FLUJO DE DATOS – IKNX WATCH

Identificador es.iknx.smartwatch

Contenido

1. RECOPILACIÓN Y TRATAMIENTO DE DATOS DE USUARIO

1.1 Datos de registro y perfil

La aplicación recopila la siguiente información del usuario durante el registro y gestión del perfil:

Datos enviados al servidor:

- **Nombre completo** (nombre_apellidos)

- **Nombre de usuario** (usuario)

- **Dirección de correo electrónico** (email)

- **Contraseña** (almacenada encriptada en el servidor)

Datos adicionales del perfil:

- **Altura, peso, edad y género**: estos datos se solicitan únicamente para el **cálculo local del Índice de Masa Corporal (IMC)**.

Importante: Esta información **NO se envía ni almacena en nuestros servidores**, permanece estrictamente en el dispositivo local del usuario.

1.2 Autenticación y seguridad

Todas las comunicaciones se realizan a través del protocolo **HTTPS** para garantizar el cifrado en tránsito.

El sistema utiliza **tokens JWT (JSON Web Tokens)** para la autenticación del usuario. Una vez iniciada sesión, todas las comunicaciones posteriores utilizan estos tokens como identificador único (encriptado). Es decir, que reconocer al usuario solo es posible si se conoce la clave de desencriptado.

Las contraseñas se almacenan **encriptadas** en el servidor.

Excepción de cifrado: solo el proceso de registro inicial no utiliza token JWT, ya que aún no existe el usuario en el sistema. Por otro lado, el inicio de sesión tampoco requiere token, ya que es lo que permite recibir un token único.

2. DATOS DE DISPOSITIVOS WEARABLE (ALMACENAMIENTO EXCLUSIVAMENTE LOCAL)

2.1 Tipos de datos biométricos recopilados

La aplicación recopila los siguientes datos de salud a través de **conexión Bluetooth** con dispositivos wearable:

- **Frecuencia cardíaca** (BPM)

- **Presión arterial** (sistólica/diastólica en *mmHg*)

- **Saturación de oxígeno en sangre** (SpO2)

- **Temperatura corporal**

- **Frecuencia respiratoria**

- **Nivel de estrés**

- **Nivel de fatiga**

- **Pasos diarios**

- **Variabilidad de la frecuencia cardíaca** (RRI)

2.2 Política de almacenamiento local estricto

Todos estos datos biométricos se mantienen ESTRICTAMENTE EN LOCAL en el dispositivo del usuario. **NUNCA se envían a nuestros servidores** para su almacenamiento permanente. Sin embargo, **con el CONSENTIMIENTO del usuario** se pueden transmitir en tiempo real a otros dispositivos por medio de un **WEBSOCKET SECURE (servidor)**.

2.3 Sistema de alertas locales

Los usuarios pueden configurar **alertas personales** estableciendo valores mínimos y máximos para cada parámetro biométrico.

Estas alertas incluyen **períodos de histéresis** (tiempo de enfriamiento) para evitar notificaciones excesivas.

Todo el procesamiento de alertas se realiza **localmente en el dispositivo**.

NO se requiere conexión a servidor para el funcionamiento de las alertas personales.

3. COMPARTICIÓN DE DATOS EN TIEMPO REAL CON CONSENTIMIENTO EXPRESO

3.1 Mecanismo de consentimiento mediante QR

Para la compartición de datos biométricos en tiempo real, la aplicación implementa un **sistema de consentimiento expreso**:

1. **Generación de QR**: el usuario genera un código QR personal que contiene su identificador único.

2. **Consentimiento explícito**: antes de compartir el QR, el usuario debe aceptar un mensaje de consentimiento específico.

3.2 Transmisión segura mediante WebSocket

Una vez otorgado el consentimiento:

- Los datos biométricos se transmiten en **tiempo real** a través de **WebSocket Secure (WSS)**, es decir, nuestro servidor (pero no se almacenan, solo se transmiten).

- Solo se envían a usuarios propietarios del mismo grupo.

- La transmisión incluye: frecuencia cardíaca, SpO2, temperatura, presión arterial, frecuencia respiratoria, nivel de estrés, nivel de fatiga, RRI, pasos y fecha y hora.

3.3. Gestión de los grupos

Los usuarios pueden gestionar sus grupos (eliminarlos, salirse de un grupo o eliminar usuarios del grupo) en cualquier momento.

