Módulo: Programador - Proyecto ABP

Ética y Deontología Profesional

Este informe forma parte del ABP del Módulo Programador en la cual se encuentra esta materia. Se nos ha solicitado que respondamos las siguientes consignas:

1. 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 .

El botón de arrepentimiento está implementado en **en el archivo main.py de la parte de programación en este ABP.**

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

La protección de código que hemos desarrollado se encuentra contemplada en el ámbito de los Derechos de Autor, mediante la Ley de Propiedad Intelectual en donde incorporó en su artículo 1º a los programas de computación fuente y objeto dentro de las obras que se protegen bajo dicho régimen y se puede registrar ante la Dirección Nacional del Derecho de Autor (DNDA).

Podríamos implementar algunas medidas que nos aseguren que nosotras hemos trabajado en el código y que particularmente quede asentado nuestro trabajo en algún lugar:

Autoría: tener un encabezado en el archivo del código que incluya la información de los autores (integrantes del grupo), la fecha de creación y un aviso de derechos basado en la ley.
Versiones y su resguardo: utilización de GitHub para registrar de forma cronológica los avances y aportes individuales, garantizando tener el historial y poder ver el seguimiento del trabajo realizado por cada integrante del grupo de trabajo.
Contrato o licencia de uso: en caso de que la empresa SkyRoute S.R.L quiera nuestro código nos basaremos en el tipo de contrato que hayamos firmado donde se especificará la posible cesión del código o cuál puede ser la licencia de uso sin dejar de respetar nuestra autoría en él.

3. 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.

La base de datos diseñada en este proyecto se regirá de acuerdo a los principios establecidos en la **Ley de Protección de los Datos Personales**, donde garantizamos el tratamiento legal, seguro y responsable de la información personal de los usuarios.

Si nos basamos en la ley arriba mencionada tendremos en cuenta aspectos claves como:

Finalidad: sólo se almacenarán datos personales que sean necesarios para el funcionamiento del sistema, con un propósito legítimo y claro,ya que la ley exige que los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

Confidencialidad: los usuarios deberán aceptar el tratamiento de sus datos a través de formularios o políticas de privacidad visibles que provea el sistema respondiendo a la obligación legal de informar el uso de datos al momento de solicitar el consentimiento.

Seguridad: se deben adoptar las medidas que resulten necesarias para garantizar la seguridad e integridad de los datos personales. La ley prohíbe tener archivos, registros o bancos de datos no reúnan condiciones adecuadas de seguridad.

Transparencia: se garantizará que todo titular de datos personales sea informado de forma clara y previa sobre:

- La finalidad y el carácter del tratamiento de sus datos.
- El carácter obligatorio o facultativo de su entrega.
- Las consecuencias de brindar información incorrecta o negarse a proporcionarla.
- Su derecho a acceder, rectificar y suprimir sus datos personales.

Es obligación que el usuario esté bien informado y que sepa cómo va a ser el tratamiento de su datos y si quiere, tomar decisiones informadas sobre ellos.

Posible inscripción de la Base de Datos: se puede inscribir la BD formalmente ante la autoridad de control ya que será la responsable de las decisiones que se tomen con esa información y debe asegurar el correcto cumplimiento de la ley y hacerse cargo ante un posible incidente.

4. 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?

Implementación del Convenio de Budapest

El Convenio de Budapest establece una serie de normas a fin de incrementar la eficacia de las investigaciones y los procedimientos penales para hacer efectiva la lucha contra el cibercrimen. España, como país que forma parte del convenio, está obligada a cumplir con dichas normas; y si bien Argentina no es miembro, ha manifestado su intención de adherirse y actualmente puede colaborar mediante tratados o convenios de asistencia legal internacional.

En este caso particular, en el que un cliente argentino presenta una denuncia por un inconveniente de seguridad, el marco del Convenio de Budapest permitiría la

cooperación internacional entre los países, donde España debe responder a un pedido de colaborar y actuar conforme a las normas establecidas como facilitar el acceso a la investigación del delito informático, a los datos si se encuentran en servidores españoles, poner a disposición la información requerida, preservar la evidencia digital y contribuir al desarrollo de una investigación eficaz y coordinada entre países, que, en caso de comprobarse alguna responsabilidad legal, permita aplicar las sanciones correspondientes.

5. Si se implementara Inteligencia Artificial para éste proyecto, bajo que legislación debería estar regulado y que buenas prácticas deberían implementar?

Como primera regla fundamental es considerar la prioridad de los Derechos Humanos sobre la Inteligencia Artificial y alinear su desarrollo con marcos legales y éticos reconocidos internacionalmente.

De acuerdo con el material brindado en la plataforma, podemos ver que si quisiéramos implementar Inteligencia Artificial a nuestro proyecto deberemos basarnos en **Ley de IA de la UE** para que esté regulado, la cual establece una clasificación de los sistemas de IA en función del riesgo que puedan generar y según el nivel de peligro implican más o menos requisitos para el cumplimiento de la normativa.

Consideramos buenas prácticas a la:

Transparencia: informar claramente cuándo se está utilizando IA, y explicar de forma comprensible para el usuario cómo toma decisiones o recomendaciones.
Supervisión humana: asegurar que los procesos y toma de decisiones importantes puedan ser revisados y controlados por personas, especialmente si afectan derechos del consumidor.
Gestión de riesgos y ética: realizar evaluaciones de impacto antes de desplegar el sistema y diseñar mecanismos de corrección de errores o sesgos.
Protección de datos personales: cumplir con la protección de datos minimizando cualquier tipo de incidente que pueda ocurrir.
No discriminación: es importante que los modelos no reproduzcan sesgos, asegurando así diversidad en los datos utilizados para entrenar cualquier algoritmo. Un algoritmo basado en sesgos no es transparente.

Documentación técnica clara: mantener registros claros de cómo funciona el sistema y con qué fin.

Referencias:

NIC Argentina. (s.f.). *¿Qué es el Convenio de Budapest?* https://nic.ar/es/enterate/novedades/que-es-convenio-budapest

Organización de los Estados Americanos. (s.f.). *Convenio sobre la Ciberdelincuencia (Convenio de Budapest)* [PDF]. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Parlamento Europeo. (2023). *Ley de IA de la UE: primera normativa sobre inteligencia artificial*. https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial