IBERUS

Guidelines Buenas prácticas de seguridad en el dominio IoT

Entregable:	**E5.3**
Versión:	2.0
Fecha:	15/12/2023

Proyecto (CER-20211003) reconocido como **Red de Excelencia CERVERA**

IBV INSTITUTO DE BIOMECÁNICA DE VALENCIA
CTIC
ITCL CENTRO TECNOLÓGICO
Tekniker MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE
Financiado por la Unión Europea
NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN
CDTI INNOVACIÓN

Historial de versiones

Versión	Fecha	Descripción	Revisado por
1.0	27/11/2023	Primera versión	CTIC
1.1	05/12/2023	Versión revisada	TEK
2.0	15/12/2023	Versión final	CTIC

Lista de autores

Autor principal:	CTIC
Colaboran:	TEK

1. INTRODUCCIÓN 5

2. DISPOSITIVOS IOT EN EL ÁMBITO DE LA SALUD DIGITAL 7

2.1. Retos en el almacenamiento y gestión de datos 7

2.2. Riesgos y amenazas 7

2.3. Buenas prácticas y confidencialidad 11

2.4. Retos éticos 19

2.4.1. Dispositivos IoT 19

2.4.2. Protocolos de Datos 23

2.4.3. Aspectos prácticos asociados a los cuidados 26

2.5. Aspectos legales 27

3. IOT E INTELIGENCIA ARTIFICIAL EN LA PROVISIÓN DE SOLUCIONES INNOVADORAS PARA LA PROMOCIÓN DE LA AUTONOMÍA Y VIDA INDEPENDIENTE EN EL HOGAR 31

3.1. Modelos de IA dirigidos a la promoción de la vida independiente en el hogar 31

3.2. Principales casos de uso 32

3.3. Tecnologías empleadas en el despliegue de soluciones innovadoras en el hogar 33

3.4. Retos asociados a las tecnologías de visión e IA en la creación de entornos inteligentes en el hogar 34

3.4.1. Retos éticos 35

3.4.2. Retos legales 36

3.4.3. Retos sociales 42

3.5. Necesidad de un enfoque centrado en la persona 43

3.6. Buenas prácticas en el diseño de soluciones basadas en IA para la vida independiente 46

3.6.1. Buenas prácticas en el ámbito ético 46

3.6.2. Buenas prácticas en el ámbito legal 47

3.6.3. Buenas prácticas en el ámbito social 49

4. LÍNEA FUTURAS 50

4.1. Oportunidades respecto a la atención sanitaria y el bienestar de las personas 50

4.2. Implicaciones tecnológicas 51

4.3. Necesidades de investigación 51

5. REFERENCIAS 53

RESUMEN

La seguridad de IoT es el segmento de tecnología centrado en proteger los dispositivos y redes conectados en el Internet de las cosas (IoT). Permitir que los dispositivos se conecten a Internet los expone a una serie de vulnerabilidades graves si no están debidamente protegidos, lo cual es especialmente trascendental, en términos de comunicaciones, procesamiento y almacenamiento de datos, en aquellos casos en que se trabaja con datos de salud. A ello se añaden, además, cuestiones asociadas tanto a la privacidad como a aspectos éticos que, complementando a las cuestiones técnicas, permitan no sólo identificar riesgos existentes, sino también la futura definición de buenas prácticas que, asegurando la confidencialidad e integridad de la información, permitan un adecuado manejo de los mismos en un entorno interoperable y abierto en donde la ruptura con los silos de información actuales resulta cada vez más necesaria. Este intercambio y explotación de la información da lugar al uso de la IA como herramienta para maximizar la utilidad de los datos y aportar un importante valor añadido a los diferentes tipos de usuarios implicados en la creación de entornos inteligentes que favorezcan el cuidado de la salud.

En base a ello, a lo largo del documento se desgranan riesgos, amenazas y retos tanto puramente técnicos como especialmente éticos y se identifican, adicionalmente, una serie de buenas prácticas que deberían integrarse en cualquier proyecto que implique tecnologías IoT como base fundamental en la captación de información sensible del usuario en materia de salud e incorpore, al mismo tiempo, tecnologías de IA para su posterior explotación. A ello se añade un caso práctico que trata de materializar el despliegue de soluciones para afrontar de forma adecuada retos asociados a la privacidad desde el diseño (PbD), mediante el ejemplo de uno de los componentes del demostrador extraclínico en medio rural de IBERUS. Finalmente, se sugieren algunas líneas futuras de trabajo que se considera necesario profundizar y proveer de nueva evidencia científica, suponiendo, a su vez, nuevas oportunidades que den continuidad al trabajo realizado en la Red de Excelencia IBERUS.

1. INTRODUCCIÓN

El concepto de medicina de precisión es una clara tendencia en los últimos años, indicando la necesidad de desarrollar soluciones que permitan satisfacer las necesidades precisas de las personas. En consecuencia, es ineludible establecer mecanismos que permitan captar información de forma habitual y entornos que reflejen la realidad personal, así como explotar este conjunto de información de forma avanzada a fin ofrecer servicios médicos de mayor calidad, efectivos y eficientes. Relacionado con esta necesidad, la tecnología del Internet de las Cosas (IoT) ha dado lugar a un nuevo concepto de atención médica inteligente (Awad, et al., 2021).

El IoT está cambiando rápidamente la forma de vida de las personas. A pesar de ser un concepto relativamente novedoso, propuesto apenas hace 30 años, su desarrollo y aplicación a múltiples campos ha sido asombrosamente rápido, especialmente en los últimos años (Wang, 2021).

Dentro de estos ámbitos de aplicación, el sector salud es uno de los más destacados por múltiples motivos en términos económicos y técnicos pero, especialmente, por las múltiples virtudes de utilizar el IoT en la atención sanitaria como, por ejemplo, la accesibilidad a los servicios de salud, la disminución de costes operativos e incremento de la eficiencia, la mejora de la experiencia del paciente, la notable reducción de los errores o la creación de espacios físicos más inteligente e integrados que faciliten tanto la predicción de manera proactiva de problemas de salud como el cuidado, tratamiento y monitorización de pacientes tanto en el ámbito clínico como extrahospitalario, entre muchas otras (Farahani, Firouzi, & Chakrabarty, 2020) (Kelly, Campbell, Gong, & Scuffham, 2020). A ello se añade el efecto COVID (Ndiaye, et al., 2020), el cual ha avivado un replanteamiento de los modos tradicionales de prestación de servicios de salud, potenciando las modalidades virtuales y remotas (Torous, Jän Myrick, Rauseo-Ricupero, & Firth, 2020) (Tobore et al., 2019) y permitiendo generar entornos inteligentes conectados con un alto valor para el profesional sanitario, la persona y la comunidad en general.

Un conjunto de beneficios, especialmente potenciado por la IA, que impactan sobre las múltiples fases de transición asociadas a la enfermedad, desde el diagnóstico, la toma de decisiones clínicas basadas en un mayor conocimiento individual, la monitorización ubicua para la gestión de enfermedades o la mejor comprensión de la evolución de cualquier enfermedad y tratamiento (Miller y Brown, 2018) (Tobore, et al., 2019).

Unos beneficios que se espera que se incrementen exponencialmente, entre otros aspectos, por su importante escalabilidad. En todo el mundo, se estima que más de 21.000 millones de dispositivos se conectaron a Internet en 2020, que es 5 veces la cantidad de dispositivos 4 años antes (Kelly, Campbell, Gong, & Scuffham, 2020). Aunque es una cifra destacable, está en aumento y en 2030 se espera que el número de dispositivos médicos conectados a redes sanitarias e Internet se multiplique por tres, de manera que prácticamente el 70 por ciento tengan conexión. En esta línea, el conjunto de nuevas soluciones tecnológicas que permiten a las organizaciones gestionar mejor su información tendrá un protagonismo creciente en todo tipo de organizaciones públicas y privadas. Hoy en día se generan más datos, se analiza más

información y se consumen más resultados de análisis que nunca. El tiempo que media entre la aparición de los datos y la toma de decisiones basada en los mismos es cada vez menor, y cada vez mayor la importancia económica y social de dichas decisiones.

Estas predicciones se sustentan en base a datos de mercado. El sector de la salud digital se ha expandido de forma exponencial en los últimos años, y se prevé que el mercado de dispositivos médicos basados en IoT (o dispositivos médicos conectados) pase de los 52.200 millones de dólares a casi 136.800 millones en 2028 (KPMG, 2022). Este rápido crecimiento de la demanda de dispositivos médicos conectados está estrechamente relacionado con el hecho de que las solicitudes de patentes de dispositivos médicos conectados se han multiplicado por 100 en un periodo de 20 años (European Patent Office, 2021).

Parece evidente el conjunto de beneficios asociados a los dispositivos médicos basados en IoT. No obstante, en la otra cara de la moneda, el uso del IoT en el ámbito de la salud no está exento de obstáculos, considerándose la protección del entorno IoT en este sector como un problema complejo por las implicaciones que puede acarrear para las personas (Farahani, et al., 2018). Por ello, uno de los principales desafíos es precisamente cómo diseñar dispositivos y protocolos para recopilar, compartir, procesar y validar datos a través de diferentes dominios de aplicación de manera económicamente eficiente, tecnológicamente robusta, científicamente fiable y éticamente sólida.

Al respecto de ello, al tratar con información de carácter personal y sensible, las soluciones IoT no sólo tienen que considerar en su diseño cuestiones técnicas, sino que deben tener en cuenta cuestiones éticas como, por ejemplo, la posibilidad de identificar al responsable de los datos recogidos, la definición de fronteras entre la vida pública y la privada de las personas o los posibles ataques que afecten a la salud o la vida de las personas usuarias (Azer & Ahmed Abo Bakr, 2017).

A ello se añade que, una vez estos dispositivos han permitido captar la información, la misma tiende cada vez más a ser explotada mediante soluciones basadas en Inteligencia Artificial, maximizando su valor y aportando a profesionales sanitarios y población, una herramienta de especial utilidad para la mejora de su salud y calidad de vida, tanto en el aspecto puramente clínico, como respecto al fomento de la autonomía y vida independiente en el hogar. En relación a esta cuestión, es importante considerar que este tipo de soluciones en el ámbito de IBERUS presentan un alto impacto sobre la persona, por lo que enfoques emergentes como el diseño y desarrollo de soluciones centradas en la persona en base a retos, riesgos y necesidades de la misma cobra cada vez mayor preponderancia. Por este motivo, se entiende necesario considerar el conjunto de retos asociados a las tecnologías implicadas en la generación de los citados entornos inteligentes, incluyendo dispositivos IoT, soluciones basdas en visión por computador y, en general, sistema de Inteligencia Artificial, así como buenas prácticas para su adecuado diseño y consecuente salvaguarda de los aspectos éticos de las personas que hacen uso de los mismos.

2. DISPOSITIVOS IOT EN EL ÁMBITO DE LA SALUD DIGITAL

2.1. Retos en el almacenamiento y gestión de datos

Aunque depende mucho del tipo de dispositivo y de los servicios prestados, la fase de utilización contiene todas las tareas necesarias para poner en marcha el dispositivo en la ubicación final del cliente. Para un dispositivo típico, esto suele implicar tareas que van desde la entrega al cliente, la instalación física en la ubicación operativa, configuración inicial del dispositivo, establecimiento de un usuario seguro y credenciales tanto a nivel de dispositivo como de servicios remotos, emparejamiento con dispositivos móviles y acuerdos de recopilación/compartición hasta la nube/servicios de terceros.

Como ocurre en general en el conjunto de fases desarrollo y despliegue de los dispositivos IoT para datos clínicos, el complejo almacenamiento y la gestión de información exige un importante número de actores potenciales que participarán en esta fase. Por ejemplo, las empresas de logística para transportar los dispositivos de IoT, minoristas, técnicos para participar en el proceso de implementación o proveedores de servicios en la nube que ofrecen los componentes básicos de las plataformas de IoT. Estos actores suelen estar también involucrados en las siguientes fases de apoyo y retirada de equipamiento o dispositivos.

2.2. Riesgos y amenazas

La manipulación de datos asociados a los despliegues IoT presenta una serie de riesgos y amenazas intrínsecas. Estas resultan aún más relevantes dentro de la vertical de salud, por el hecho implica la manipulación de datos de origen clínico, pues los datos clínicos demandan un conjunto de garantías de privacidad del más alto nivel, siendo los **riesgos principales** a los que se enfrenta un despliegue IoT en este contexto, los siguientes:

- El daño irreparable causado por la ruptura de privacidad de las personas afectadas. Esto se ve agravado por las delicadas circunstancias particulares en las que se suelen encontrar las personas involucradas en procesos médicos.
- El daño de imagen pública para la organización causado por una filtración, ya sea maliciosa o no, de datos privados relacionados con la historia clínica de personas. El riesgo de este tipo de daño tiene efectos persistentes en el tiempo. Es razonable argumentar que esto puede llevar a un impacto a largo plazo en la confianza que el público en general deposita en las nuevas tecnologías IoT. En este caso el riesgo es el de la aparición de rechazo y barreras sociales al aprovechamiento de las nuevas posibilidades abiertas por el IoT.
- Los daños económicos directos derivados de las sanciones impuestas por los organismos pertinentes como consecuencia de la ruptura de regulaciones y leyes relacionadas con la privacidad.
- Los daños económicos indirectos causados por el aumento de inestabilidad en la posible explotación económica de los despliegues IoT.

Estos riesgos son el resultado principal de la materialización de un conjunto de amenazas al sistema IoT. En la siguiente tabla se detallan las **amenazas más relevantes** que se pueden identificar en este caso.

Tabla 1. Principales amenazas asociadas a dispositivos IoT en el ámbito de la salud digital

Principales amenazas de dispositivos IoT en el ámbito de la salud digital	IBERUS
Amenaza	**Descripción**
Vulneración de los flujos de datos en tránsito	Esta amenaza contempla la posibilidad de que una tercera parte consiga acceso a los datos que se encuentran en tránsito a través de, por ejemplo, un ataque de *Man in the Middle*. Los datos deben transportarse entre todas las capas del despliegue, incluyendo desde la capa de sensores hasta los dispositivos en el eje, desde el eje hasta los servicios centrales y también entre los servicios individuales dentro de la infraestructura en la nube. Además, existe una heterogeneidad elevada en los protocolos de capa de aplicación que también tiene un impacto negativo (MQTT, HTTP, AMQP, Websockets, etc). Una de las defensas más efectivas para esta amenaza es la implementación de tecnologías de encriptación modernas y la adopción de todos los mecanismos de seguridad proporcionados por los protocolos en cuestión.
Vulneración de los conjuntos de datos almacenados en repositorios	Esta amenaza existe de manera complementaria a la amenaza de datos en tránsito. Una vez que los datos llegan a su destino deben almacenarse en una base de datos, en una caché en memoria, en un fichero o en otro destino en función del nivel de persistencia y capacidad de acceso que sea necesario. La implementación de unas medidas estrictas de encriptación en tránsito puede no ser suficiente en algunos casos, así que también se recomienda la encriptación dentro de los repositorios para los conjuntos de datos más sensibles, denominada encriptación *at rest*.
Phishing	El phishing es un ataque basado en conseguir la apariencia de legitimidad a través de la imitación fiel de una aplicación, formulario o interfaz pública de cualquier tipo perteneciente a la organización que se pretende suplantar. Por ejemplo, un atacante puede copiar el aspecto de una aplicación web para que el usuario piense que se encuentra en la página real e introduzca su contraseña. En este caso se debe asegurar que las aplicaciones utilizan certificados actualizados con

	nombres fácilmente reconocibles y se debe concienciar a los usuarios de los riesgos que supone el phishing.
Ingeniería social	La ingeniería social puede interpretarse como una categoría de más alto nivel que incluye el phishing. Este tipo de ataques tienden a aprovecharse de la buena fe de las personas y de las convenciones sociales para engañar a los usuarios finales a que revelen información confidencial. La mayoría de las personas no se encuentran normalmente en estado de alerta, por lo que una interacción inesperada (por ejemplo, una llamada telefónica para una encuesta) puede coger por sorpresa y resultar en la filtración de datos privados.
Vulneración de la integridad estructural de dispositivos desplegados en campo	Esta amenaza impacta especialmente a los dispositivos IoT que, por sus objetivos y funcionalidades, deben encontrarse desplegados en entornos que no son plenamente seguros (por ejemplo, espacios públicos). En estos casos se abre la amenaza del vandalismo o, en un caso peor, la amenaza de que un atacante con conocimientos expertos estudie y modifique de manera imperceptible el dispositivo en cuestión. Esto puede derivar, incluso, en la instalación de malware transparente que tenga impacto a largo plazo y cause daño significativo antes de ser detectado. Es recomendable asumir que todos los dispositivos desplegados en entornos que no se consideren plenamente seguros pueden estar comprometidos, por lo que todas las interacciones con ellos deberían llevarse a cabo con un nivel elevado de garantías de seguridad.
Utilización de configuraciones de seguridad por defecto	Los conceptos y técnicas de seguridad no siempre resultan fácilmente explicables a usuarios sin conocimiento experto. Además, los usuarios finales tienden a evitar pasos de configuración que no son estrictamente necesarios y no tienen un impacto claro en el rendimiento de los dispositivos. Esta tendencia resulta en que la configuración de seguridad de los dispositivos tiende a permanecer sin actualizar con los valores por defecto de fábrica, lo cual es naturalmente una amenaza. Técnicamente se pueden implementar mecanismos para bloquear la funcionalidad del dispositivo hasta que se actualice la configuración de seguridad, por desgracia, esto no es viable en una mayoría significativa de los casos por las barreras que esto impone en las personas. La alternativa pasa por aumentar la visibilidad de estos problemas y concienciar a los usuarios finales.

Uso de dispositivos desactualizados	La utilización de paquetes y librerías software de terceras partes es una realidad inescapable en el diseño y desarrollo de la mayoría de los componentes software. No suele resultar viable afrontar la reconstrucción de todos los bloques fundamentales que componen una aplicación (por ejemplo, un driver para acceso a base de datos). Por desgracia, la integración de componentes de terceros introduce incógnitas en la seguridad del sistema. Las vulnerabilidades de estos paquetes deben ser tenidas en cuenta como una amenaza de gran impacto, incluso en los casos en los que el desarrollador original proporciona actualizaciones frecuentes. Por otra parte, también es importante destacar la amenaza que emana de la dificultad de mantener la homogeneidad de las versiones instaladas en los dispositivos en campo. La detección de vulnerabilidades y el lanzamiento de nuevas versiones seguras no resulta de mucha utilidad si no se adoptan estrategias para asegurar que esas versiones se despliegan en los dispositivos.
Interrupciones en los servicios centrales del sistema	Las aplicaciones modernas tienden a depender de un conjunto de servicios centrales, que suelen estar instalados en servicios de computación en la nube, ya sean públicos o privados. Ejemplos de servicios centrales incluyen sistemas de autenticación, bases de datos y servicios de inferencia para exposición de modelos basados en inteligencia artificial. Existe una amenaza en el hecho de diseñar despliegues IoT que tengan una dependencia estrecha y acoplada con estos servicios. Cuando los servicios fallan o no están disponibles por problemas de red, se pueden abrir superficies de ataque inesperadas que pueden ser explotadas por usuarios maliciosos. Se deben implementar pruebas que validen la estabilidad del firmware en ausencia de acceso a servicios centrales.
Explotación de dispositivos indebidamente retirados	Puede existir una falsa sensación de seguridad con respecto a dispositivos que han sido retirados y que se han transferido a una organización de gestión de residuos. Estos dispositivos pueden tener datos almacenados, o podría también darse el caso de que los datos no han sido borrados con mecanismos seguros que bloqueen la recuperación por parte de usuarios expertos. También se pueden identificar amenazas por parte de la oportunidad que esto supone para estudiar el hardware. Es altamente recomendable que todos los dispositivos se destruyan concienzudamente y todos los datos se eliminen con mecanismos seguros.

2.3. Buenas prácticas y confidencialidad

Uno de los objetivos de este documento es abordar las principales cuestiones de seguridad y consideraciones a adoptar para el dominio IoT dentro del contexto particular de la salud. El objetivo es proporcionar recomendaciones para el público objetivo que puedan ayudar a contrarrestar y mitigar las amenazas asociadas a los dispositivos IoT. Las recomendaciones se enfocan en cubrir los problemas superpuestos, ya que la mayoría de las prácticas no son efectivas en todas las industrias y usuarios.

Antes de detallar un conjunto de buenas prácticas, conviene destacar dos consideraciones de seguridad que aplican de manera horizontal a todas las etapas, como son, por un lado, el hecho de que los procesos que están más allá del control directo de la organización (es decir, gestionados por un tercero) son inherentemente desafiantes, pudiendo las auditorías e inspecciones ayudar con esta consideración, pero siendo difíciles de hacerse cumplir. Y, por otro lado, el grado de fiabilidad de los propios dispositivos IoT, es decir, la capacidad de poder brindar un servicio continuo de operación.

A continuación, se lista una serie de buenas prácticas que deberían integrarse no sólo en un proyecto como el que nos ocupa relacionado con la salud, sino en cualquier proyecto IoT que pretenda salir al mercado, o trate con datos sensibles de la persona usuaria.

Priorizar el trabajo con proveedores que aporten garantías de seguridad

Existe una amenaza inherente en trabajar con proveedores externos debido a la falta de control en sus medidas de seguridad, sin embargo, esta es regularmente una realidad comercial que no se puede evitar. Esta amenaza se puede minimizar favoreciendo a las empresas que implementan estándares y recomendaciones de seguridad. En entornos clínicos, y tratando con datos de esta índole, es fundamental la búsqueda de proveedores fiables.

Una empresa que busca certificarse suele ser una señal de que está dispuesta a trabajar seriamente para mejorar la seguridad de este tipo de dispositivos. La certificación suele ser un proceso costoso que no es adecuado para todas las organizaciones: las organizaciones que no están estandarizadas pero que cuentan con medidas de seguridad integrales y son transparentes al respecto (por ejemplo, derecho a auditoría, requisitos de seguridad contractuales) también deben considerarse confiables.

Trabajar en pos de la transparencia

La transparencia es crucial para controlar la seguridad. Las partes interesadas, especialmente los proveedores, deben ser transparentes, ofreciendo información clara y detallada sobre las operaciones y el comportamiento normal de los productos suministrados; así como comunicar toda la información relevante al siguiente paso de la cadena. Un mayor nivel de transparencia tendría el efecto secundario deseable de reforzar la confianza entre los participantes (NIST, 2021).

Adoptar un principio de diseño basado en la seguridad

Los módulos de seguridad deben considerarse componentes de alta prioridad, más aún en ámbitos clínicos, y tenerse en cuenta ya en el proceso de diseño, desde las primeras etapas a fin de evitar la amenaza que se origina cuando los módulos de seguridad se tratan de manera tardía o se consideran de menor prioridad. La integración de una sólida cadena de confianza debe ser una prioridad para garantizar la integridad de los módulos de hardware y software en los dispositivos IoT. El uso de técnicas y pruebas de codificación seguras centradas en la seguridad (por ejemplo, pruebas de penetración, análisis de vulnerabilidades) debe incluirse en las etapas apropiadas del IoT para implementar y validar las características de seguridad adecuadas. Se debe definir una línea de base de seguridad para cubrir los componentes más importantes de IoT. Dicho modelo de seguridad debe cubrir los elementos básicos de seguridad: protección, detección y respuesta a incidentes.

Los factores humanos también deben tenerse en cuenta en la etapa de diseño. Las mejores prácticas deben aplicarse y seguirse rigurosamente para evitar que se socave la seguridad debido a las malas decisiones de los usuarios. La inclusión de departamentos legales en las evaluaciones de seguridad y privacidad es otra práctica importante que debe integrarse en el proceso de diseño. Además, los expertos en seguridad deben participar directamente en las primeras discusiones de diseño conceptual con el equipo de gestión del producto, para que puedan incluir su punto de vista en la selección de los materiales de acuerdo con sus requisitos de seguridad (ISO, 2015).

Adoptar la seguridad como un proceso continuo

La seguridad no debe caracterizarse como una actividad ocasional o un estado, ya que las garantías que brindan las acciones en el plano de la seguridad (por ejemplo, las pruebas de penetración) pierden valor con el tiempo una vez obtenidas. El concepto de proceso implica flujo y consenso formal entre las partes interesadas, así como aprobación y aceptación. La seguridad debe incluirse en todas las etapas como un proceso continuo e iterativo (NIST, 2021).

Integración de una fuente raíz de confianza

Una raíz de confianza es el primer elemento de la cadena de confianza de un dispositivo; comúnmente se implementa utilizando un componente de hardware dedicado que proporciona un conjunto de capacidades y primitivas criptográficas que el dispositivo puede asumir como confiables. Estos componentes suelen ser resistentes a la manipulación a nivel de hardware y se pueden utilizar como base para medidas de seguridad, como la firma de firmware o el arranque seguro. También existen alternativas de software con costos más bajos, aunque son significativamente más vulnerables y, por lo tanto, en general, son aptos para un alcance limitado de aplicaciones. Los actores deben basar sus contribuciones en esta base de seguridad cuando sea posible (ISO, 2015) (Group, 2020).

Mantener y entrenar a un grupo de trabajo cualificado

Como es el caso con muchos campos tecnológicos, el dominio IoT muestra un rápido ritmo de cambio. Mantener una plantilla capacitada que tenga acceso a capacitación regular en seguridad y los recursos necesarios para mantenerse al día en el campo es de gran importancia para enfrentar los desafíos de seguridad que plantea IoT. Los equipos profesionales dedicados

únicamente a la seguridad deberían estar presentes en la mayoría de las organizaciones; aquellos que carezcan de los recursos para mantener dichos equipos deberían al menos asegurarse de que otros equipos técnicos tengan un grado adecuado de conocimiento sobre seguridad (NIST, 2021).

Promoción de una cultura de trabajo con un enfoque basado en el análisis del riesgo

Los desarrolladores de software a veces tienden a invertir recursos significativos en la búsqueda de una funcionalidad extendida para el producto final, lo que puede tener el efecto secundario no deseado de tomar dichos recursos de las tareas relacionadas con la seguridad. Este problema puede verse exacerbado por algunas decisiones de las capas de gestión, si se separan del enfoque de desarrollo. Un ejemplo perfecto de esto son los plazos poco realistas. Promover un proceso de desarrollo que considere los riesgos al distribuir los recursos y garantice que la seguridad reciba la atención adecuada puede tener un impacto significativo en la seguridad.

Aprovechamiento de las tecnologías emergentes para controlar y auditar la seguridad

Las tecnologías emergentes podrían ayudar a brindar visibilidad a los despliegues IoT para la salud y deberían evaluarse. Las organizaciones primero deben evaluar su viabilidad desde el punto de vista de la seguridad antes de comprometerse con una aplicación. Ejemplos de tales tecnologías incluyen Blockchain, que se puede utilizar para proporcionar sólidas garantías de integridad en los sistemas de trazabilidad; e Inteligencia Artificial (IA), que podría ayudar a los profesionales clínicos en el proceso de diagnóstico.

Por ejemplo, Device Fingerprinting (DFP) es una aplicación en la que la identidad del dispositivo se deriva de su actividad en la red sin necesidad de leer una identidad inequívoca. Sin embargo, las organizaciones deben tener en cuenta el hecho de que la IA no proporciona garantías absolutas de rendimiento y debe usarse como una herramienta complementaria.

Sistema de gestión de identidad integrado en dispositivos IoT

La capacidad de identificar de manera unívoca cada dispositivo IoT es crucial y tiene profundas repercusiones relacionadas con la visibilidad y la responsabilidad en el IoT. Los sistemas de gestión de identidad deben integrarse para proporcionar estos identificadores únicos. Por lo general, se incluyen en el contexto más amplio de los sistemas de gestión de acceso e identidad (IAM) que regulan el ciclo de vida de la identidad del dispositivo y brindan servicios de autenticación y autorización. En este caso, la identificación de cada dispositivo es crucial para gestionar los datos y asociarlos con el paciente, trámite o diagnóstico correcto en cada caso.

Proporcionar listas de materiales software (SBOM) para los dispositivos IoT

Un SBOM describe los componentes de software utilizados como bloques de construcción de cualquier producto de manera exhaustiva, incluidos paquetes o librerías comerciales y de código abierto. Estas listas aumentan la visibilidad del producto y permiten que tanto el fabricante como los usuarios externos verifiquen las vulnerabilidades conocidas y validen el dispositivo desde el punto de vista de la seguridad, lo que ayuda a reducir las brechas de vulnerabilidad que pueden permitir a los atacantes aprovechar esta brecha con fines

maliciosos. Una mayor visibilidad del producto también puede conducir a una mayor confianza entre los actores. Idealmente, los SBOM deberían estar disponibles para todos los productos de IoT de cualquier organización, independientemente de si se distribuyen comercialmente o no. Los SBOM pueden servir como un componente básico para la implementación de un sistema de control de versiones y gestión de la configuración; estos sistemas respaldan la evolución de los componentes de software, mejorando la trazabilidad y permitiendo a los usuarios y organizaciones establecer una línea de tiempo de las versiones de software. Esto, a su vez, puede usarse para volver a estados estables anteriores en caso de problemas inesperados (Buchheit, 2020).

Identificación de software de terceros

El uso de software de terceros introduce un grado de incertidumbre que actúa como una amenaza para la seguridad. Estos componentes de software deben estar documentados como parte del proceso de seguridad, incluyendo los criterios seguidos para su selección; las organizaciones deberían preferir aquellos que hayan pasado un proceso de evaluación y certificación, e incluir un plan de mantenimiento. Se recomienda un análisis exhaustivo del código fuente para los casos de código abierto en los que no se puede identificar una comunidad acreditada de usuarios, desarrolladores y partes interesadas de la industria; un enfoque posible para cubrir el código vulnerable es implementar una capa personalizada en la parte superior, aunque esto obliga a la organización a seguir las actualizaciones del desarrollador original.

Para ayudar con el proceso de identificación del software, las organizaciones pueden utilizar herramientas de software especializadas en Análisis de componentes, como OWASP Dependency-Track, que es una herramienta para generar SBOM. Los productos de escaneo también pueden aprovecharse para identificar vulnerabilidades y componentes de software; Las herramientas de escaneo de código fuente están disponibles para componentes internos y de código abierto, mientras que las herramientas de escaneo binario se pueden aplicar en el contexto de código cerrado. Cabe señalar que las herramientas de código abierto pueden desempeñar un papel importante en la seguridad de IoT, ya que la transparencia y la apertura son muy importantes. La comunidad de código abierto también es eficiente al encontrar fallos y corregirlos rápidamente. La industria se beneficia enormemente cuando las soluciones para las vulnerabilidades descubiertas en las herramientas de código abierto en el contexto de una organización privada o pública se devuelven a la comunidad de código abierto (NIST, 2021).

Establecer y mejorar la recolección, medida y gestión de los datos

No todas las partes interesadas tienen los recursos para realizar auditorías o análisis de seguridad, por lo que la mayoría realiza asunciones de confianza en algún momento. Es deseable minimizar estas suposiciones cuando sea factible, mientras se mantienen garantías de privacidad para el usuario final. Una herramienta o mecanismo avanzado para ayudar con la recopilación y medición de datos sería de gran ayuda en este sentido. El uso de estándares clínicos y la adopción de las pautas que declaran es una buena práctica en este aspecto (NIST, 2021).

Establecimiento de un plan de pruebas integral

Todas las soluciones de IoT deben incluir un plan de prueba integral para verificar que el producto muestre las funciones esperadas tanto en el software como en el hardware. Más si cabe en el ámbito clínico, donde un mal funcionamiento podría resultar en un mal diagnóstico, lesión o riesgo para la vida de un paciente. Las pruebas de aceptación deben realizarse independientemente de cualquier prueba anterior que pudiera haberse realizado en etapas anteriores. Una fracción de los dispositivos debe inspeccionarse en la última parte de la fabricación y someterse a pruebas de ciberseguridad para detectar configuraciones incorrectas o errores (Khan & Rogers, 2019).

Crear una documentación completa

Cree un conjunto integral de recursos de documentación para combatir los errores humanos que incluya pautas claras o puntos de acción para implementar en cada entregable, particularmente en los aspectos de administración de configuración y restauración después de un fallo. Este es un tema crítico ya que la ausencia de dichos recursos es una amenaza. Además, la presencia de documentación por debajo de la media podría ser activamente dañina. Las etapas de soporte y final son especialmente vulnerables a estas amenazas. IBERUS podría desempeñar un papel importante en este sentido alojando y manteniendo un repositorio de recursos, como una lista de pilas de software defectuosas que los proveedores deben evitar, o una lista de componentes seguros y combinaciones comprobadas que se utilizarán como guía en la etapa de diseño (Johnson, 2019).

