Caso 4

Nota: La Resolución 509 del Consejo de Europa de 1968, aunque fue promulgada hace décadas, sigue siendo un pilar fundamental en la protección de datos y tiene una relevancia directa en los proyectos actuales de analítica y ciencia de datos.

Contexto: Una empresa de comercio electrónico desea desarrollar un modelo de recomendación de productos altamente personalizado para sus clientes. Para ello, recolectan una gran cantidad de datos sobre las preferencias de compra, historial de navegación y datos demográficos de sus usuarios.

Objetivo
¿Cómo garantizar que la recopilación y el uso de estos datos cumplen con las normativas de protección de datos y no infringen los derechos de los usuarios?

Estrategia

La Resolución 509, siendo uno de los primeros documentos internacionales en abordar la protección de datos, establece principios clave que deben ser considerados en este proyecto:

- Principio de finalidad: La empresa debe establecer los fines para los que se recolectan los datos (mejoran las recomendaciones de productos) y no usarlos para otros propósitos sin el consentimiento previo de los usuarios.
- Principio de calidad: Los datos recopilados deben ser precisos, completos y actualizados. Esto implica implementar medidas para garantizar la calidad de los datos y corregir cualquier error o inconsistencia.
- Principio de limitación del almacenamiento: Los datos personales no deben conservarse más tiempo del necesario para los que se recolectaron. La empresa debe establecer políticas de retención de datos y eliminar los datos obsoletos o innecesarios.
- Principio de seguridad: La empresa debe implementar medidas técnicas y organizativas adecuadas para proteger los datos personales de cualquier acceso no autorizado, pérdida, alteración o destrucción. Esto incluye el cifrado de datos, la autenticación de usuarios y la realización de copias de seguridad.
- Derechos de los individuos: Los usuarios deben tener derecho a acceder a sus datos personales, rectificarlos en caso de errores y oponerse a su tratamiento. La empresa debe establecer mecanismos sencillos y transparentes para que los usuarios puedan ejercer estos derechos.

Aplicación en el proyecto

- Consentimiento informado: Antes de recolectar los datos, la empresa debe obtener el consentimiento expreso de los usuarios, informándoles claramente sobre los fines de la recopilación, los tipos de datos que se recolectarán y sus derechos.
- Anonimización y seudonimización: En la medida de lo posible, la empresa debe

anonimizar o seudonimizar los datos para proteger la identidad de los usuarios.
- Auditorías de privacidad: La empresa debe realizar auditorías periódicas para verificar el cumplimiento de las normas de protección de datos y detectar posibles vulnerabilidades.
- Informes de impacto: Antes de implementar cualquier nuevo proyecto que implique el tratamiento de datos personales, la empresa debe realizar una evaluación de impacto en la protección de datos para identificar y mitigar los riesgos.

Observación

La Resolución 509, aunque antigua, sienta las bases para una gestión responsable de los datos personales en proyectos de analítica y ciencia de datos. Al comprender y aplicar estos principios, los científicos de datos pueden desarrollar modelos y soluciones innovadoras sin comprometer la privacidad de los usuarios.

Actividad: envía al correo edgar.diaz@ucags.edu.mx la respuesta de las siguientes preguntas:

¿Cuáles son los principales desafíos para garantizar la privacidad en proyectos de ciencia de datos?

- **Recolección masiva de datos**: En proyectos como sistemas de recomendación, se recopilan enormes cantidades de datos personales. El desafío radica en asegurar que solo se recolecten los datos estrictamente necesarios para el objetivo del proyecto, en línea con el principio de minimización de datos de la Resolución 509 y regulaciones modernas como el RGPD.
- **Anonimización y seudonimización**: A pesar de ser medidas esenciales, garantizar la efectividad de la anonimización y seudonimización de los datos es complejo. Existen riesgos de reidentificación, donde usuarios pueden ser identificados indirectamente a partir de patrones o combinaciones de datos, lo cual podría comprometer la privacidad.
- **Retención de datos**: Otro desafío es asegurar que los datos no se almacenen por más tiempo del necesario. Esto requiere implementar políticas de retención de datos claras, gestionadas de manera eficiente, y que incluyan mecanismos para eliminar datos que ya no son útiles o relevantes.
- **Transparencia y consentimiento**: Obtener un consentimiento informado y claro por parte de los usuarios puede ser un reto, especialmente en proyectos complejos que utilizan múltiples tipos de datos. La empresa debe ser clara y transparente sobre qué datos se recopilan, con qué fines, y cómo se protegerán.
- **Seguridad de los datos**: Implementar medidas técnicas robustas para proteger los datos es esencial. Esto incluye la encriptación, autenticación, y controles de acceso que deben estar continuamente actualizados frente a nuevas amenazas. Además, la empresa debe asegurar que solo personal autorizado acceda a los datos.

¿Cómo se pueden conciliar los objetivos de innovación con la protección de datos?

- **Cumplimiento de principios éticos:** La innovación debe estar alineada con los principios éticos y legales. Por ejemplo, el principio de finalidad de la Resolución 509 establece que los datos sólo deben utilizarse para los fines especificados y no para otros propósitos sin el consentimiento de los usuarios. Esto garantiza que la innovación se mantenga dentro de los límites del respeto a la privacidad.
- **Evaluación de impacto en la protección de datos:** Antes de desarrollar cualquier modelo o sistema, es fundamental realizar evaluaciones de impacto para identificar posibles riesgos relacionados con la privacidad. Esto ayuda a equilibrar la innovación tecnológica con la protección de los derechos de los usuarios, permitiendo mitigar los riesgos desde el inicio.
- **Tecnologías de privacidad avanzada:** Las empresas pueden utilizar tecnologías emergentes como la privacidad diferencial o el aprendizaje federado, que permiten desarrollar modelos predictivos sin comprometer los datos individuales. Estas herramientas facilitan la innovación al tiempo que garantizan un mayor nivel de protección.
- **Auditorías de privacidad continuas:** Mantener auditorías periódicas asegura que los proyectos de ciencia de datos cumplan con las normativas de protección de datos en cada etapa de desarrollo. Estas auditorías permiten detectar vulnerabilidades y ajustar las medidas de seguridad sin frenar los avances tecnológicos.
- **Transparencia y confianza del usuario:** La transparencia es clave para equilibrar innovación y privacidad. Al explicar de forma clara cómo se utilizan los datos y los beneficios que aportan al usuario, la empresa puede fomentar la confianza y obtener el consentimiento necesario para el desarrollo de proyectos innovadores.