

Aspectos Legales y Sociales de la Informática

Seguridad y Legislación Aspectos Éticos, Legales y Profesionales

**2025
Práctico N° 3**



Protección de Datos Personales y Privacidad (Parte 2)

Profesor: Garis Ana Gabriela
Alumno: Lucero Pollio Augusto

1. Análisis de una aplicación de salud

App elegida: Fitia (aplicación contadora de calorías y seguimiento nutricional).

a) Consentimiento y datos recopilados

Consentimiento: al registrarse, el usuario debe aceptar los Términos y la Política de Privacidad. La app solicita permisos opcionales como acceso a notificaciones y conexión con Google Fit/Apple Health.

Datos almacenados: correo electrónico, datos de perfil (edad, peso, altura, género), historial de alimentación y entrenamientos, objetivos nutricionales, progreso físico y datos técnicos del dispositivo.

b) Información al usuario

Finalidad: registrar la ingesta de alimentos y actividad física, calcular calorías consumidas y gastadas, y ofrecer métricas de seguimiento del progreso nutricional del usuario. También utilizan los datos para análisis internos y mejora de la plataforma.

Tiempo de retención: mientras la cuenta esté activa; cierta información puede conservarse más tiempo por obligaciones legales.

Seguridad: Fitia indica que aplica cifrado y medidas técnicas para proteger la información. Los datos no se venden, aunque pueden compartirse con proveedores de servicios necesarios para el funcionamiento de la app.

c) Opinión crítica

Adecuación: los datos solicitados están en línea con la finalidad de la app (seguimiento nutricional y de actividad). Algunos permisos opcionales, como la integración con otros servicios, pueden exceder lo mínimo necesario.

Confidencialidad: aplican buenas prácticas de seguridad, pero la dependencia de terceros podría generar riesgos de filtración.

Riesgo de vigilancia: medio, dado que los datos de salud son muy sensibles; podrían ser explotados más allá del propósito de seguimiento nutricional si se compartieran con fines de marketing u otros socios externos.

2. Caso elegido: Filtración de datos personales en la provincia de San Juan

En 2021, el gobierno de la provincia de San Juan fue sancionado por la Dirección Nacional de Protección de Datos Personales tras detectarse que la base de datos del portal de permisos de circulación presentaba vulnerabilidades que exponían información de salud de los ciudadanos. La sanción se debió a la falta de medidas de seguridad y al riesgo para la confidencialidad de los datos.

a) Aspectos de la Ley de Protección de Datos Personales que fueron infringidos:

La filtración de datos personales en San Juan violó varios principios establecidos en la Ley 25.326 de Protección de Datos Personales:

Seguridad de los datos personales (Artículo 9): La base de datos del portal de permisos de circulación no contaba con las medidas de seguridad adecuadas para proteger la información personal de los ciudadanos.

Confidencialidad (Artículo 10): El gobierno provincial no garantizó la seguridad de los datos personales, lo que puso en riesgo la confidencialidad de la información sensible almacenada en la base de datos. Aunque no hubo acceso indebido por terceros, la vulnerabilidad constituía un incumplimiento de las obligaciones de manejo seguro de los datos.

Finalidad (Artículo 4): Los datos personales fueron recolectados para gestionar permisos de circulación durante la pandemia, pero la exposición no estaba justificada por la finalidad original.

b) Sanciones para los infractores

La Dirección Nacional de Protección de Datos Personales, dependiente de la Agencia de Acceso a la Información Pública, sancionó al gobierno de San Juan por dos infracciones graves:

Falta de medidas de seguridad: Mantener bases de datos sin las debidas condiciones de seguridad.

Incumplimiento del deber de confidencialidad: No garantizar la protección de los datos personales.

Como resultado, se impusieron dos apercibimientos al gobierno provincial.

3. Motivos de Suspensión de **ChatGPT** y **Deepseek** en Italia

La Autoridad Italiana de Protección de Datos (Garante) suspendió a ChatGPT y Deepseek basándose en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Las razones clave son:

ChatGPT:

Falta de base legal: No tenía un fundamento jurídico sólido para la recopilación masiva de datos personales para entrenar su IA.

Protección de menores: Ausencia de un sistema de verificación de edad, lo que permitía el acceso de niños sin consentimiento parental.

Falta de transparencia: No informaba claramente a los usuarios sobre cómo se procesaban sus datos.

Deepseek:

Dudas sobre datos: La empresa china no proporcionó información satisfactoria sobre la recopilación, almacenamiento y transferencia de datos de usuarios italianos.

Riesgo de soberanía de datos: El Garante sospechaba que los datos podrían ser transferidos a servidores en China, fuera del alcance de las leyes de protección de datos de la UE.

4.

Desarrollado por JIGSAW

¡Correcto! Se frustró el intento de phishing.

Debes haber notado que los estafadores usan el sentido de urgencia para ocultar el uso de las "notas del vendedor" y otros campos de la factura.

Mostrar