Implementar ajustes de fábrica que incluyan el uso de seguridad por defecto

Un porcentaje significativo de clientes tiende a ignorar las características de seguridad por razones de conveniencia o falta de conocimiento técnico; esto suele dar lugar a vulnerabilidades que podrían evitarse con un uso adecuado de las funciones de seguridad ya incluidas en los dispositivos y productos. Estas medidas de seguridad son imperativas en dispositivos médicos, ya que los datos que almacenan son altamente confidenciales. La seguridad por defecto debe ser el enfoque para los fabricantes y proveedores de dispositivos médicos, por lo que los clientes que necesiten desactivar la seguridad deben hacerlo de manera consciente y explícita. Este enfoque se basaría en un modelo de seguridad consistente que es obligatorio aplicar y garantizar que los datos se recopilen, manipulen y transfieran correctamente.

Promover la atención a la ciberseguridad entre los usuarios

Un porcentaje significativo de usuarios carece de conocimientos sobre la configuración de seguridad y no son plenamente conscientes del impacto de una seguridad débil. Los dispositivos IoT vulnerables en posesión de los usuarios a veces se pueden utilizar como punto de entrada a los sistemas y servicios (por ejemplo, servidores utilizados para el aprovisionamiento o la configuración). La carga de la seguridad nunca debe dejarse como responsabilidad del usuario; sin embargo, las entidades sanitarias podrían beneficiarse de invertir recursos en campañas y acciones para crear conciencia sobre la importancia de una seguridad adecuada. Por ejemplo, esto podría tomar la forma de campañas de marketing o módulos de configuración cuidadosamente diseñados para brindar orientación y una excelente experiencia de usuario. Además, se debe exigir a los fabricantes que incluyan una

guía o manual completo para el usuario, que proporcione instrucciones sobre el uso seguro de sus productos tanto a médicos como a pacientes. De manera relacionada, también se debe educar a los consumidores para garantizar que vean la falsificación como una práctica inaceptable y peligrosa (iotsecurityprivacy, 2021).

Promesas de seguridad hacia los clientes

Los clientes deben recibir de forma clara y explícita información completa relacionada con la seguridad. Esto incluye, por ejemplo, posibles vulnerabilidades que podrían descubrirse durante el ciclo de vida del producto, o la relación de actualizaciones de software que se implementan en los dispositivos en uso. La transferencia de esta información a los actores de la cadena es crucial para lograr una seguridad continua.

Comprometerse a crear parches de seguridad durante un periodo de tiempo determinado

Los dispositivos IoT heredados basados en software sin mantenimiento son una amenaza para la integridad de los datos y la seguridad de profesionales y pacientes. El soporte extendido y la entrega oportuna de parches de seguridad deben tenerse en cuenta en el diseño y la planificación de un producto de IoT. Esto incluye el dimensionamiento adecuado de los recursos (por ejemplo, memoria) para admitir actualizaciones futuras. Los fabricantes deben tener la obligación de entregar parches de seguridad al menos hasta el final del tiempo de garantía, y preferiblemente hasta el final del tiempo de soporte. En cualquier caso, el período de tiempo que el fabricante se compromete a proporcionar los parches de seguridad debe indicarse explícita y claramente antes de la adquisición, y estar disponible sin costo adicional durante su uso.

Establecimiento y mejora de la planificación y gestión de actualizaciones y obsolescencia de los dispositivos

La necesidad de modernizar y mejorar la calidad y funcionalidades de los dispositivos suele dar lugar a soluciones IoT donde coexisten varias generaciones de dispositivos y software, que necesitan ser actualizados para no quedar obsoletos y evitar así lidiar con diferentes niveles de seguridad. El alcance debe extenderse hacia el final de la vida útil de cualquier dispositivo conectado, especialmente si se trata de actualizaciones OTA. La actualización de los dispositivos IoT son complicadas ya que los productos generalmente se basan en varios paquetes de diferentes fuentes y utilizan diferentes herramientas y componentes de terceros. La planificación y gestión de estas actualizaciones es algo importante a tener en cuenta (NIST, 2021).

Integración de mecanismos de actualización remota

La capacidad de aplicar actualizaciones de forma remota y automatizada para los dispositivos en uso es fundamental en el proceso de seguridad. Las etapas del ciclo de vida de la mayoría de los dispositivos IoT no son discretas, es decir, puede generarse una nueva funcionalidad una vez que se implementa el dispositivo; y las vulnerabilidades con impacto en los sistemas se pueden descubrir en una fecha posterior o como resultado de los datos recopilados de un ataque real. La capacidad de reaccionar rápidamente a los cambios en el entorno e implementar actualizaciones para dispositivos remotos es una parte importante en los

dispositivos relacionados con la salud, por lo que se incluirá y considerará desde las primeras etapas de diseño. Además, estos mecanismos deberán ser seguros para evitar el mal uso y la inyección de malware (Group, 2020).

Integración de procesos seguros de gestión de desechos

Los materiales y componentes producidos en las etapas de desarrollo y fabricación que no pasen las pruebas de calidad o que no se consideran listos para la producción por cualquier motivo posible deben procesarse y eliminarse de manera segura (por ejemplo, evitando dejar las unidades defectuosas en contenedores no asegurados). Esto es para evitar la amenaza de que actores malintencionados accedan a dichos componentes, ya que contienen datos privados que podrían distribuirse, componentes hardware que podrían lanzarse al mercado de forma gratuita o sin pasar las pruebas pertinentes, servir como activos valiosos para estudiar y descubrir vulnerabilidades o producir falsificaciones mediante ingeniería inversa.

Uso de técnicas seguras de eliminación de datos

Los dispositivos generalmente se restauran a la configuración de fábrica y se borran todos los datos privados del usuario durante las etapas de desmantelamiento y recuperación. Las prácticas de eliminación de datos inseguras (por ejemplo, un proceso de eliminación simple que no sobrescribe todos los sectores de almacenamiento) pueden dejar rastros de datos privados del paciente en el almacenamiento persistente que otro usuario con acceso al dispositivo puede recuperar más tarde utilizando herramientas de software especializadas. Las técnicas seguras de borrado de datos deben integrarse en estas etapas para garantizar que todos los datos privados de los pacientes y los datos de configuración se eliminen efectivamente de manera segura (Kissel, 2014).

Tabla 2. Resumen de buenas prácticas sugeridas asociadas a dispositivos IoT en el ámbito de la salud digital

Buenas prácticas sugeridas asociadas a dispositivos IoT en el ámbito de la salud digital IBERUS	
Recomendaciones	**Buena práctica sugerida**
Recomendación 1	Priorizar el trabajo con proveedores que aporten garantías de seguridad
Recomendación 2	Trabajar en pos de la transparencia
Recomendación 3	Adoptar un principio de diseño basado en la seguridad
Recomendación 4	Adoptar la seguridad como un proceso continuo
Recomendación 5	Integración de una fuente raíz de confianza
Recomendación 6	Mantener y entrenar a un grupo de trabajo cualificado

Recomendación 7	Promoción de una cultura de trabajo con un enfoque basado en el análisis del riesgo
Recomendación 8	Aprovechamiento de las tecnologías emergentes para controlar y auditar la seguridad
Recomendación 9	Sistema de gestión de identidad integrado en dispositivos IoT
Recomendación 10	Proporcionar listas de materiales software (SBOM) para los dispositivos IoT
Recomendación 11	Identificación de software de terceros
Recomendación 12	Establecer y mejorar la recolección, medida y gestión de los datos
Recomendación 13	Establecimiento de un plan de pruebas integral
Recomendación 14	Crear una documentación completa
Recomendación 15	Implementar ajustes de fábrica que incluyan el uso de seguridad por defecto
Recomendación 16	Promover la atención a la ciberseguridad entre los usuarios
Recomendación 17	Promesas de seguridad hacia los clientes
Recomendación 18	Comprometerse a crear parches de seguridad durante un periodo de tiempo determinado
Recomendación 19	Establecimiento y mejora de la planificación y gestión de actualizaciones y obsolescencia de los dispositivos
Recomendación 20	Integración de mecanismos de actualización remota
Recomendación 21	Integración de procesos seguros de gestión de desechos
Recomendación 22	Uso de técnicas seguras de eliminación de datos

2.4. Retos éticos

El IoT en el sector de la salud plantea una serie de problemas éticos derivados de los propios riesgos inherentes a los dispositivos conectados, la sensibilidad específica de los datos relacionados con la salud y su impacto en la prestación de asistencia sanitaria, especialmente cuando ello se lleva a cabo de forma automática e independiente de los usuarios. En el ámbito concreto de la ética, si bien su retos/riesgos pueden considerarse desde varias perspectivas (véanse algunos ejemplos como (Afzal & Arshad, 2021) (Rayan, Tsagkaris, & Iryna, 2021) (Calvillo-Arbizu, Román-Martínez, & Reina-Tosina , 2021) entre muchos otros), cada una de las cuales pone de relieve preocupaciones relacionadas pero diversas, tras analizar el conjunto de las mismas y atendiendo al ámbito de actuación de IBERUS, se ha considerado más adecuado desglosar estos retos en torno a tres ejes fundamentales: dispositivos, protocolos de datos y aspectos prácticos de la propia tarea asistencial con especial foco en el usuario civil.

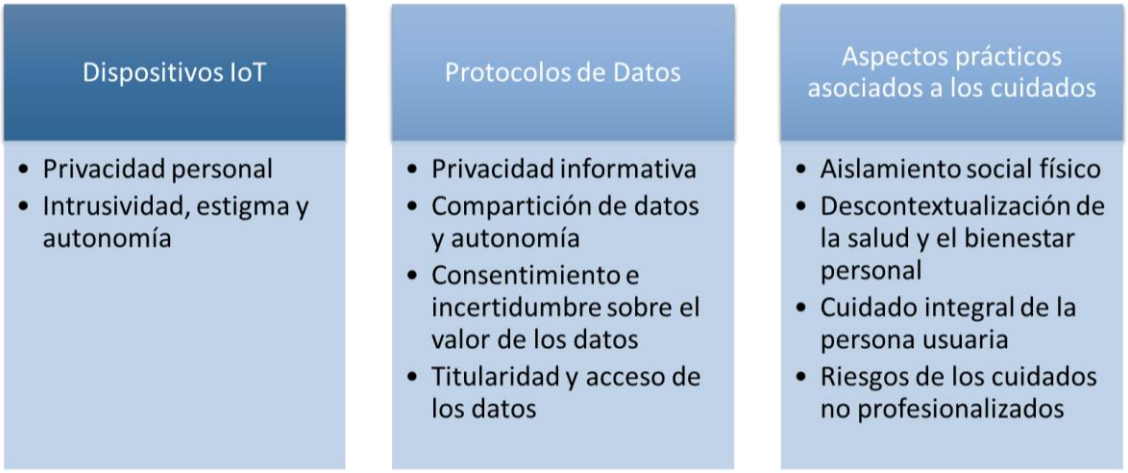

Figura 1. Ejes fundamentales de retos éticos a considerar en el dominio IoT salud

2.4.1. Dispositivos IoT

En primer lugar, es necesario prestar atención a los propios dispositivos que hacen posible captar la información para ser posteriormente transmitida y explotada a nivel asistencial. Dentro de este primer nivel, destacan dos aspectos fundamentales relacionados con la privacidad y aspectos relacionados con la valoración subjetiva individual como son el grado de intrusividad, el estigma que su uso puede generar y la percepción de autonomía personal.

Privacidad personal

En su origen, las soluciones IoT están diseñadas para ser aplicadas tanto en ámbitos privados como públicos. Respecto al primero, su uso provoca un acceso a las actividades de la vida privada que permiten la recogida de datos sobre la salud y los comportamientos del usuario y su análisis por parte de terceros.

En su nivel más amplio, la actividad personal puede ser monitorizada y analizada por terceros, generando oportunidades para el intercambio de datos, la explotación de los mismos y la categorización social (Lyon,, 2003). Si bien, al hilo de la necesidad de la medicina de precisión

que se citaba con anterioridad, estas funciones básicas pueden mejorar la asistencia sanitaria a través de un seguimiento cada vez más granular y personalizado (Pasluosta, Gassner, Winkler, Klucken, & Eskofier, 2015), también crean escenarios de riesgo relacionados con las expectativas de las personas usuarias en cuanto a su privacidad personal e informativa (la cual se abordará más adelante). De forma más específica, los dispositivos IoT pueden provocar una pérdida gradual de la intimidad, especialmente cuando se alude a entorno domésticos inteligentes (Brand, DiGennaro Reed, Morley, Erath, & Novak, 2019) (Haney, Furman, & Acar, 2020), pudiendo generar una sensación de intrusividad sobre la actividad personal y/o la interacción social que, incluso, pueden derivar en situaciones de aislamiento social en función del tipo de dispositivo empleado.

Si bien, el concepto de privacidad personal puede ser más común y sencillo de comprender, en este punto también es relevante aludir a este concepto en términos grupales, entendido como la privacidad correspondiente a grupos definidos por cualquier característica o combinación de características que se asocian a determinadas personas. Una caracterización o agrupación derivada del perfilado conjunto de grupos de personas a partir de sus datos y en los que, habitualmente, sus integrantes no son conscientes de la pertenencia a los mismos. Dicha agrupación puede hacerse de forma manual, pero, con el crecimiento reciente principalmente del Big Data y el uso de la Inteligencia Artificial, estos grupos pueden establecerse, no a partir de una acción positiva de una persona, sino que establecen de forma automática a partir de la definición abstracta de una IA que “agrupa algorítmicamente” personas en función de un conjunto de datos, los cuales pueden ser o no de carácter únicamente personal.

Los potenciales riesgos derivados de esta práctica, la cual resulta habitual a la hora, por ejemplo, de generar modelos predictivos en relación a una enfermedad o estratificaciones poblacionales, por ejemplo, no se beneficiarían de una protección efectiva ligada a los perfiles generados al no estar establecidos como tal y no estar sujetos a ninguna forma jurídica, careciendo así el perfilado y las inferencias sobre estos grupos de cualquier protección legal.

Adicionalmente, resultaría posible tomar decisiones sobre las personas que conforman dichos grupos, independiente de la percepción que tiene la persona de su propia individualidad o de su desvinculación con las características de otras. Las intervenciones basadas en estos criterios conllevan riesgos, no sólo por la inclusión implícita de la persona en un grupo del que no tiene conocimiento, sino de por decisiones que le afectan y pueden verse afectadas por sesgos de los que se desconoce su alcance y posibles consecuencias (e.g. por razón de género, raza, localización geográfica, etc.).

En términos regulatorios, la protección de la privacidad grupal no se logra automáticamente al proteger la privacidad individual. Por esta razón, recientes trabajos abogan por el complemento de la identificación personal con un enfoque en la identificación de información sobre categorías o grupos (Rath & Kumar, 2021).

Una conclusión importante es la concienciación de las personas sobre la importancia de preservar la propia privacidad, que va más allá de las consecuencias que puede tener para su propia privacidad ya que también puede afectar a los derechos y libertades de la sociedad en

su conjunto. Dicha sensibilización puede entenderse como condición básica para explotar el potencial que ofrece la tecnología desde una perspectiva responsable (Ruotsalainen & Blobel, 2020).

Por otro lado, a nivel legal, y desde la perspectiva del profesional que desarrolla dichos dispositivos, el Reglamento (UE) 2016/679, General de Protección de Datos (BOE, 2016) (en adelante, RGPD), en su artículo 25 (Parlamento Europeo y Consejo de la Unión Europea, 2016) y bajo el epígrafe '*Protección de datos desde el diseño y por defecto'*, incorpora a la normativa de protección de datos la práctica de considerar los requisitos de privacidad desde las primeras etapas del diseño de productos y servicios (Kounoudes & Kapitsaki, 2020). Es decir, el principio conocido como 'privacidad desde el diseño' o *Privacy by Design* (PbD, según sus siglas en inglés).

Este concepto implica emplear un enfoque orientado a la gestión del riesgo y de responsabilidad de forma proactiva para incorporar la protección de la privacidad a lo largo de todo el ciclo de vida del objeto. Si bien existen diversos marcos en torno a la privacidad por diseño (Semantha, Azam, Yeo, & Shanmugam, 2020) a continuación se muestran los nueve principios de la Guía de Privacidad desde el Diseño definidos por la Agencia Española de Protección de datos (Agencia Española de Protección de Datos, 2019).

