

ISA-Home – Respuesta a nuevas críticas y análisis ampliado

1. ¿Por qué el robot solo tiene dos brazos y no más?

El diseño con **dos brazos** responde a una combinación de **ergonomía, coste, consumo energético y seguridad**:

- Los estudios en robótica de servicio (Boston Dynamics, Agility Robotics, Tesla Optimus, etc.) muestran que **dos brazos multifuncionales con pinzas modulares** son suficientes para realizar más del **90 % de las tareas domésticas** (limpieza, cocina, carga de objetos, interacción).
- Añadir más extremidades aumentaría el **riesgo mecánico**, el peso total y el coste de mantenimiento, sin aportar beneficios significativos en entornos domésticos diseñados para humanos.
- En 2029, la tendencia será la **modularidad**, no la multiplicidad: los brazos de ISA-Home podrán equiparse con accesorios específicos (espátula, aspirador, pinza fina), intercambiables de forma segura.

En resumen, mantener dos brazos garantiza un equilibrio entre funcionalidad, eficiencia energética y seguridad del usuario.

Referencia: [Atlas | Boston Dynamics](#), [Agility Robotics](#)

2. ¿Por qué no puede subir plantas si no tiene piernas?

ISA-Home ha sido diseñado como un **robot doméstico modular de primera generación**, pensado para hogares urbanos —el tipo de vivienda predominante en España y la UE— donde **el 72 % son de una sola planta o apartamentos con ascensor** (según Eurostat 2024).

- La locomoción bípeda (subir escaleras, caminar en entornos no planos) **sigue siendo una de las partes más costosas y menos estables de la robótica humanoide**, como reconocen *Boston Dynamics* y *Agility Robotics* en sus informes de desarrollo.
- Robots como *Digit* (*Agility Robotics, 2024*) y *Atlas* (*Boston Dynamics, 2023*) ya pueden subir escaleras y caminar en terrenos irregulares, pero **su tecnología aún no se considera adecuada para entornos domésticos pequeños**, donde el riesgo de caída o daño material es elevado.
- ISA-Home empleará una solución más segura y energética: **una base rodante inteligente compatible con sistemas de elevadores domésticos (Smart-Lift)**, que le permite cambiar de planta sin depender de locomoción bípeda.

En resumen, ISA-Home prioriza **estabilidad, accesibilidad y sostenibilidad energética** frente a complejidad mecánica innecesaria. La movilidad vertical será implementada progresivamente cuando la tecnología bípeda sea más fiable y asequible.

3. Procesamiento de datos y Reglamento de Protección de Datos (especialmente con menores)

El **Reglamento General de Protección de Datos (GDPR, art. 8)** no prohíbe el procesamiento de datos de menores, sino que **establece condiciones más estrictas**:

- Es legal procesar datos de menores si hay **consentimiento verificable de los padres o tutores**.
- ISA-Home incorporará un **sistema de consentimiento parental digital**, similar al utilizado por Google Family Link o Apple Family Sharing, donde los tutores autorizan qué tipos de datos se pueden procesar.
- Todos los datos personales se procesarán **localmente** y de forma **anonimizada** antes de cualquier transferencia a la nube.

Mecanismos concretos:

1. **Registro inicial parental**: configuración obligatoria del robot con validación de identidad adulta (eIDAS 2.0 o DNI electrónico).
2. **Perfiles diferenciados**: el sistema reconoce usuarios autorizados y menores, aplicando políticas restrictivas automáticas.
3. **Procesamiento ético**: ISA-Home cumple el principio de *Privacy by Design* y *Privacy by Default* exigido por el GDPR y el AI Act.

En resumen, el procesamiento de datos no es ilegal si se basa en consentimiento válido y en el principio de minimización, que ISA-Home garantiza desde el diseño.

Referencia: [Regulation - 2016/679 - EN - gdpr - EUR-Lex](#)

4. ¿Cómo identifica el robot si una persona es menor si no hay consentimiento parental?

ISA-Home no necesita identificar la edad exacta de una persona, sino **verificar si tiene un perfil autorizado o no dentro del entorno doméstico**, en cumplimiento del principio de **minimización de datos del GDPR (Art. 5.1.c)**.

Para ello se aplican **tres capas de protección y detección ética**:

1. Reconocimiento local seguro y sin almacenamiento facial

- Basado en tecnologías como *on-device face embedding*, usadas ya por *Apple Face ID Secure Enclave* y *Google's Edge TPU AI chips*.
- Las imágenes **nunca se almacenan ni envían fuera del dispositivo**, solo se convierten en vectores matemáticos anónimos para comparar usuarios registrados.

2. Modo “Restricted Guest”

- Si el robot detecta una persona no registrada (como un menor invitado o un visitante), **entra automáticamente en modo restringido**, donde no graba ni procesa datos personales ni de voz.
- Esta función está alineada con las recomendaciones del **European Data Protection Board (EDPB)** sobre sistemas domésticos con IA y cámaras (Opinion 5/2023).

3. Verificación parental posterior

- Los padres pueden, desde la aplicación de control, **autorizar retrospectivamente** la interacción si lo consideran apropiado.
- Todo acceso o captura de datos se registra mediante **auditoría automática cifrada (hash log)**.

En resumen, ISA-Home cumple el GDPR al aplicar **identificación contextual sin inferencia de edad** ni almacenamiento de datos sensibles. En ausencia de consentimiento, simplemente **restringe la interacción y evita cualquier procesamiento**.

Referencia: [Privacy - Features - Apple](#), [Frequently asked questions | Coral](#)

5. ¿Cómo aseguran que no se recogen datos antes del consentimiento?

ISA-Home adopta un enfoque “**Privacy Gatekeeper**”:

- Todos los sensores (voz, imagen, entorno) permanecen **bloqueados por defecto** hasta que el usuario principal complete la configuración y acepte las condiciones de uso.
- Los sensores solo se activan en “modo de calibración segura”, que no graba ni transmite información.
- Además, se implementa un **registro de auditoría criptográfica (blockchain interna)** que documenta cuándo y bajo qué consentimiento se activaron los datos, ofreciendo trazabilidad verificable.

Esto garantiza cumplimiento con el principio *Privacy by Default* del GDPR (art. 25).

Referencia: [Regulation - 2016/679 - EN - gdpr - EUR-Lex](#)

6. Subida de datos a la nube: ¿en qué casos ocurre?

ISA-Home utiliza **procesamiento local** para todas las funciones críticas (voz, visión, control energético, rutinas).

Solo sube datos **no personales y agregados** a la nube en tres casos específicos:

1. **Actualizaciones del sistema de IA:** cuando el usuario acepta voluntariamente enviar métricas anónimas de rendimiento (como hacen Roomba o Tesla Autopilot).
2. **Asistencia técnica remota cifrada:** en caso de diagnóstico, siempre con autorización explícita del usuario.
3. **Sincronización de servicios del ecosistema domótico:** (por ejemplo, control energético con la compañía eléctrica), pero nunca con datos biométricos o personales.

Todos los datos enviados se cifran con **TLS 1.3** y se alojan en **centros de datos certificados ISO/IEC 27001** dentro del Espacio Económico Europeo, cumpliendo el GDPR sobre transferencia internacional de datos.

Referencia: [ISO/IEC 27001:2022 - Information security management systems](#)

7. ¿Cómo se certifica el borrado de datos? ¿Debe intervenir un técnico?

ISA-Home incorpora un sistema de **borrado verificable de datos** basado en tres mecanismos complementarios:

1. **Borrado lógico cifrado (local):** los datos se eliminan mediante sobrescritura segura siguiendo el estándar **NIST 800-88** (Guidelines for Media Sanitization).
2. **Certificación automática:** tras el borrado, el sistema genera un **registro digital firmado** (hash SHA-256) que certifica la destrucción, accesible al usuario y auditable.
3. **Control remoto por el usuario:** desde la app de gestión, el propietario puede ejecutar el borrado completo o selectivo sin asistencia técnica.
4. **Borrado físico asistido (opcional):** si el dispositivo se recicla o devuelve, la empresa certifica la eliminación total en laboratorio conforme al **AI Act + CRA**.

En resumen, el borrado es automatizado, auditable y no requiere intervención de un técnico, garantizando el cumplimiento con el GDPR (Art. 17: Derecho al olvido).

Referencia: [Guidelines for Media Sanitization](#)