4. SISTEMA DE CONTACTOS DE EMERGENCIA

4.1 Establecimiento de contactos

Los usuarios pueden designar **contactos de emergencia** mediante intercambio de códigos QR o por nombre de usuario.

Cada solicitud de contacto requiere **aceptación explícita** del destinatario.

Los usuarios pueden gestionar sus contactos (agregar/eliminar) en cualquier momento.

4.2 Alertas de emergencia automáticas

Con consentimiento expreso del usuario:

- Se pueden configurar **umbrales de emergencia** para parámetros biométricos específicos.

- Si se superan estos límites, se envían **alertas automáticas** a los contactos de emergencia designados.

- Las alertas incluyen **períodos de histéresis** para evitar notificaciones repetitivas.

Importante: Solo los contactos previamente autorizados reciben estas alertas.

4.3 Función SOS Manual

Los usuarios pueden activar **manualmente una alerta SOS** manteniendo pulsado el botón del dispositivo IKNX Watch.

Esta alerta aparece como **mensaje emergente** en los dispositivos móviles de los contactos de emergencia. Requiere **configuración previa** y **consentimiento expreso** de los contactos.

5. SISTEMA DE GRUPOS

5.1 Creación y gestión de grupos

Datos almacenados en el servidor:

- **Nombre del grupo.**

- **Identificador único del grupo.**

- **Lista de miembros** con sus roles (propietario/miembro).

- **Información de membresía**: quién pertenece a qué grupo y con qué rol.

5.2 Funcionalidades de grupo

Monitorización en tiempo real entre miembros (con consentimiento previo).

Compartición de datos biométricos dentro del grupo vía **WebSocket Secure (servidor)**.

Los propietarios pueden gestionar la membresía del grupo (eliminar usuarios del grupo, salirse, eliminar el grupo).

6. DATOS DE UBICACIÓN Y SERVICIOS DE TERCEROS

6.1 Recopilación de ubicación

La aplicación **recopila datos de ubicación** del usuario utilizando:

- **GPS del dispositivo móvil.**
- Servicios de localización de Google (Google Location Services).

6.2 Compartición con terceros - OpenMeteo

Único servicio de terceros para datos de ubicación:

- **Destinatario**: API de OpenMeteo (https://open-meteo.com/).
- **Datos enviados**: coordenadas de latitud y longitud.
- **Propósito**: obtener alertas meteorológicas localizadas.
- **Frecuencia**: cuando el usuario accede a la función de alertas climáticas.

Datos recibidos de OpenMeteo:

- Temperatura máxima/mínima diaria
- Índice UV máximo
- Precipitación acumulada
- Velocidad del viento
- Código meteorológico

6.3 Presentación de alertas meteorológicas

La aplicación procesa localmente los datos meteorológicos para generar:

- **Alertas de temperatura alta** (>35°C).
- **Alertas de índice UV alto** (>8).
- **Alertas de precipitación intensa** (>50mm).

7. SISTEMA DE VALORACIONES OPCIONALES

7.1 Datos de reseñas

Los usuarios pueden **opcionalmente** enviar valoraciones que incluyen:

- **ID del usuario** (identificador interno)
- **Valoración numérica** (escala definida)
- **Comentario de texto** (opcional)
- **Versión de la aplicación**

7.2 Almacenamiento de reseñas

Datos almacenados en el servidor:

- Todas las reseñas enviadas voluntariamente por los usuarios
- Asociación entre reseña e ID de usuario para análisis estadísticos

8. VALIDACIÓN DE DISPOSITIVOS Y POLÍTICAS DE PRIVACIDAD

8.1 Validación MAC

La aplicación valida la **dirección MAC** de dispositivos IKNX Watch.

- **Propósito**: verificar compatibilidad y autenticidad del dispositivo.
- **Datos enviados**: dirección MAC del dispositivo.
- **Respuesta del servidor**: confirmación de validez y compatibilidad.

8.2 Políticas de privacidad

La **primera vez** que el **usuario inicia sesión en un dispositivo** está **obligado a aceptar** los términos y condiciones, la política de privacidad y la política de cookies.

> **IMPORTANTE**: en el servidor se almacena **fecha y hora** en la que se **acepta cada política por separado**.