Tabla 3. Principios de la privacidad desde el diseño

Principios fundamentales	Descripción
1	Proactivo, no reactivo; preventivo, no correctivo
2	La privacidad como configuración predeterminada
3	Privacidad incorporada en la fase de diseño
4	Funcionalidad total: pensamiento "todos ganan"
5	Aseguramiento de la privacidad en todo el ciclo de vida
6	Visibilidad y transparencia
7	Enfoque centrado en la persona

Haciendo especial mención al tercer principio, al considerar el enfoque de IBERUS, es necesario, concretamente:

- Considerar como un requisito necesario en el ciclo de vida de sistemas y servicios, así como en el diseño de los procesos de la organización.
- Ejecutar un análisis de los riesgos para los derechos y libertades de las personas y, en su caso, evaluaciones de impacto relativas a la protección de datos, como parte integral del diseño de cualquier nueva iniciativa de tratamiento.
- Documentar todas las decisiones que se adopten en el seno de la organización con un enfoque "*privacy design thinking*"

El objetivo último del PbD es que la protección de datos exista desde las primeras fases de desarrollo y no sea una capa añadida a un producto, siendo así parte integral de la naturaleza del mismo (Agencia Española de Protección de Datos, 2019).

Si bien se define como principio, la realidad es que en el RGPD le otorga la categoría de requisito legal con el objetivo de integrar las garantías para la protección de los derechos y libertades de los ciudadanos con relación a sus datos personales ya desde las primeras etapas del desarrollo de sistemas y productos.

Atendiendo a la relevancia de este aspecto, existen ejemplos de buenas prácticas dentro del ámbito de la Salud Digital que pueden servir como guía a llevar a cabo (Figura 2).

SALUD DIGITAL	
Detección de caídas	Los sensores IoT pueden detectar caídas y pedir ayuda para que se reduzca el tiempo que los ancianos permanecen en el suelo después de una caída. Servicio de detección de caídas Wallabot: https://walabot.com/walabot-home
Refrigeradores médicos	Los refrigeradores médicos dotados de sensores IoT permiten cumplir todas las normas de seguridad y las regulaciones nacionales del mercado farmacéutico. Sistema de monitorización de temperatura Efento: https://getefento.com/application/temperature-monitoring-for-medicines-and-vaccines-in-health-clinics
Monitorización de pacientes	Los médicos pueden observar los datos de los pacientes y proporcionar diagnósticos tempranos sin necesidad de que los pacientes estén físicamente presentes en los centros de salud o hospitales. Telit Healht Monitoring: https://www.telit.com/industries-solutions/healthcare/health-monitoring

Figura 2. Ejes de Buenas prácticas en el ámbito de la Salud Digital

Intrusividad, estigma y autonomía

A la hora de utilizar cualquier dispositivo IoT, especialmente asociado a la salud, existe un importante componente de percepción subjetiva en cuanto al grado de molestia o intrusividad en la actividad diaria, fundamentalmente, ligada a su visibilidad, que afecta a la aceptación por parte de la persona usuaria y al uso del propio dispositivo a largo plazo (Schomakers, Biermann, & Ziefle, 2021). En este sentido, los dispositivos altamente intrusivos o visibles pueden ser problemáticos desde el punto de vista ético en la medida en que alteran el comportamiento normal de la persona o su toma de decisiones autónoma, generando datos sesgados y pudiendo impactar de forma negativa en su salud en base a las decisiones tomadas a partir de los mismos (Jo, Ma, & Cha, 2021).

En este punto, es relevante diferenciar entre aquellas personas que utilizan dispositivos comerciales (por lo general, para fomentar el ejercicio físico o el bienestar) y quienes utilizan dispositivos médicos. En referencia a lo expuesto previamente, la preocupación por la molestia que puede generar y su intrusividad es más evidente en el caso de los dispositivos médicos, a los que se puede atribuir un estigma debido a su asociación con una enfermedad o condición de salud personal (Stavropoulos, Papastergiou, Mpaltadoros, Nikolopoulos, & Kompatsiaris, 2020).

Teniendo en cuenta estas cuestiones, y en relación también al diseño previamente señalado, parece necesario considerar especialmente el diseño de los dispositivos, de tal manera que se minimice su visibilidad y, con ello, la sensación de intrusión protegiendo así la toma de decisiones de forma autónoma y el sentido de identidad de la persona e, igualmente, incrementando la validez ecológica de la información. A este aspecto se añade otro concepto también relevante que se abordará nuevamente más adelante como es la necesidad de incrementar la transparencia de los dispositivos, de tal manera que incrementando el conocimiento la persona entienda su relevancia y promueva su uso.

2.4.2. Protocolos de Datos

Los dispositivos IoT generan un gran volumen de datos heterogéneos que describen la salud personal y los comportamientos de sus usuarios, siendo posible emplear muchos de estos datos para la investigación y toma de decisiones clínicas, lo que se refuerza especialmente con su combinación de datos de otras fuentes. Si bien previamente se abordaba la relevancia de aspectos de los propios dispositivos, el diseño de protocolos para permitir el acceso tanto de usuarios como terceros a los conjuntos de datos generados también plantea problemas éticos en relación a las siguientes cuestiones.

Privacidad informativa

La privacidad informativa se refiere al control de los datos sobre uno mismo. En un contexto de hiperconexión este es un aspecto complejo, tanto a nivel técnico como, fundamentalmente, respecto a las expectativas personales generadas en cuanto a dicho control. En este sentido, la preocupación por el control de los datos es un tema frecuente en las investigaciones que evalúan las experiencias de privacidad percibida por las personas usuarias de este tipo de dispositivos (Henze, Hermerschmidt, Kerpen, Häußling, & Wehrle, 2016) (Fei Wu, Vitak, & Zimmer, 2020).

En base a este interés, se han generado diferentes potenciales soluciones para su abordaje incluyendo aspectos como, por ejemplo, la anonimización local de los datos antes de la comunicación para ayudar a evitar el acceso no autorizado o la identificación del usuario (Clarke & Steele, 2015), o la posibilidad de permitir a los usuarios aplicar las preferencias de privacidad antes de transmitir datos sensibles de cara a proteger las expectativas de privacidad específicas de cada contexto particular (Baldini, Botterman, Neisse, & Tallacchini, 2016).

Sin embargo, estas medidas deben tener muy presente los riesgos de una posible reidentificación de los datos anonimizados a través de métodos como la agregación y la reutilización, así como la compensación entre el valor científico o comercial de los datos y su desidentificación (Ebersold & Glass, 2016) (Baldini, Botterman, Neisse, & Tallacchini, 2016).

Estas preocupaciones van directamente ligadas no sólo a protocolos de seguridad, sino al incremento del conocimiento por parte de las personas usuarias de aspectos ligados a los mismos. Así, si bien la confianza se ha convertido en uno de los retos a los que se enfrentan los usuarios de esta tecnología debido a su “novedad” en el día a día, los conocimientos

insuficientes de algunos usuarios, así como a la incertidumbre que puede generar el control remoto de algunos dispositivos conectados a la red. Existe una brecha en la conciencia pública y la comprensión de la seguridad de los datos de salud almacenados en la nube. Esto es preocupante, pues se considera la mayor amenaza individual para la adopción del IoT desde una perspectiva social (Jalali, Kaiser, Siegel, & Madnick, 2019).

Por lo tanto, la concienciación de la importancia de estas cuestiones y, especialmente, la generación de confianza en la población en general, y los pacientes que utilizan estos dispositivos en particular, se considera que pueden facilitar la implantación real de esta tecnología.

A este último respecto, la transparencia de las relaciones entre los datos recogidos y los fines para los que son recabados es fundamental para proteger la privacidad de los usuarios, que son quienes toman (o deben tomar) las decisiones sobre los usos que consideran aceptables. Si bien esta es una cuestión deseable a la hora de diseñar y aplicar cualquier dispositivo, esta necesidad viene reafirmada por la necesidad de cumplir el Principio de Transparencia, materializado en el derecho de información el RGPD, el cual regula el derecho de información en sus Artículos 13 y 14, distinguiendo entre la información que se debe facilitar al titular de los datos dependiendo si los datos personales se han obtenido del mismo o no. Esta transparencia contribuye, además, a reforzar la confianza en este tipo de dispositivos y las potenciales decisiones clínicas asociadas a los mismos, junto con otros factores también relevantes como la reputación de quienes desarrollan las soluciones o las motivaciones reales y usos esperados de quienes explotarán la información.

Compartición de datos y autonomía

En el contexto que nos ocupa el concepto de autonomía alude al derecho a tomar decisiones personales en relación a los datos relacionados con la propia persona. Este concepto se relaciona directamente con la citada privacidad en cuanto a que esta puede considerarse un requisito previo para la autonomía, así como con la intrusividad también reseñada y el consentimiento al que se hace referencia más adelante. Al respecto de este último punto, el hecho de compartir información no deseada o entrometerse en los espacios físicos o las relaciones sociales puede impedir la capacidad real de decisión del usuario (Abdulameer & Oubida, 2021).

Como se indicaba previamente, en este caso el abordaje de esta cuestión pasa por la definición de autorizaciones expresas, entendidas como consentimientos, en cuanto al uso, recogida y compartición de datos.

Consentimiento e incertidumbre sobre el valor de los datos

Si bien cada vez se alude en mayor medida a la nueva economía en torno a los datos, la realidad es que existe un enorme grado de incertidumbre inherente al valor futuro de los propios datos, tanto en el contexto investigador como en el ámbito asistencial o comercial, por lo que los fabricantes de estos dispositivos deben también valorar el valor potencial de los datos generados por sus dispositivos a largo plazo. A este respecto, la literatura indica la necesidad de considerar dos cuestiones relacionadas. En primer lugar, ¿recoge el dispositivo

la cantidad y los tipos de datos mínimos necesarios para prestar el servicio ofrecido, de modo que se minimicen los riesgos para la privacidad de la persona usuaria? En segundo lugar, ¿hasta qué punto se informa a dichos usuarios del valor potencial y de los posibles usos de los datos por parte de terceros? (Chikukwa, 2021).

Ambas cuestiones ya se han abordado: la primera mediante la Privacidad informativa; mientras que la segunda, si bien tiene relación con el consentimiento informado, requiere de un mayor grado de profundidad. En este sentido, los modelos tradicionales de consentimiento informado no son directamente aplicables a los datos obtenidos con dispositivos médicos basados en IoT, ya que las condiciones de servicio y otros acuerdos de usuario final que rigen estas aplicaciones tienden a permitir la recopilación, la agregación y el análisis de los datos de uso y actividad personal sin indicaciones claras de cómo se utilizarán los datos en el futuro, más allá de las declaraciones generales sobre el acceso de terceros, pero estos dispositivos pueden generar "datos invisibles" para los que la persona usuaria desconoce el alcance o la granularidad de los parámetros que se miden (Yeh, 2020) (Bietz, y otros, 2016).

El consentimiento se concede normalmente para la participación en un único estudio, no cubriendo las investigaciones no relacionadas resultantes de compartir, agregar o incluso reutilizar los datos (Hutchings, Loomes, Butow, & Boyle, 2021). Sin embargo, este "consentimiento de instancia única" se ve desafiado por las nuevas oportunidades de análisis secundario basadas en datos vinculados y agregados, y que a menudo revelan conexiones e inferencias imprevistas (Maloy & Bass, 2020). Este es un reto con un alto componente ético, ya que mientras los riesgos y beneficios iniciales de la adopción de este tipo de dispositivos pueden presentarse de forma razonablemente clara y justificada a las personas usuarias potenciales, la utilidad futura y la invasividad de los datos (es decir, lo que los datos pueden revelar sobre su vida privada) no pueden realmente conocerse en el momento de la adopción o implantación. Esta incertidumbre, potenciada por el crecimiento del Big Data, implica que el consentimiento para una intervención específica o “de una sola instancia” es en gran medida inadecuado para fomentar el valor científico de los datos en general, y del IoT aplicado al sector salud en particular.

Por ello, los fabricantes de estos dispositivos deben diseñar acuerdos de usuario específicos que representen de manera justa el valor incierto de los datos generados por la propia persona y, particularmente, su potencial derivado de la agregación y vinculación por parte de terceros.

Titularidad y acceso a los datos

Las personas usuarias generadoras de la información y los responsables de su tratamiento comparten derechos de "propiedad" imprecisos en relación con la redistribución y la modificación de los mismos en el ámbito IoT (Ali & Askar, 2021). Estos derechos se garantizan a través de la legislación sobre privacidad y protección de datos. En Europa, por ejemplo, los titulares de los datos conservan los derechos garantizados por ley de ser "mantenidos en el bucle" en relación con el procesamiento y el almacenamiento de los datos (Tene & Polonetsky, 2013), lo que significa que los titulares de los datos conservan los derechos a ser notificados cuando se crean, modifican o analizan los datos sobre ellos, y deben disponer de medios para

acceder y corregir los errores o las interpretaciones erróneas de los datos y los conocimientos derivados de ellos (Rashid, Parah, Wani, & Gupta, 2020). Ello implica que, para ejercer este derecho, las personas interesadas a acceder y modificar los datos dependen de que el sujeto sea consciente de qué datos existen sobre él, quién los tiene, qué significan (potencialmente) y cómo se están utilizando. No obstante, existen lagunas entre las protecciones ideales de la privacidad informativa y la capacidad real de los sujetos de los datos para ejercer un control significativo sobre sus datos (Andrejevic, 2014). Sin una mayor asistencia por parte de los responsables del tratamiento, una parte importante de las personas interesadas no presentan la capacidad de comprender el significado y el alcance de sus datos tratados o solicitar modificaciones y correcciones, siendo la supervisión y el control significativos de los datos personales expectativas poco realistas (Qiu, y otros, 2020).

A la hora de afrontar esta cuestión, es claro que las modificaciones de la normativa asociada a la protección de datos es una posibilidad para la accesibilidad y visibilidad de la recopilación y el procesamiento de datos basados en IoT, un enfoque ético por parte de los propios desarrolladores puede ser más factible a corto plazo. De este modo, los protocolos de dispositivos médicos basados en IoT pueden diseñarse para cumplir normas éticas que vayan más allá de los requisitos legales, por ejemplo, permitiendo a las personas interesadas un mayor acceso u oportunidades de modificar o corregir sus datos que las exigidas por el RGPD. En esta línea, algunos expertos como McNeely y Hahm (McNeely & Hahm, 2014) han propuesto un conjunto de "principios básicos de la ampliación del intercambio de datos" que debe seguir "cualquier sistema que se adopte en última instancia para ampliar el acceso a los datos de los participantes". Estos principios se centran en varias normas y conceptos, como la responsabilidad, la privacidad, la igualdad de trato de todas las personas solicitantes de datos, la responsabilidad de los responsables de los datos y de solicitantes, la viabilidad del sistema en términos de respuestas transparentes y oportunas a las solicitudes de datos y la ausencia de otras barreras innecesarias para el acceso.

2.4.3. Aspectos prácticos asociados a los cuidados

Sumado a las cuestiones técnicas de los propios dispositivos y los protocolos para el acceso e intercambio de información, la finalidad principal de estos dispositivos es mejorar la calidad asistencial. Por ello, también es importante considerar las cuestiones éticas que implican dichos cuidados, especialmente contemplando que este tipo de soluciones permite llevar a cabo un uso de dispositivos médicos por parte de personas (población general) que no tienen conocimientos técnicos avanzados ni en términos tecnológicos ni clínicos. De ello se derivan algunas cuestiones que se plantean brevemente, sumando así la perspectiva del paciente en el ámbito más práctico de su uso.

Aislamiento social físico

Los importantes beneficios ya señalados, especialmente los relacionados con la posibilidad de tener un seguimiento continuado remoto de las personas garantizando su adecuado estado de salud, intervención inmediata en caso de alteraciones y, con ello, la reducción de visitas clínicas puede realmente llevar a una reducción de la interacción social de algunas personas y

al incremento del sentimiento de soledad, especialmente en población mayor que vive sola en sus domicilios o en centros residenciales. A este respecto, múltiples estudios han estudiado precisamente como la tecnología puede promover la reducción del aislamiento social e incrementar la interacción (e.g. (Batool, Loke, Fernando, & Kua, 2021), incluso en situaciones particulares como la COVID-19 (Priyadarshini & Swain, 2021), pudiendo ser, en la otra cara de la moneda, una herramienta excelente para promover estos aspectos como contrapartida.

Descontextualización de la salud y el bienestar personal

Otro de los riesgos asociados, precisamente, a esa reducción en la interacción asistencial es la simplificación de la salud y la atención al paciente (Burr, Taddeo, & Floridi, 2020). Por ello, si bien este tipo de dispositivos son una herramienta excelente, deben entenderse como un complemento asistencial evitando centrar la atención clínica exclusivamente a parámetros objetivos que son medidos de forma automatizada o desatendida, siendo necesario considerar otros aspectos personales y subjetivos que influyen directamente sobre la salud.

