Questa è una nav-bar

Selecciona tu idioma preferido

IT EN ES FR DE

Aviso Extendido de Tratamiento de Datos Personales

Aviso de conformidad con el Reglamento (UE) 2016/679 (GDPR)

Última actualización: 28 de diciembre de 2025

RescueCom es una plataforma de comunicación de emergencia (Prueba de Concepto), desarrollada en el ámbito académico para facilitar las operaciones de rescate en escenarios sin conectividad a internet.

Este aviso describe en detalle cómo tratamos sus datos personales y especiales (de salud), las medidas de seguridad criptográfica adoptadas y sus derechos. Nuestra prioridad es garantizar la máxima confidencialidad: adoptamos un enfoque de **Privacy by Design** e **Privacy by Default**, minimizando la recopilación de datos a lo estrictamente necesario para salvar vidas humanas.

El sistema utiliza una red descentralizada (Mesh) donde la seguridad está garantizada matemáticamente mediante cifrado de extremo a extremo. Ningún intermediario puede acceder al contenido de sus comunicaciones.

Descargar aviso legal completo (PDF firmado digitalmente)

1. Categorías de Datos Tratados y Finalidades

De conformidad con el principio de minimización de datos, recopilamos exclusivamente la información indispensable para la gestión eficaz de emergencias:

- **Datos Identificativos Comunes:** Nombre, apellidos, fecha de nacimiento y un identificador de usuario único (UUID). Estos datos sirven para identificar inequívocamente a la persona que solicita rescate.
- **Categorías Especiales de Datos (Datos de Salud):** El tratamiento incluye datos sensibles críticos para el triaje médico, tales como: grupo sanguíneo, alergias farmacológicas conocidas, discapacidades específicas (motoras, sensoriales o cognitivas) y patologías crónicas relevantes (ej. diabetes, cardiopatías).
- **Datos de Geolocalización:** Coordenadas GPS precisas (latitud/longitud) adquiridas en tiempo real o introducidas manualmente, utilizadas exclusivamente para localizar el dispositivo en escenarios de crisis.
- **Datos de Telemetría Técnica:** Metadatos relativos al estado de la batería y conectividad, necesarios para evaluar la fiabilidad del nodo en la red mesh.

2. Base Jurídica del Tratamiento

El tratamiento de sus datos personales está legitimado por las siguientes bases jurídicas:

- **Consentimiento Explícito:** En cumplimiento del pseudorequisito técnico del sistema PR_L.1, el almacenamiento de datos de salud se produce solo previo consentimiento libre, específico e informado, manifestado a través de una acción positiva inequívoca (opt-in) en la aplicación.
- **Protección de Intereses Vitales:** En situaciones de emergencia donde el interesado se encuentre física o legalmente incapacitado para dar su consentimiento, el tratamiento es necesario para proteger la vida del interesado o de otra persona física.

3. Arquitectura del Sistema y Modalidades de Tratamiento

El tratamiento se realiza mediante una infraestructura híbrida resiliente, diseñada para operar incluso en escenarios catastróficos:

- **Almacenamiento Local (Edge):** Los datos residen principalmente en el dispositivo del usuario en una base de datos SQLite cifrada (SQLCipher). Esto garantiza que el usuario mantenga la posesión física de sus datos.
- **Red Mesh Peer-to-Peer (P2P):** En ausencia de internet, los datos viajan a través de una red de dispositivos interconectados vía Bluetooth LE o Wi-Fi Direct. Cada dispositivo actúa como repetidor, pero sin acceso a los datos (ver punto 4).
- **Sincronización Cloud Segura:** Cuando se restablece la conectividad, los datos críticos se sincronizan con el servidor central mediante API REST protegidas, garantizando la coherencia de los expedientes médicos de emergencia.

4. Medidas de Seguridad Técnicas

Para mitigar riesgos de acceso no autorizado, pérdida o alteración, implementamos medidas de seguridad de última generación:

- **Cifrado AES-GCM-256:** Todos los datos sensibles, tanto en reposo como en tránsito en la red mesh, están cifrados con Advanced Encryption Standard (AES) en modo Galois/Counter Mode (GCM) a 256 bits, garantizando confidencialidad e integridad autenticada.
- **Protocolo Blind Relay (RF_16):** Los dispositivos que reenvían mensajes en nombre de otros usuarios actúan como "blind relays" (nodos ciegos). Transportan paquetes cifrados sin poseer la clave de descifrado, haciendo técnicamente imposible el acceso al contenido de los mensajes de rescate por parte de terceros intermediarios.
- **Gestión de Claves:** Uso de curvas elípticas (ECDH y ECDSA) para la negociación segura de claves de sesión y firma digital de los mensajes, previniendo ataques Man-in-the-Middle.

5. Segregación de Roles y Control de Acceso

El sistema impone una estricta separación de roles, definida a nivel de código e inmutable:

- **Usuario "Rescuee" (Solicitante):** Puede acceder, modificar y eliminar exclusivamente sus propios datos. No tiene privilegios para consultar datos de otros usuarios.
- **Usuario "Rescuer" (Rescatista Cualificado):** Obtiene acceso temporal a los datos de salud y ubicación del Rescuee solo en el contexto activo de una misión de rescate. El acceso es registrado y monitoreado.
- **Administrador del Sistema:** Gestiona la infraestructura técnica pero no posee claves privadas para descifrar datos de salud de usuarios, garantizando confidencialidad incluso respecto al proveedor del servicio.

6. Política de Retención y Derechos del Interesado

Período de Conservación: Los datos operativos se conservan durante la duración de la emergencia. Posteriormente, se archivan con fines médico-legales por el período prescrito por la ley (ej. 10 años para responsabilidad médica) o se anonimizan irreversiblemente con fines estadísticos y de investigación.

Ejercicio de Derechos: Puede ejercer en cualquier momento el derecho de acceso, rectificación, supresión ("derecho al olvido"), limitación, portabilidad y oposición. Puede retirar el consentimiento a través de la configuración de la aplicación, lo que conlleva la eliminación de datos locales y remotos. Para reclamaciones, puede dirigirse a la Autoridad de Protección de Datos nacional.