proceso judicial.

En resumen, la implementación del Convenio de Budapest en el caso de SkyRoute S.R.L. y el cliente argentino requiere cooperación internacional, notificación y denuncia, investigación y persecución, y protección de la evidencia.

Por su parte, en caso de que se implementara Inteligencia Artificial (IA) en el presente sistema de gestión de pasajes aéreos desarrollado por Hélice S.A.S., dicha incorporación podría regirse conforme a los principios y disposiciones establecidas por la legislación vigente en la Unión Europea, particularmente el Reglamento de Inteligencia Artificial (AI Act), aprobado por el Parlamento Europeo en el año 2024, como marco legal de referencia.

Sin dejar de lado que si se implementara Inteligencia Artificial para éste proyecto debería estar bajo la Leyes y normativas aplicables: Ley de Protección de Datos Personales (Ley 25.326): Regula la protección de datos personales y su tratamiento en Argentina y Ley de Defensa del Consumidor: (Ley 24.240): Protege los derechos de los consumidores y puede ser aplicable en casos de IA que interactúan con consumidores.

“AI Act” establece un marco normativo orientado a garantizar que el desarrollo y uso de sistemas de IA se realicen de manera ética, transparente y segura, sin comprometer los derechos fundamentales de las personas. Dado que el sistema en cuestión contempla la gestión de datos personales, operaciones de compraventa de pasajes y, eventualmente, funciones automatizadas para la atención al cliente, la clasificación del riesgo que le correspondería según el AI Act sería como sistema de **riesgo alto**. Esta categoría incluye aquellos sistemas de IA utilizados en sectores sensibles, como transporte y servicios esenciales.

En este marco, la empresa Hélice S.A.S. debería garantizar que el sistema cumpla con los requisitos establecidos para este tipo de aplicaciones. Esto implica realizar evaluaciones de impacto en materia de protección de datos, implementar procedimientos de gobernanza interna, asegurar la calidad de los datos de entrenamiento en caso de usarse modelos predictivos, y establecer mecanismos de supervisión humana. Asimismo, sería necesario documentar y explicar de forma clara el funcionamiento de los algoritmos empleados, especialmente si influyen en decisiones que afectan directamente a los usuarios, como la asignación de pasajes, recomendaciones de destinos o sugerencias personalizadas de tarifas.

El principio de transparencia exige, además, informar adecuadamente a los usuarios cuando están interactuando con un sistema basado en IA, asegurando que puedan comprender sus implicancias y ejercer su derecho a obtener intervención humana en decisiones automatizadas. Esta disposición coincide con los derechos reconocidos en el Reglamento General de Protección de Datos (RGPD), con el cual el AI Act se articula de manera complementaria.

En síntesis, la regulación de la inteligencia artificial en este proyecto no solo exige el cumplimiento de requisitos técnicos y organizacionales específicos, sino también la adopción de un enfoque preventivo y ético que sitúe en el centro la protección de los usuarios. La aplicación del AI Act permitiría establecer un marco de confianza en el sistema, garantizando que las funcionalidades basadas en IA operen de forma justa, segura y conforme a los valores fundamentales reconocidos por la normativa europea.

A continuación, se presentan algunas buenas prácticas que deberían implementar:

**1-** Transparencia y explicabilidad:

- La IA debe ser transparente en sus decisiones y acciones.

- Debe ser posible explicar cómo la IA llegó a una determinada decisión o resultado.

**2-**  Privacidad y seguridad:

- La IA debe proteger la privacidad y seguridad de los datos personales y sensibles.

- Debe implementarse medidas de seguridad adecuadas para proteger los datos y prevenir accesos no autorizados.

**3-**  No discriminación:

- La IA no debe discriminar a individuos o grupos basados en características protegidas.

- Debe ser diseñada para evitar sesgos y prejuicios.

**4-** Responsabilidad y rendición de cuentas:

- La IA debe ser diseñada para ser responsable y rendir cuentas de sus acciones y decisiones.

- Debe haber un proceso claro para abordar errores o problemas.

**5-** Pruebas y validación:

- La IA debe ser probada y validada para garantizar su precisión y eficacia.

- Debe haber un proceso de prueba y validación riguroso antes de implementar la IA en producción.

**6-**  Monitoreo y supervisión:

- La IA debe ser monitoreada y supervisada para garantizar su cumplimiento con las buenas prácticas.

- Debe haber un proceso de monitoreo y supervisión continuo para detectar y abordar problemas.

**7-**  Actualizaciones y mantenimiento:

- La IA debe ser actualizada y mantenida regularmente para garantizar su precisión y eficacia.

- Debe haber un proceso de actualización y mantenimiento planificado y ejecutado de manera regular.