Cuidado integral de la persona usuaria

En relación directa con lo comentado anteriormente, este tipo de dispositivos generan el riesgo de producir rutinariamente una visión más pobre o simplificada de múltiples factores sociales y contextuales que tienen un importante influjo sobre la salud de un paciente, en particular en relación con la salud mental y su bienestar (Anmulwar, Gupta, & Derawi, 2020). La aplicación de dispositivos para la monitorización de síntomas o situaciones específicamente centradas en una enfermedad pueden evitar conocer señales y emociones psicológicas que impiden el conocimiento global del estado del paciente.

Riesgos de los cuidados no profesionalizados

Finalmente, y como se anticipaba al inicio de este tercer bloque, si estos dispositivos se emplean únicamente como medio para reducir la carga de los recursos profesionales en cuanto a la atención médica (y/o social), se traslada implícitamente una carga a los miembros de la familia, los amigos y la comunidad convirtiéndolos en cuidadores informales quienes, además de deber sustituir las interacciones interpersonales y sociales que de otro modo se perderían, asumen una importante responsabilidad en términos de cuidados de salud del propio paciente con las implicaciones que ello conlleva.

2.5. Aspectos legales

Existe un amplio espacio de desarrollo entre los dispositivos médicos basados en el IoT y la relación legal y ética. Si bien la RGPD contempla unas directivas exigentes que contemplan el tratamiento y la propiedad de los datos, la protección de los mismos, el sesgo y otras cuestiones éticas, esta relación requiere adaptarse continuamente a las nuevas implementaciones y nuevos desarrollos asegurando la aplicación normativa y la adaptación de ésta a la nueva realidad y a las evoluciones que se deriven. La evolución tecnológica y su amplitud en cuanto a nuevos campos de aplicación exige realmente que las nuevas leyes y normas deberían complementar las diferentes leyes existentes para mantener la seguridad y

la privacidad completas y cubrir todas las cuestiones legales (Azer & Ahmed Abo Bakr, 2017). A ello se añade el hecho de que el crecimiento de apps y tecnologías a nivel de consumidor general hace cada vez más difusos los límites entre los dispositivos médicos y no médicos y plantea retos éticos adicionales relacionados con la forma de regularizar dichas tecnologías (Schmietow & Marckmann, 2019), un aspecto exacerbado por la velocidad con la que se expanden, a nivel global, este tipo de soluciones en el ámbito salud (Cortez, 2018).

En relación a esto, desde el punto de vista político, el mayor reto es el del convencimiento de que es posible establecer políticas de buen uso de aquellos datos que impacten de lleno en aspectos de privacidad, junto con el establecimiento de mecanismos de compensación adecuados para los propietarios de los datos por el uso y explotación de los mismos.

A ello se añade la necesidad de permanecer atentos a la identificación de los riesgos y peligros asociados a los dispositivos médicos conectados, incluidos los riesgos relacionados con la ciberseguridad, conociendo y aplicando las directrices más relevantes para garantizar su legalidad, las cuales se han acelerado en los últimos años. Precisamente por este motivo, esta tampoco es una cuestión sencilla de abordar debido a la heterogeneidad de directrices existentes a nivel mundial. Si bien este punto no es objeto de abordaje en el presente documento, en la Figura 3 se muestra un resumen sucinto de documentos de orientación y las directivas de varios organismos reguladores mundiales para los dispositivos médicos conectados en todo el mundo, los cuales se han acelerado en los últimos años.

No obstante, en los últimos meses, sobre algunos de ellos se han producido nuevas actualizaciones recientes, tanto por la rapidez de avance de la tecnología implicada como por deficiencias e incoherencias en cuanto a los productos incluidos en su ámbito de aplicación y a los procedimientos de evaluación de la conformidad. Ello hace necesario mejorar, simplificar y adaptar las disposiciones de estas directivas a las necesidades actuales del mercado, así como establecer normas claras acerca de cómo se pueden comercializar los productos que están cubiertos por las disposiciones de este Reglamento, dentro de un marco específico.

En esta línea, por ejemplo, la FDA aprobó recientemente la Ley de Asignaciones Consolidadas que incluyó autorización para que la FDA regulara la ciberseguridad de los dispositivos médicos. Esta ley exige que los fabricantes de dispositivos médicos presenten planes de mantenimiento y monitoreo de seguridad, respalden los ciclos de vida de seguridad de los dispositivos a través de actualizaciones de software y proporcionen SBOM para dispositivos nuevos. Actualmente, la FDA continúa estudiando requisitos a la espera de publicar una guía nuevamente actualizada.
De manera análoga, la UE ha publicado el Reglamento (UE) 2023/607 del Parlamento Europeo y del Consejo, de 15 de marzo de 2023[1], por el que se modifican los Reglamentos (UE) 2017/745 y (UE) 2017/746 en lo que respecta a las disposiciones transitorias para determinados productos sanitarios y productos sanitarios específicos para diagnóstico *in vitro* (In Vitro Diagnostic Medical Devices Regulation, IVDR). El Reglamento introduce una ampliación escalonada del período transitorio previsto en el Reglamento (UE) 2017/745 sobre productos sanitarios (European Medical Device Regulation, MDR), sujeto a determinadas

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2023.080.01.0024.01.ENG

condiciones. También suprime tanto en el MDR como en el IVDR el plazo de "liquidación", tras el cual los dispositivos comercializados antes o durante los períodos transitorios que aún se encuentran en la cadena de suministro habrían tenido que ser retirados. Con ello, la eliminación del plazo de "liquidación" proporciona una mayor claridad en la cadena de suministro de dispositivos médicos. Este documento se ha definido tomando como prioridad el hecho de garantizar un marco regulatorio sólido, transparente y sostenible y mantener un alto nivel de seguridad, al tiempo que se apoyaba la innovación. Estos recientes cambios sugieren la necesidad de que España incorpore y adapte estas regulaciones a su propio contexto para asegurar un marco regulatorio sólido y sostenible que respalde la seguridad y la innovación en el sector de la salud.

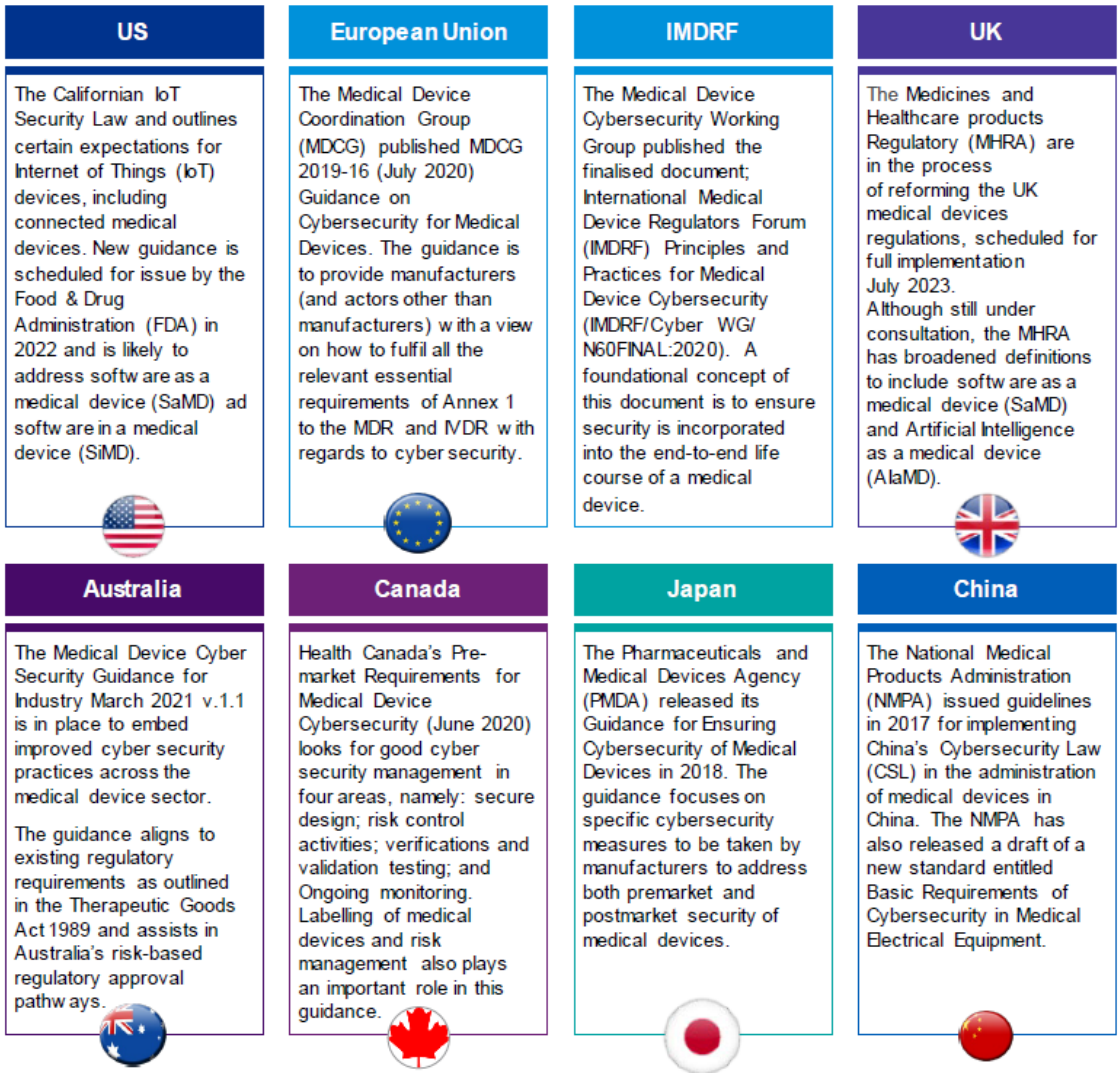

Figura 3. Documentos de orientación y directivas mundiales representativas de dispositivos médicos conectados

Adicionalmente, la Unión Europea ha propuesto la Ley Europea de Resiliencia Cibernética con el objetivo de mejorar la seguridad de todos los dispositivos IoT vendidos en Europa, donde la seguridad no es actualmente un requisito obligatorio. Esta propuesta implica que los dispositivos IoT deben contar con una configuración predeterminada de "nivel adecuado de

ciberseguridad habilitado", prohíbe la venta de productos con vulnerabilidades conocidas y busca minimizar el impacto de incidentes de seguridad. A pesar de que la implementación de las medidas de seguridad aún no está completamente definida en ambos casos, estos representan los primeros pasos fundamentales para fomentar la adopción generalizada de controles de seguridad en dispositivos IoT en Europa. En el caso de España, es imperativo mantener una estrecha vigilancia sobre la implementación de estas regulaciones y considerar activamente su propia adopción. Esto no solo servirá para proteger a los ciudadanos españoles, sino que también fortalecerá significativamente la seguridad de los dispositivos IoT en el país, contribuyendo así a un entorno más seguro y confiable para la creciente infraestructura de dispositivos conectados en el territorio nacional

3. IOT E INTELIGENCIA ARTIFICIAL EN LA PROVISIÓN DE SOLUCIONES INNOVADORAS PARA LA PROMOCIÓN DE LA AUTONOMÍA Y VIDA INDEPENDIENTE EN EL HOGAR

Como se ha avanzado al inicio del documento, los dispositivos IoT y sistemas Web of Things (WoT) aplicados a la atención sanitaria tienen beneficios tanto en el contexto hospitalario como en el extrahospitalario. Uno de ellos es la posibilidad de captar múltiples y heterogéneos datos del entorno en el que el paciente se desenvuelve durante sus actividades en la vida diaria. Esta captación de datos puede permitir crear entornos físicos inteligentes que favorezcan el apoyo tanto en la predicción de problemas de salud, como en el tratamiento y monitorización del paciente una vez que abandona el entorno clínico y vuelve a su contexto habitual, en el cual pasa la mayor parte de su tiempo y en donde genera un gran volumen de información valiosa con una elevada validez ecológica. Por ello, generar ecosistemas inteligentes apoyados en sistemas IoT y WoT supone un fuerte potencial para la asistencia a pacientes en fase de recuperación de problemas médicos, entre ellos el ictus, en el contexto extrahospitalario. En definitiva, la creación de entornos inteligentes en el hogar busca promover la autonomía y vida independiente en el hogar (enfoque conocido internacionalmente como '*Ambient Assisted Living*'). En esta línea, la Comisión Europea reconoce que las funcionalidades de los hogares inteligentes son importantes para la población que envejece y explica que el IoT puede "aumentar la eficiencia en la atención, promover la independencia y mejorar la calidad de vida de las personas mayores y sus cuidadores".

Dentro de este contexto, los sistemas y plataformas de IA desarrollados hasta la fecha son numerosos, estando estos adaptados a diferentes necesidades de los usuarios y condiciones de salud con el objetivo último de maximizar la información recabada para mejorar la calidad de vida de las personas y de su entorno más cercano.

Este tipo de soluciones plantea numerosos beneficios potenciales y da respuesta a importantes retos, como el creciente envejecimiento poblacional. No obstante, también lleva aparejados (al igual que se ha indicado en torno a los dispositivos IoT) importantes retos emergentes que resulta necesario afrontar para garantizar la provisión de servicios, no sólo de calidad, sino también adecuados desde el punto de vista de seguridad y dignidad de la persona, los cuales se indican posteriormente con mayor detalle.

3.1. Modelos de IA dirigidos a la promoción de la vida independiente en el hogar

Como se ha mencionado, el desarrollo tecnológico de los dispositivos IoT y entornos WoT está permitiendo incrementar la generación y capacidad de captación de datos extrahospitalarios en entorno real. Esta gran, y creciente, cantidad de información puede ser posteriormente explotada con herramientas avanzadas de Inteligencia Artificial que, por ejemplo, permitan realizar la predicción de eventos de salud que favorezcan la prevención o intervención

temprana. De este modo, la IA ha emergido como una herramienta que aporta una interesante capacidad de apoyo a la toma de decisiones también en el contexto extrahospitalario, permitiendo el apoyo objetivo del seguimiento de las intervenciones, el reajuste y personalización de los itinerarios clínicos que pueden maximizar la recuperación o, incluso, la modificación del tratamiento en caso de ser necesario, entre otros aspectos.

Dentro de este contexto, es posible emplear múltiples técnicas de IA. Entre ellas, los modelos de IA con mayor desarrollo e implantación se basan, por orden de popularidad, en deep learning (DL), procesamiento del lenguaje natural (PLN), instance-based learning y técnicas de clustering. De entre ello, el dominio del DL se debe a la enorme complejidad y heterogeneidad de los datos que deben captar, procesar y generar los sistemas de IA, estando generalmente basados en numerosas fuentes de datos recibidos de forma continuada en formato de imágenes, eventos acústicos (e.g. pasos), información conversacional, métricas conductuales (e.g. actividad física o sueño) o indicadores biológicos (e.g. presión arterial, temperatura corporal), entre muchos otros (Jovanovic et al., 2022).

Más en concreto, dentro de los modelos de DL, los algoritmos más comunes en la aplicación de este tipo de soluciones han sido las redes neuronales convolucionales. Esto es debido a que permiten la transformación de datos recibidos de los diversos sensores en representaciones basadas en imágenes, así como detectar los movimientos a través de cámaras. En el campo del PLN, si bien uno de sus primeros usos fue el reconocimiento y comprensión del lenguaje, en los últimos años, gracias a la incorporación de modelos generativos, su aplicación ha virado hacia la generación de diálogos y provisión de información, principalmente mediante robots que interaccionan con las personas usuarias. Por otra parte, los modelos de instance-based learning están siendo relegados a un menor uso debido al creciente avance del DL, mientras que las técnicas de clustering han destacado en este contexto por su utilidad en contextos en que, por diversos motivos (e.g. cese en el uso de un dispositivo vestible) no se cuenta con información completa de la persona a lo largo del tiempo, pero su perfilado en base a tareas previas o personas con comportamientos similares permite predecir una secuencia de acciones de la persona a partir de dicho perfilado con datos asociados a su conducta habitual (Jovanic et al., 2022).