9. RESUMEN DE DATOS ALMACENADOS EN SERVIDOR

9.1 Información de usuarios

- Datos de identificación personal (nombre, usuario, email).
- Contraseñas encriptadas.
- Tokens de autenticación JWT.

9.2 Relaciones y contactos

- **Contactos de emergencia**: quién tiene a quién como contacto de emergencia.

- **Grupos**: membresía y roles dentro de grupos.

- **Solicitudes de contacto**: pendientes, aceptadas, rechazadas.

9.3 Valoraciones y *feedback*

Reseñas de usuarios con valoraciones y comentarios opcionales con ID de usuario asociado a cada reseña.

9.4 Aceptación de políticas

Estado de aceptación de términos y condiciones, política de privacidad y política de cookies (**con fecha y hora** en la que el usuario **aceptó** cada una de ellas).

10. DATOS QUE PERMANECEN EXCLUSIVAMENTE LOCALES

10.1 Datos biométricos completos

- **Todos los registros históricos** de datos de salud del IKNX Watch.

- **Configuraciones de alertas personales.**

- **Umbrales de monitorización** establecidos por el usuario.

10.2 Información personal sensible

- **Altura, peso, edad, género** (solo para cálculo de IMC).

- **Configuraciones locales** de la aplicación.

- **Preferencias de usuario** no relacionadas con funcionalidades de servidor.

11. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

11.1 Cifrado y comunicaciones

- **HTTPS** para todas las comunicaciones con el servidor.

- **WebSocket Secure (WSS)** para transmisión en tiempo real.

- **Cifrado de contraseñas** en el servidor.

- **Tokens JWT** para autenticación segura.

11.2 Control de acceso

- **Consentimiento expreso** para compartición de datos biométricos.

- **Gestión granular** de permisos de contactos.

- **Revocación inmediata** de grupos y contactos de emergencia por parte del usuario.

TABLA-RESUMEN DATOS RECOPILADOS, COMPARTIDOS Y LOCALES

Dato	*Almacenamiento local*	*Almacenamiento en servidor*	*Transmisión en tiempo real*	*Método de seguridad*
Nombre completo	Sí	Sí	Sí (consentimiento)	JWT, HTTPS y WWS
Usuario	Sí	Sí	Sí (consentimiento)	JWT, HTTPS y WWS
Email	Sí	Sí	No	JWT, HTTPS
Contraseña	Sí	Sí	No	Encriptada y HTTPS
Altura	Sí	No	No	Solo local
Peso	Sí	No	No	Solo local
Edad	Sí	No	No	Solo local
Género	Sí	No	No	Solo local
Frecuencia cardíaca	Sí	No	Sí (consentimiento)	JWT, HTTPS y WWS
Presión arterial	Sí	No	Sí (consentimiento)	JWT, HTTPS y WWS
SpO2	Sí	No	Sí (consentimiento)	JWT, HTTPS y WWS
Temperatura corporal	Sí	No	Sí (consentimiento)	JWT, HTTPS y WWS
Frecuencia respiratoria	Sí	No	Sí (consentimiento)	JWT, HTTPS y WWS
Nivel de estrés	Sí	No	Sí (consentimiento)	JWT, HTTPS y WWS
Nivel de fatiga	Sí	No	Sí (consentimiento)	JWT, HTTPS y WWS
Pasos	Sí	No	Sí (consentimiento)	JWT, HTTPS
HRV/RRI	Sí	No	Sí (consentimiento)	JWT, HTTPS y WWS
Configuración de alertas personales	Sí	No	No	Solo local
Contactos de emergencia	Sí	Sí	No	JWT y HTTPS
Alertas a los contactos de emergencia	Sí	No	Sí (consentimiento)	JWT, HTTPS y WWS
Grupos	Sí	Sí	No	JWT y HTTPS
Membresía de grupos	Sí	Sí	No	JWT y HTTPS
Solicitudes de contacto	No	Sí	No	JWT y HTTPS
Ubicación (GPS)	No	No	Se comparte a OpenMeteo	HTTPS
Reseñas	No	Sí	No	JWT y HTTPS
MAC dispositivo	Sí	Sí	No	JWT y HTTPS
Aceptación de políticas	Sí	Sí	No	JWT y HTTPS
Tokens JWT	Sí	Sí	No	Encriptado y HTTPS