3.2. Principales casos de uso

Dentro del fomento de la vida independiente en el hogar, la IA se ha utilizado principalmente para la provisión de apoyo en las actividades diarias significativas para la persona y para el reconocimiento de dichas actividades. En el primer caso, destacan las soluciones dirigidas a mejorar la movilidad funcional individual, empleando para ello formatos diversos como robots de apoyo a la marcha o dispositivos vestibles (i.e. gafas basadas en Realidad Aumentada para facilitar el tránsito por espacios físicos a personas con problemas de visión). Por otro lado, el reconocimiento de patrones de movimiento y de actividad física suponen otra de las principales aplicaciones, tratando de promover con ello diferentes aspectos de salud, instrumentales y de bienestar (Jovanic et al., 2022). No obstante, a pesar de las múltiples

aplicaciones creadas en este sentido, existe un importante reto dirigido a la predicción de patrones de movimiento de la persona a medio y largo plazo.

Atendiendo más específicamente al caso de uso planteado en IBERUS, existen pocas propuestas encaminadas a la rehabilitación física personal, en comparación con los programas enfocados en la movilidad general o el reconocimiento de la actividad ya citada. Es decir, respecto a aquellos con un propósito más básico de mera promoción de la salud, los cuales no permiten abordar problemas o patologías específicas que exigen unos requerimientos concretos para que estos tengan utilidad práctica.

Dentro de la rehabilitación de ictus, es posible identificar algunas aplicaciones basadas en smartphone que buscan (por frecuencia de uso): promover la funcionalidad de extremidades superiores, facilitar el uso y adherencia a la medicación, favorecer la movilidad funcional, apoyar la rehabilitación del lenguaje y de habilidades cognitivas, facilitar el control del tronco, proveer de asistencia en las actividades de la vida diaria, mejorar la funcionalidad de extremidades inferiores y mejorar la seguridad del hogar (Burns et al., 2020).

A la vista de esta información, es posible observar cómo las soluciones presentan un alto grado de especificidad, siendo un reto complejo pendiente en este campo, en consecuencia, la creación de ecosistemas conectados con un carácter más integral y complejo encaminados a la rehabilitación terapéutica, pero que puedan ser replicables y transferibles a otros trastornos del sistema neuromusculoesquelético u otras patologías. Sumado a ello, otro de los retos es que dichos ecosistemas presenten una arquitectura abierta que permita la interoperabilidad. Con este enfoque, resultaría viable integrar múltiples fuentes de datos (tal y como se plantea en IBERUS) de forma progresiva para maximizar el verdadero potencial de los sistemas de IA.

3.3. Tecnologías empleadas en el despliegue de soluciones innovadoras en el hogar

Casi sin darnos cuenta estamos viviendo una transformación de nuestros hogares. En poco tiempo, hemos comenzado a convivir con elementos inteligentes que nos hacen la vida más fácil como agentes conversacionales, acelerómetros en dispositivos digitales que portamos a diario o sensores de métricas corporales (e.g. para controlar la glucemia en diabéticos), entre otros. Hablamos de numerosos dispositivos cotidianos que, gracias a la tecnología, pueden comunicarse entre ellos dentro del citado ecosistema WoT y generar el ya expuesto entorno inteligente, aportando información continua de la persona que puede ser explotada con fines terapéuticos, cada vez en mayor medida.

De entre ellas destacan notablemente los dispositivos basados en IoT debido a que, generalmente, estos permiten preservar en mayor medida la privacidad del usuario y, además, presentan un carácter especialmente flexible, pudiendo actuar como elementos pasivos (e.g. registrando las condiciones del ambiente en el que se desenvuelve la persona), pero también cuentan con capacidad para adoptar un rol más activo (e.g. como medio para sugerir actividades a realizar, por ejemplo, dentro de un programa de rehabilitación).

Si bien se han investigado y aplicado otras alternativas que pueden parecer más innovadoras, como la robótica asistencial o los dispositivos vestibles, estas no cuentan realmente con un amplio uso en entornos reales, más allá del contexto de investigación. En el caso de la robótica asistencial, debido a su alto coste de desarrollo e implantación, y sus propósitos mayoritarios se dirigen a ofrecer compañía y asistencia. Por otro lado, en el caso de las tecnologías vestibles, su reducida aplicación suele deberse a una percepción de elevada intrusividad que limita su aceptación y consecuente uso, especialmente en determinadas circunstancias o entornos en donde la demanda de privacidad es más elevada (aspecto referido en la Sección 2) (Jovanic et al., 2022).

Si bien en esta sección se han apuntado algunas barreras o retos asociados al despliegue y uso de este tipo de soluciones en entornos reales (e.g. intrusividad, privacidad, etc.), a continuación, se proveen una serie de retos adicionales que deben ser tenidos en consideración y abordados para proveer de soluciones efectivas.

3.4. Retos asociados a las tecnologías de visión e IA en la creación de entornos inteligentes en el hogar

Como se ha comentado, las soluciones para la vida independiente pueden emplear múltiples dispositivos para monitorizar un entorno y a sus habitantes, recopilando información que permite describir acontecimientos, acciones, personas, objetos e interacciones entre todos ellos. Por este motivo, es urgente un enfoque ético y una comprensión profunda de todas las implicaciones asociadas a los dispositivos de monitorización pues, al margen del efecto sobre las personas, son aspectos también relevantes tanto para su aceptación inmediata como para su uso a largo plazo por parte de los potenciales usuarios.

Como se ha avanzado, una de las cuestiones principales es el hecho de que estas soluciones pueden ser consideradas intrusivas por algunos usuarios finales, como las personas que reciben la intervención, así como los cuidadores profesionales e informales.

Entre los retos pendientes para el desarrollo de futuras tecnologías para la vida independiente, se destacan varios aspectos, los cuales han sido agrupados en tres ámbitos: ético, legal y social (Figura 4), en base a la categorización de Ake-kob et al. (2021).

Figura 4. Resumen de retos para la adopción de tecnologías y generación de entornos inteligentes en el contexto extraclínico

3.4.1. Retos éticos

- **Intrusividad y autonomía:** la percepción subjetiva de intrusividad es una de las principales barreras para conseguir su adopción en el hogar. Dentro de esto hay que analizar tanto la posible intrusividad física como la mental (e.g. sensación de sentirse observados), como el grado de visibilidad del dispositivo. Si los dispositivos son muy visibles, pueden generar sentimientos de estigma, y en último término, distorsionar el comportamiento del usuario y afectar a su sentimiento de libertad e independencia.
- **Consentimiento y propiedad de los datos:** uno de los dilemas éticos vigentes es si en el caso de que la persona olvide que está siendo supervisada por los dispositivos IoT, el consentimiento que otorgó en un primer momento sigue siendo válido o debe revisarse de forma periódica. Por otro lado, existe el debate sobre los derechos de propiedad de los datos cuando estos tienen potencial valor más allá de la supervisión del usuario, por ejemplo, por uso por terceros para fines de investigación. En este último caso, uno de los dilemas es quién sigue siendo el propietario final de los datos (i.e. el usuario o el servicio que provee de las tecnologías), así como la pregunta sobre cómo gestionar estos consentimientos de uso de los datos.
- **Privacidad del usuario para usos secundarios de los datos:** el sector salud es especialmente sensible a aspectos de privacidad y estrictas regulaciones de estas, en comparación con otros sectores como el comercio electrónico. Esto es debido a que contiene datos altamente sensibles y especialmente delicados en caso de ser revelados. La falta de una protección robusta de los servidores donde se almacenan estos datos del usuario puede llevar a violaciones de la privacidad, y exponer dichos datos a terceros, perdiendo el control de los mismos y no habiendo autorizado explícitamente sobre su uso, independientemente de los beneficios que pueda generar.
- **Desigualdades en el acceso a las tecnologías para la vida independiente basadas en IA:** la población mayor y sus cuidadores, en caso de tenerlos, suelen ser el colectivo

objetivo para estas tecnologías. Sin embargo, son uno de los segmentos poblacionales que puede presentar más barreras a la hora de adoptarlas. Primero, la falta de conocimiento tecnológico de este grupo puede llevar a no ser conscientes de las posibilidades de los dispositivos IoT. Segundo, el diseño de estos sistemas no está lo suficientemente adaptado a sus preferencias y necesidades. Tercero, el coste de las tecnologías puede dificultar su adopción en colectivos y centros de bajos recursos económicos, lo que se une al hecho de que no suelen ser financiadas por el sistema sanitario ni los seguros médicos. Finalmente, existe aún una notable falta de evidencia empírica de estos ecosistemas en términos de utilidad clínica.

3.4.2. Retos legales

- **Protección de datos desde el diseño:** en Europa, el diseño e implementación de los entornos inteligentes debe cumplir con el Reglamento General de Protección de Datos (RGPD). A pesar de su importancia, su operativa en la práctica está mostrando dificultades ya que, en el caso de las tecnologías para la vida independiente, hay que tener en cuenta que el tipo de datos que generan son altamente dependientes de su contexto, implicando entonces la aplicación de diferentes leyes según estos.
- **Ciberseguridad:** los entornos inteligentes son enormemente complejos a la hora de asegurar sus sistemas IoT debido a la heterogeneidad de los dispositivos utilizados. A esto se suma el hecho de que, durante muchos años, los dispositivos IoT han dirigido sus esfuerzos en avanzar en su interoperabilidad, teniendo como contrapartida el hecho de no velar especialmente por su seguridad, mostrando una clara debilidad en este sentido que debe ser afrontada.
- **Regulación de dispositivos médicos y leyes de salud:** Los dispositivos médicos se consideran objetos de alto riesgo, lo que implica mayor escrutinio legal, derivando en que su entrada al mercado sea más costosa económicamente y demorada en el tiempo, limitando así sus potenciales beneficios sobre las personas. Los desarrolladores de entornos inteligentes médicos deben tener en cuenta además las leyes de protección del paciente en el contexto sanitario, que son diferentes y más estrictas que las relacionadas con dispositivos con fines exclusivamente comerciales. Esto supone un reto en el sentido de añadir más pasos y complejidad en el desarrollo del entorno inteligente dirigido a mejorar la independencia en el hogar, demorando su salida al mercado, en comparación con dispositivos similares, pero con fines puramente comerciales.
- **Protección del consumidor:** los dispositivos tecnológicos deben cumplir con las leyes relacionadas con la protección de las personas usuarias. En el caso de dispositivos médicos, buscan asegurar que los los entornos inteligentes no promueven finalidades o utilidades inexactas, pudiendo anunciarlos como generadores de beneficios más allá de los reales si las leyes no hacen una cobertura específica de estos temas. Sin embargo, actualmente el alcance de estas leyes para estas tecnologías es ambiguo.
- **Propiedad intelectual:** La definición de patentes de herramientas basadas en software no es una opción aún posible en la Unión Europea, siendo viable el registro y la propiedad intelectual de algunos componentes, como las instrucciones del producto o

datos generados por el dispositivo; pero no incluyendo otras cuestiones como, por ejemplo, sus aspectos funcionales. Esta limitación supone en muchos casos una cortapisa para las empresas a la hora de plantearse desarrollar estos productos y sacarlos al mercado, y por consiguiente mostrarlos ante la competencia, derivando en que los potenciales clientes de estos dispositivos no puedan beneficiarse de ellos.

- **Regulación de la IA:** Los dispositivos médicos basados en IA se consideran de alto riesgo, lo que supone que sus proveedores deben someterse a una serie de obligaciones legales antes de poder lanzarlos al mercado. Este proceso de cumplimiento de dichas obligaciones supone una demora en la salida al mercado y, por consiguiente, su uso por parte de las personas usuarias finales.

El reto de la privacidad desde el diseño (PbD) en el caso de IBERUS: un ejemplo práctico

Tal y como se ha expuesto con anterioridad, las soluciones de IoT equipadas con IA en el entorno domiciliario dirigidas al cuidado y promoción de la salud se están presentando y comercializando cada vez más como incorporaciones inteligentes esenciales que transformarán radicalmente los mercados de atención médica y bienestar a medio plazo. Sin embargo, al hilo de los retos anteriores, destaca cómo su uso puede ser considerado intrusivo por algunas personas usuarias finales. De hecho, las principales preocupaciones de las personas usuarias respecto a estas soluciones son la privacidad y la aceptación (Loncar-Turukalo, Zdravevski, Machado da Silva, Chouvarda y Trajkovik, 2019).

Así, es evidente que la presión por lanzar rápidamente al mercado dispositivos de este tipo no puede pasar por alto el hecho de que los entornos en los que operan son en su mayoría privados, como el hogar. Por ello, deben considerarse, al menos, dos cuestiones esenciales para su diseño y despliegue.

Por un lado, llevar a cabo una **evaluación de la tecnología** respecto a criterios esenciales ligados con:

- **Su bondad**, es decir, qué beneficios aportará este nuevo dispositivo, para quién, durante cuánto tiempo y si existen mejores alternativas. Esto requerirá un análisis muy detallado para determinar quién se beneficiará. Una solución tecnológica que permite que una persona viva en su propia casa y monitorizada de manera rutinaria por un tercero puede brindar beneficios a este último, pero no necesariamente es la mejor opción para la propia persona a la que se supone que brinda beneficios.
- Un **análisis de riesgo/beneficio**, alineado con el concepto de “ética desde el diseño” para determinar todos los riesgos involucrados, tanto actuales como futuros, y evaluarlos en comparación con los beneficios.
- El respeto a la **autonomía**, lo que requiere una comprensión de la responsabilidad conferida a un adulto autónomo y una apreciación del hecho de que esto no se aplica a todas las personas, como lo establece la ley.
- El mantenimiento de **información confidencial y datos** que pueden revelar información privada, pudiendo implicar riesgos de divulgación de la misma.

Por otra parte, potenciar la **privacidad desde el diseño** (PbD), ya citado en la Sección 2.4.1., concepto originado en 1990 gracias a Ann Cavoukian, ex Comisionada de Información y Privacidad, que, desde entonces, se ha convertido en un principio fundamental en la protección de la privacidad y la gestión de datos personales a raíz de una evolución constante que ha implicado diferentes hitos asociados a los Principios de Tecnologías de Privacidad (PETs), destacando:

- **Informe de la Comisión Europea de 2007**: Promovió y respaldó el desarrollo de PETs.
- **Resolución de Jerusalén de 2010**: Reconoció a la PbD como un componente esencial de la protección de la privacidad y promovió su adopción en la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad.
- **Informe de la FTC de 2012**: Mencionó la PbD como un principio en su marco de privacidad y recomendaciones de implementación.
- **Directrices de Privacidad de la OCDE de 2012**: Reconocieron la privacidad por diseño como un nuevo concepto a implementar.
- **Publicación del Reglamento General de Protección de Datos en 2016:** Incluyó, en su Art. 25, la identificación de los responsables del tratamiento de datos, quienes son responsables de implementar medidas por diseño y por defecto. Aunque esto no considera que un tercero a menudo diseñe infraestructuras técnicas, impone el deber de cumplir con la normativa al responsable de los datos tan pronto como este determine los medios y fines del procesamiento.
  Dicho artículo requiere, además, que los responsables de los datos consideren la tecnología actual, los costos de implementación de dicha tecnología, el contexto y las circunstancias del procesamiento de datos, así como el riesgo asociado con dicho procesamiento. Sin embargo, estos aspectos son bastante amplios y otorgan mucho margen para que los responsables de los datos determinen las medidas adecuadas en un contexto particular.
- **Actualización de la Convención 108 en 2018**: Incluyó un mandato sobre la PbD en su protocolo para garantizar la compatibilidad y coherencia con otros marcos legales de protección de datos, especialmente con la Unión Europea.

No obstante, hasta la fecha, la responsabilidad de garantizar la legalidad del procesamiento de datos, junto con la preservación de la privacidad, seguridad, calidad de los datos y el respeto de los derechos individuales, recae en manos de aquellos a quienes se les confía la gestión de los datos, siendo su responsabilidad solicitar a los desarrolladores dentro de su organización y a terceros contratados que implementen las medidas técnicas y organizativas apropiadas con este fin. En resumen, lo que se puede desprender de manera concluyente es la **necesidad de desarrollar metodologías/técnicas que permitan la integración fiable de valores como la privacidad y la protección de datos** en los sistemas de visión e IA a la hora de desplegar sistemas asociados a entornos inteligentes en el hogar.

En esta línea, la salvaguarda de la privacidad asociada a sistemas que emplean visión por computador se justifica principalmente por dos razones fundamentales. La primera reside en la protección de la identidad, donde se torna imprescindible ocultar la identidad de una persona frente a entidades que efectúan análisis de imágenes sin autorización, las cuales

pueden corresponder a modelos de aprendizaje automático que entrenan y deducen a partir de los datos de las personas usuarias sin su consentimiento, o individuos que visualizan imágenes sin contar con el permiso adecuado para acceder a ellas. Y la segunda vinculada a la propia confidencialidad, tanto por la divulgación de aspectos de la apariencia (e.g. si la persona está desnuda en su domicilio en momentos en que no se requiere el uso de las soluciones), como de conductas o comportamientos que no deben ser objeto de tratamiento (e.g. interacciones con terceros). Es en este punto en donde el enfoque de Privacidad por Diseño (PbD) se erige como un marco que persigue garantizar la privacidad.

Al respecto de esta última cuestión, en los últimos años, se han propuesto diferentes métodos para preservar la privacidad visual con el fin de proteger la identidad. Tal y como se muestra en la Figura 5, extraída de Ravi, Climent-Pérez y Florez-Revuelta (2023), estos se pueden agrupar en cinco categorías: métodos de intervención, visión ciega, procesamiento seguro, ocultación de datos y ofuscación visual.

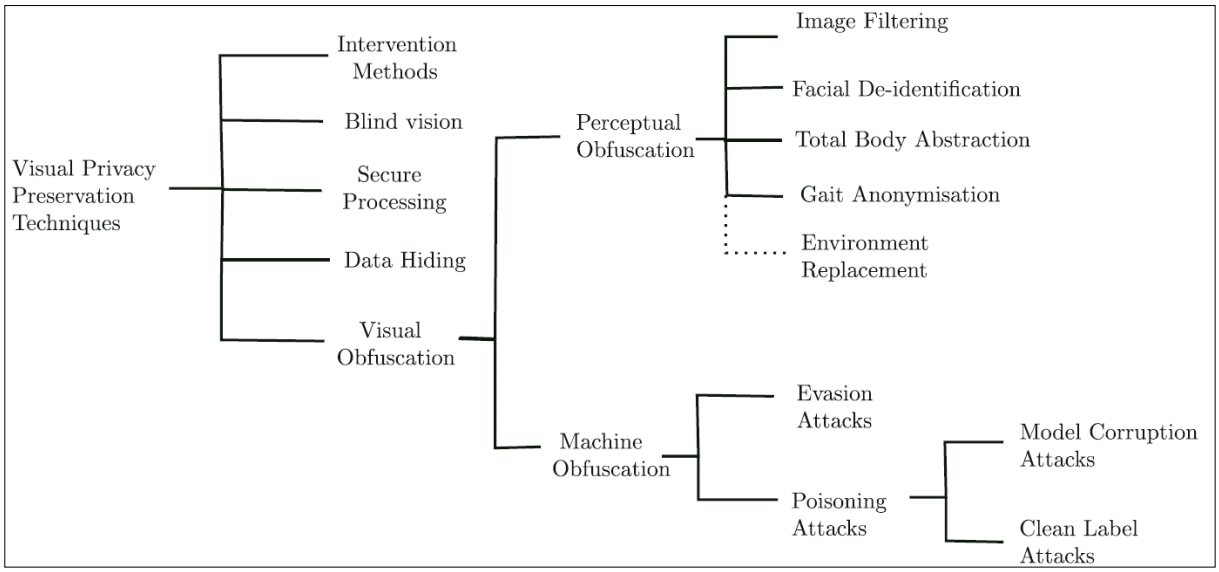

Figura 5. Taxonomía de las técnicas de preservación de la privacidad visual en el hogar

Atendiendo al conjunto de tecnologías implicadas en este documento, y a modo de ejemplo práctico, a continuación, se ha empleado una de las funcionalidades del demostrador desarrollado en IBERUS dentro del entorno extraclínico. Para ello, se ha utilizado el desarrollo ligado a la monitorización de ejercicios de rehabilitación en el hogar, a partir del cual se detallan las medidas que, basadas en PbD, ha sido empleadas para garantizar la privacidad en cuanto a la 1) **abstracción corporal** (i.e. ofuscación perceptual) y 2) el **procesamiento seguro** de la información.

Como se ha indicado, como ejemplo práctico se emplea uno de los módulos desarrollados dentro del ciclo de vida de la Red de Excelencia, dirigido a la provisión, ejecución y evaluación postural de ejercicios de rehabilitación, el cual forma parte del demostrador en entorno domiciliario asociado a medio rural.

Ofuscación perceptual mediante modelos de esqueleto humano en visión por computación

Dentro del conjunto de técnicas disponibles para garantizar la privacidad a la hora de analizar la imagen captada mediante cámara web en el domicilio de la persona usuaria, se ha optado por el **reconocimiento de acciones basado en el esqueleto humano** (*Skeleton-based action recognition*, por sus siglas en inglés).

El reconocimiento de acciones basado en esqueletos se ha convertido en uno de los temas más populares de investigación utilizados en métodos de IA, como la visión por computador. La tarea consiste en analizar las características de las articulaciones humanas y clasificar con precisión sus comportamientos mediante técnicas de aprendizaje profundo (i.e. Deep Learning).

El uso del esqueleto ofrece numerosas ventajas únicas en comparación con otras modalidades de datos, como robustez, tamaño reducido, resistencia a las interferencias de otros datos (e.g. luz natural, fondo ambiental…), etc. (Xin et al., 2023). En particular:

- Los datos del esqueleto proporcionan **información detallada** sobre la posición y el movimiento de las articulaciones humanas proporcionando una representación estructurada de la postura, lo que facilita la construcción de características espacio-temporales y de movimiento, incrementando la precisión del reconocimiento y la comprensión de la postura en términos de relaciones articulares
- Habilita un **seguimiento robusto** de las articulaciones en situaciones donde las condiciones de iluminación, fondo o apariencia de la persona pueden variar, lo que permite la detección de posturas en una variedad de entornos y situaciones, especialmente en entornos complejos.
- Es una técnica extremadamente **eficiente** en cuanto a necesidades de computación, lo cual es especialmente beneficioso para la investigación de aprendizaje profundo en entornos con recursos limitados y, en este caso, altamente útil para su despliegue en entornos domiciliarios, en donde el equipamiento no debe ser sofisticado.
- Permite analizar y procesar, exclusivamente, la postura y el movimiento, **descartando información no esencial**, que este caso, además, garantiza la privacidad.

A modo de síntesis, esta técnica implica el reconocimiento de acciones humanas a partir de una secuencia de datos de articulaciones esqueléticas en 3D sobre los que desarrollar algoritmos que puedan comprender y clasificar el movimiento, y en este ejemplo práctico, la pose o ejecución del ejercicio propuesto. Así, en una primera etapa se estima el esqueleto en 3D (identificando las articulaciones, conectando estas articulaciones para configurar las partes del cuerpo y estableciendo relaciones entre las mismas, Figura 6), a partir de secuencias de fotogramas RGB-D mediante estimación de pose en 3D. Posteriormente, los movimientos se analizan y clasifican utilizando un conjunto de modelos de reconocimiento de acciones basados en estos esqueletos previamente entrenados.

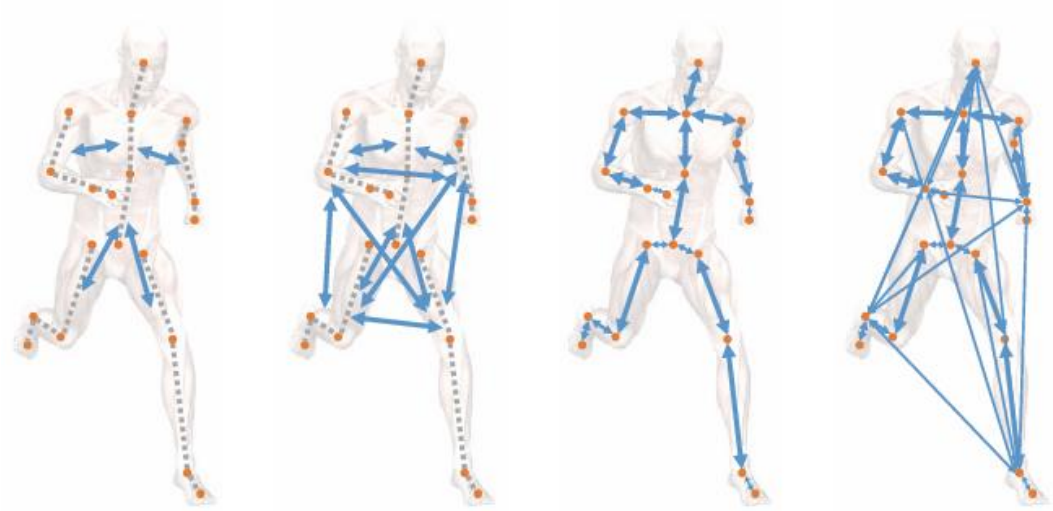

Figura 6. Síntesis del proceso de creación de esqueleto a partir de visión por computador

Bajo esta lógica, dentro de IBERUS, se ha procedido a identificar un conjunto de ejercicios de rehabilitación en base a los cuales se ha entrenado un conjunto de modelos de reconocimiento de acciones que permiten evaluar, única y exclusivamente, la pose de la persona usuaria (i.e. esqueleto en color azul turquesa) de cara a verificar tanto la ejecución del ejercicio como la calidad del mismo (Figura 7).

Figura 7. Usuario modelo para análisis de movimiento bajo técnica de esqueleto

En base a ello, la persona usuaria cuenta con una interfaz en la que identifica el ejercicio a realizar, visualiza su ejecución correcta y observa, en tiempo real, la calidad y cumplimentación de su ejecución, recibiendo feedback a la par que garantizando su privacidad. A modo de ejemplo, la Figura 8 muestra a un usuario modelo ejecutando un ejercicio concreto en la interfaz de paciente, sobre cuya imagen se define el esqueleto para procesar la información sobre el modelo entrenado. En la misma interfaz se aporta

información sobre las instrucciones para la correcta ejecución, el número de repeticiones propuestas y el total de series a ejecutar y realizadas en tiempo real.

Figura 8. Ejemplo de interfaz de usuario durante la ejecución de ejercicios en el hogar

Procesamiento seguro de la información

Atendiendo a la ya expuesta relevancia de la privacidad, junto con las características ya descritas de ofuscación perceptual, el conjunto de la información generada y explotada mediante este módulo se ha caracterizado por su almacenamiento y procesamiento seguro ya desde el período de concepción de la misma (i.e. PbD).

De forma específica, el **acceso a la información** se lleva a cabo mediante un sistema de **autenticación y control de acceso personal**, asegurando que únicamente los usuarios autorizados, en este caso personas usuarias que ejecutan los ejercicios y profesionales sanitarios que realizan su seguimiento, tengan acceso a los servicios, recursos y datos.

Una vez iniciada la ejecución de los ejercicios, los algoritmos empleados permiten procesar datos privados de manera unidireccional, hecho que implica que tanto la base de datos generada como la consulta y sus resultados se mantienen en un entorno privado. Así, las imágenes captadas por la cámara web que permite la valoración de los ejercicios **no son almacenadas** en ningún caso, solo son procesadas en un equipo local (i.e. en el hogar) y reflejadas en pantalla, registrando exclusivamente el número de repeticiones que la persona usuaria lleva a cabo, tanto para guiar el ejercicio como para ofrecer información objetivo al profesional sanitario. Del mismo modo, los datos generados no se envían a ningún servidor externo para su procesamiento ni se exponen de forma abierta, aproximación que se repite respecto al modelo de entrenamiento generado (i.e. el modelo matemático que predice el movimiento), el cual es publicado en un servidor, pero omitiendo todos los ejemplos empleados para crear el modelo.

3.4.3. Retos sociales

- **Contexto sociopolítico en torno a su adopción**: En el momento sociohistórico actual en Europa, las tecnologías en las que se basan los entornos inteligentes (e.g. visión por

computador) se perciben, generalmente, más como un medio de vigilancia que como una herramienta para facilitar los cuidados de salud, siendo una importante limitación en términos de aceptación y uso.

- **Aislamiento social**: Como ya se indicó en el apartado previo sobre aspectos prácticos asociados al cuidado, las principales personas objetivo de las tecnologías para la vida independiente son personas mayores, que viven tanto en el hogar como en entornos residenciales, teniendo de base un elevado riesgo de sentimientos de soledad en estas etapas vitales. Es crucial garantizar que la tecnología no sustituya la interacción social presencial necesaria para cualquier ser humano, pues el posible aumento de la soledad puede afectar negativamente al bienestar y la calidad de vida de estas personas.
- **Género y vulnerabilidad**: La mayoría de población en términos de personas mayores con necesidades de salud que residen en el domicilio en general y que tienden a vivir más cuando presentan discapacidades, así como el mayor porcentaje de personas que desempeñan tareas de cuidados informales son mujeres. Esta no es una cuestión baladí en términos de diseño, siendo fundamental su participación en esta fase de cara a minimizar posibles sesgos o brecha de género que genere un perjuicio a las personas usuarias.
- **Desigualdades sociales y consideraciones del espacio físico:** los colectivos privilegiados en cualquiera de los ámbitos vitales: económico, social, educativo, de clase social o cultural; suelen tener más facilidad de acceso a la tecnología por razones de accesibilidad económica y/o de conocimientos y competencias digitales. Esto es muy importante en el caso de los entornos inteligentes para la vida independiente, siendo más complejo su uso si se requiere aplicarlos en colectivos vulnerables o entornos desfavorecidos como entornos de baja penetración de medios digitales. Todo esto conlleva el reto de desarrollar e implementar tecnologías realmente inclusivas que reduzcan las asimetrías entre grupos sociales y permitan democratizar la tecnología.

3.5. Necesidad de un enfoque centrado en la persona

La IA centrada en la persona (HCAI por sus siglas en inglés, en referencia al concepto de Human-Centered Artificial Intelligence) pone el foco en las experiencias, satisfacciones y necesidades del usuario final de los sistemas de IA con el objetivo de potenciar y mejorar el rendimiento y utilidad de dichos sistemas. Paralelamente también se ocupa de analizar el impacto social de la IA, trasladándose en este caso a la influencia que pueden generar estos entornos inteligentes en la provisión de apoyo para la vida independiente en el hogar. En el caso de IBERUS, un enfoque en donde la persona esté verdaderamente en el centro, es especialmente relevante, pues sólo de este modo resulta factible comprender la interacción entre la innovación tecnológica con el cuidado de la salud, el bienestar y el ambiente interior. Esto permite proveer de insights significativos al profesional sanitario y de outputs personalizados para el individuo que se beneficia de este tipo de soluciones en su hogar.

Sumado a lo anterior, desde el punto de vista tecnológico, el principal beneficio derivado de esta aproximación está relacionado con la aceptabilidad real de esta tecnología por parte de

las personas y, en consecuencia, la fiabilidad y validez de los datos adquiridos. Esta es una cuestión especialmente relevante. Que los datos captados sean fiables, significa que reflejan el comportamiento natural de la persona. Es decir, que no se vean afectados por el condicionamiento del comportamiento individual debido a la conciencia de ser observado a través de dispositivos IoT, siendo un aspecto clave para la adecuada toma de decisiones. De este modo, cualquier tipo de solución en este ámbito debe tener como prioridad las necesidades de los usuarios, bajo un enfoque centrado en la persona, en el que las personas usuarias finales se impliquen y participen en todas las fases del proceso, desde el diseño hasta la validación y uso posterior. Precisamente en relación a este último punto, en general, una de las tareas pendientes es llevar a cabo evaluaciones de las soluciones generadas a largo plazo y en entorno real, yendo más allá de las pruebas de concepto y midiendo aspectos que no son técnicos, sino centrados en el usuario como la funcionalidad, aceptabilidad, utilidad e impacto de los sistemas (Cicirelli et al., 2021).

En un intento de que este tipo de soluciones se adhiera a principios básicos de HCAI, organismos públicos y privados han propuesto diversas guías modelo que permitan una sensibilización de este aspecto y una adherencia a algunos puntos básicos. En esta línea, cabe destacar especialmente el documento desarrollado por la Comisión Europea para la generación de soluciones de IA confiables (European Commission, 2019). En dicho documento, se alude a la necesidad de que los sistemas de IA sean transparentes (tanto en términos de uso como de comprensión de funcionamiento), dispongan de mecanismos de rendición de cuentas o responsabilidades (especialmente en ámbitos como el de la salud, en donde su impacto negativo puede ser potencial alto), promuevan el bienestar social y ambiental, se encuentren libres de sesgos, sean sensibles a la diversidad mediante la no discriminación y provisión de justicia, aseguren la privacidad de los datos de la persona, presenten sistemas robustos de seguridad y promuevan la supervisión y vigilancia por parte del humano.

Figura 9. Puntos esenciales que debe cubrir una solución de AI confiable ligado a los principios HCAI

Aunque ambiciosa, esta propuesta de aspectos ideales a considerar en términos de HCAI ha sido criticada por ser compleja de implementar en la práctica, debido a tener un planteamiento demasiado teórico y ambiguo e impidiendo que estos conceptos puedan ser realmente adoptados por los desarrolladores de IA. En este sentido, se hace necesario generar un mayor número de recomendaciones específicas y tangibles de estos principios para que puedan ser considerados en el desarrollo e implementación de soluciones para la vida independiente y, en términos generales para la salud.

Asociado con las recomendaciones previamente citadas de la Comisión Europea, este mismo organismo, a través del Grupo de expertos de alto nivel en inteligencia artificial (AI HLEG), ha elaborado una lista de autoevaluación (Assessment List for Trustworthy Artificial Intelligence - ALTAI[2]) para ayudar a evaluar si el sistema de IA que se está desarrollando, implementando, adquiriendo o utilizando cumple con los siete requisitos previamente citados. Además, es importante considerar que, debido al carácter evolutivo de los sistemas basados en IA, es recomendable que esta evaluación y estas consideraciones se tengan presentes de forma iterativa a lo largo de todo el ciclo de vida de las soluciones, incluyendo, obviamente, la reevaluación tras su uso continuado.

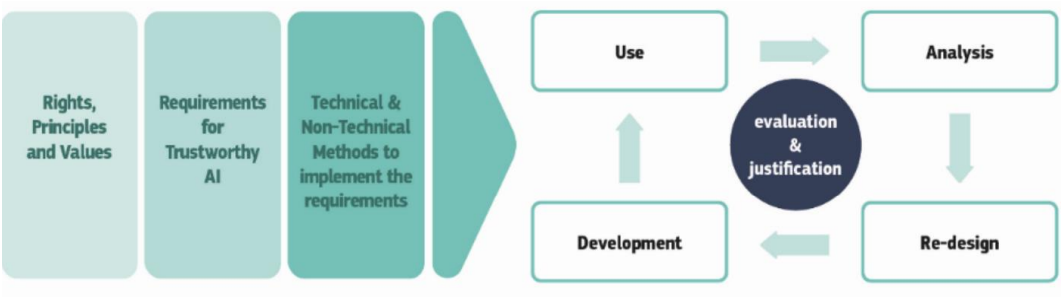

Figura 10. Fases propuestas en el proceso de implementación y evaluación de sistemas de IA confiables

Sumado a estas cuestiones, otro componente importante, para lograr que estas soluciones estén, realmente, centradas en la persona es considerar la experiencia del usuario (UX) en relación a las soluciones provistas.

Dicha experiencia incluye no sólo alinear la tecnología con sus necesidades y sensaciones subjetivas, sino también evaluar y considerar su impacto a nivel organizacional y social. Este último no es un aspecto superficial, pues diversos estudios que han analizado la perspectiva del usuario en sistemas de IA encuentran que sus prioridades son diferentes de las de los desarrolladores. Así, aunque ambos comparten la importancia de que el sistema sea útil y cumpla adecuadamente su función, para las personas usuarias es igualmente importante el impacto social que éste tiene, entendiendo impacto social como el apoyo a la hora de llevar a cabo tareas de forma más fácil y eficiente que por sí solos, beneficiándose a ellos y su entorno, y, en definitiva, generando cambios positivos en su vida. Igualmente, las personas usuarias también valoran especialmente que el sistema entienda sus necesidades y actúe conforme a sus preferencias personales, sintiéndose entendidos, en comparación con entender lo que el sistema hace, a lo cual dan una importancia menor. Obviamente, presentan también

[2] https://op.europa.eu/es/publication-detail/-/publication/73552fcd-f7c2-11ea-991b-01aa75ed71a1

preocupaciones respecto a su fiabilidad en términos de monitorización y predicciones, pero sobre ello prevalecen otras cuestiones como la facilidad de uso o la accesibilidad. Todas estas son cuestiones en las que resulta evidente que, sin la participación activa de la persona, no resulta verdaderamente viable alinear los intereses de ambas partes y, con ello, el uso y expansión tanto de los dispositivos IoT como de las soluciones basadas en IA continuará sin alcanzar su máximo exponente.

3.6. Buenas prácticas en el diseño de soluciones basadas en IA para la vida independiente

En la Sección 2.4 avanzamos los retos que tiene que solventar cualquier entorno inteligente basado en dispositivos IoT e IA, siendo además algunos particularmente sensibles para el caso que se plantea en IBERUS. Igualmente, en la sección 3.5 se ha introducido el enfoque basado en la persona y su potencial para contribuir a solventar estos retos. Uno de los problemas detectados en este ámbito es su ambigüedad, por lo que en esta sección se aportan una serie de buenas prácticas que, tanto la solución enmarcada en la Red de excelencia IBERUS, como cualquier otra persona o entidad que pretender desarrollar una solución innovadora en este contexto pueda tener en consideración, tratando de garantizar así que el producto final se alinee con las necesidades éticas, legales y sociales. A continuación se enumeran las buenas prácticas identificadas, tomando como referencia el trabajo elaborado por Ake-kob et al. (2022).

3.6.1. Buenas prácticas en el ámbito ético

Para asegurar la privacidad, promover el sentimiento de autonomía, reducir el sentimiento de intrusividad y considerar otros aspectos éticos asociados, se proponen las siguientes recomendaciones.

A nivel organizacional, en las instituciones sanitarias y sociosanitarias, resulta recomendable generar una serie de recursos asociados a los siguientes aspectos:

- Proveer de formación y material accesible a las organizaciones sobre cómo implementar los procesos éticos que requieran en su contexto profesional.
- Proporcionar explicaciones claras a las personas cuidadoras y organizaciones sobre cómo se ha desarrollado cada dispositivo, cómo cubre cada aspecto ético implicado y cómo serán integrados en la rutina diaria.
- Generación de contenidos (e.g. vídeos cortos, trípticos) con un lenguaje accesible para los colectivos de interés y no expertos en IA. Estos medios deberían incluir información sobre cómo funciona la tecnología, cómo la privacidad ha sido abordada desde el diseño y cómo uno puede dejar de usar la tecnología en un momento determinado (e.g. cómo desconectar los dispositivos cuando se desee).
- Aportar información sobre cómo se toman las decisiones que afectan a las personas usuarias en los entornos inteligentes. El desconocimiento de cómo se ha llegado a una decisión (e.g. recomendar al usuario en un momento dado la realización de una actividad de rehabilitación) puede generar incertidumbre y desconfianza.

- Por otro lado, en términos de desarrollo de los entornos inteligentes:
- El diseño de los dispositivos debe tener en cuenta desde el principio elementos relacionados con la privacidad, ya que la presión para llevar rápidamente al mercado dispositivos de IoT y aquellos equipados con IA no pueden pasar por alto el hecho de que los entornos en los que operarán son en su mayoría privados y estos involucran información sensible relacionada con la vida personal.
- Introducir mecanismos que aseguren maximizar la involucración de las personas cuidadoras y pacientes en todos los procesos de creación, desde el diseño hasta su despliegue y adopción, pudiendo con ello reducir el sentimiento de intrusividad y las preocupaciones relacionadas con la privacidad e incrementar la confianza en el sistema.
- Designar responsables de la protección de datos del sistema para aumentar la confianza de los usuarios, identificando claramente a quién/dónde acudir si tienen dudas o experimentan problemas relacionados con la privacidad durante el uso de los dispositivos.

Finalmente, a nivel gubernamental, sería interesante implementar campañas de divulgación y concienciación sobre la privacidad y la regulación legal en torno a estas tecnologías.

3.6.2. Buenas prácticas en el ámbito legal

En un primer marco más general, debe asegurarse que el diseño e implantación de los entornos inteligentes para el apoyo a la salud se ajuste a las exigencias regulatorias de cada país, atendiendo a cuestiones relacionadas con la seguridad de los productos, la protección de datos, la ciberseguridad, la propiedad intelectual, y el acceso a los datos por parte de organismos públicos, privados y gubernamentales. Existen marcos legales en el ámbito europeo para cada uno de los aspectos legales, pero hasta el momento, los entornos inteligentes no se encuentran regulados ni adaptados a nivel estatal, ni su cumplimiento legal reconocido por las autoridades legales pertinentes.

Sobre la protección de los datos, se propone lo siguiente:

- Promover la concienciación pública sobre el RGPD para que las personas comprendan y reivindiquen sus derechos en los casos en que sea necesario, siendo los colectivos vulnerables un grupo objetivo importante.
- Proporcionar directrices formales adicionales para facilitar a los desarrolladores la interpretación de la ley y promover tecnologías alineadas con aspectos importantes del RGPD en materia de productos y servicios.
- Proporcionar orientaciones claras sobre la distinción entre las distintas categorías de datos, siendo esta actualmente objeto de una gran inseguridad jurídica entre los Estados miembros de la Unión Europea.
- Sugerir enfoques metodológicos que sean aceptables para los reguladores, de modo que los responsables del tratamiento de datos puedan entender cómo cuantificar el

riesgo de reidentificación después de haber anonimizado o seudo anonimizado los datos.

- Aumentar la concienciación sobre el hecho de que la seudoanonimización y la anonimización no son suficientes, requiriendo medidas de seguridad adicionales.

Para empoderar y proteger a los usuarios y capacitar a los desarrolladores a la hora de desarrollar un manejo seguro del consentimiento de uso de datos, se propone:

- Reforzar la concienciación sobre el hecho de que el modelo de consentimiento único no es adecuado en el contexto de los entornos inteligentes. Con ello se sugiere fomentar el desarrollo de sistemas de consentimiento más flexibles y progresivos.
- Promover el desarrollo de herramientas para ocultar la identidad de las personas cuando no han dado su consentimiento.
- Fomentar la introducción de formularios breves, normalizados y fáciles de usar para los documentos informativos, presentando de forma precisa y eficaz todas las características relevantes en relación con el tratamiento de datos.
- Proveer de sistemas que permitan personalizaciones del grado de privacidad en función del consentimiento dado, incluso en tiempo real, en función de las necesidades de privacidad del usuario. Este tipo de versiones personalizadas permitiría cumplir de forma más adecuada el principio de minimización de datos.
- Formular códigos de conducta específicos sobre la aplicación del principio de minimización de datos en entornos inteligentes.
- Definir recomendaciones sobre periodos razonables de conservación de datos en entornos inteligentes.

Por último, se enumeran una serie de prácticas que permitan hacer el marco legal más accesible a todas las personas incluidas en el proceso, desde los mismos desarrolladores de entornos inteligentes, personal sanitario, hasta las personas cuidadoras y pacientes:

- Agilizar el cumplimiento de la legislación mediante directrices prácticas que desglosen los derechos y obligaciones de los usuarios finales. Para ello, pueden implantarse tecnologías que guíen a la persona objetivo a través del complejo marco jurídico (p. ej., árboles de decisión sencillos que ayuden a determinar la aplicabilidad de determinada legislación y ofrezcan recomendaciones al usuario).
- Reducir la jerga jurídica y redactar la legislación con frases claras y lógicas. Seguir y aplicar directrices que impulsen una legislación más precisa, como las iniciativas que buscan que la legislación esté "preparada digitalmente".
- Utilizar visualizaciones o herramientas audiovisuales para explicar los marcos legales a cumplir por los desarrolladores, y derechos y obligaciones para los usuarios.
- Concienciar sobre las consecuencias del incumplimiento y señalar cómo se puede exigir el cumplimiento y dónde presentar quejas formales.

Garantizar que las leyes se redacten de forma que puedan traducirse a un formato legible por los dispositivos e integrarse fácilmente en el diseño de los sistemas al inicio de su desarrollo.

3.6.3. Buenas prácticas en el ámbito social

Para reducir las desigualdades sociales en el acceso a cuidados sanitarios digitales, el contexto sociopolítico en el que se contextualiza el uso de los dispositivos y tener en cuenta las dimensiones de género y grupos vulnerables, se plantean las siguientes recomendaciones:

Desde el proceso de diseño:

- Aunque ya se avanzó en el apartado ético, se considera necesario que la toma final de decisiones se desarrolle de modo colaborativo con las personas usuarias finales y expertos en el ámbito de actuación (i.e. cuidadores, pacientes y profesionales de la salud), pues esto supondría mejorar su precisión, aumentar la confianza en los entornos inteligentes y optimizar la gestión del sistema sanitario.
- Introducir medios de integración de este tipo de soluciones con los servicios sanitarios, las cuales suelen construirse de modo independiente, siendo ideal que los modelos de IA en que emplean puedan nutrirse de los datos del sistema sanitario para complementar la información recogida mediante los dispositivos IoT y mejorar su toma de decisiones e impacto sobre las personas. Paralelamente, facilitarían el seguimiento de los pacientes y permitirían identificar cambios difíciles de observar en el contexto clínico. De este modo, mejoraría el cuidado integral y, por consiguiente, la calidad de vida de las personas.
- Asegurar la máxima personalización respecto a las circunstancias de la persona. Esto se puede conseguir involucrando a los usuarios desde la fase de diseño, como ya se ha mencionado en varias ocasiones, pero también implementando mecanismos de seguimiento para revisar periódicamente que la solución se adapte a los cambios en las necesidades que vayan surgiendo con el tiempo.

Recomendaciones para mejorar la accesibilidad digital:

- Introducir mecanismos que aseguren las infraestructuras digitales para los colectivos de interés (e.g. mejoras en la conectividad).

Desarrollar guías prácticas de uso de este tipo de dispositivos que faciliten las potenciales barreras en conocimientos y competencias digitales de las personas usuarias, así como fomentar campañas de educación digital accesibles para todos los colectivos.

4. LÍNEA FUTURAS

Atendiendo tanto al conjunto de información provisto en el documento, como a la literatura científica recientemente publicada, a continuación, se sugieren algunas líneas de trabajo en las que, a modo de decálogo y estructuradas en torno a tres grandes categorías, se considera necesario profundizar y proveer de nueva evidencia científica, suponiendo, a su vez, nuevas oportunidades que den continuidad al trabajo realizado en la Red de Excelencia IBERUS.

4.1. Oportunidades respecto a la atención sanitaria y el bienestar de las personas

- Toma de decisiones colaborativa: Los sistemas actuales de IA para la vida independiente toman decisiones de manera autónoma, impulsadas por los algoritmos de los modelos y los datos de entrada. La participación de usuarios expertos (e.g. profesionales clínicos y cuidadores) en el proceso de toma de decisiones puede mejorar su precisión, facilitar el aprendizaje automatizado sobre las personas usuarias y reducir la carga sobre los profesionales de la salud.
- Fortalecimiento de cuidadores y receptores de las soluciones digitales: Dado que estas soluciones se despliegan fuera del contexto sanitario formal, es fundamental considerar el cuidado y la atención para cumplir con los servicios de salud que deben abordar las preocupaciones de las personas participantes. La participación activa de las personas beneficiarias es crucial para una intervención exitosa de atención digital, desde la comprensión de los modelos de IA hasta el diseño y despliegue de tecnología específica.
- Intervenciones para la creación de entornos inteligentes: Los diversos estudios han considerado diversas tecnologías y plataformas para respaldar la vida independiente, sin embargo, se carece de un intercambio de conocimientos entre estudios sobre sus resultados y experiencias. El conocimiento sistematizado de modelos, dominios, tecnologías y beneficiarios puede guiar las intervenciones adaptadas a requisitos de atención clínica específicos, reforzando con ello las buenas prácticas y mitigando riesgos potenciales.
- Regulaciones y cumplimiento: Actualmente, el diseño y despliegue de este tipo de soluciones no están regulados, ni se reconoce su cumplimiento por las autoridades reguladoras a nivel mundial. Es fundamental avanzar hacia el cumplimiento de regulaciones tanto a nivel nacional como internacional para potenciar su implementación en la práctica sanitaria y su adopción general. Propuestas alineadas con la creación de repositorios compartidos de métodos de evaluación y directrices de diseño que respalden el cumplimiento y proporcionen una vista clara de cómo incorporar aspectos críticos durante el diseño en este tipo de tecnologías.

4.2. Implicaciones tecnológicas

- Transparencia y privacidad: Los modelos de IA, por su propia naturaleza, necesitan, generan y procesan grandes cantidades de datos relacionados con las personas, desde la recopilación y análisis intensivo de datos hasta la generación de recomendaciones personalizadas. En primer lugar, la tecnología debe ser transparente en cuanto a por qué y cómo se recopilan, analizan y utilizan los datos. En segundo lugar, debe respetar el derecho de la persona usuaria a controlar sus datos privados y comunicaciones y garantizar su privacidad. Ambas cuestiones son esenciales para generar confianza en este tipo de dispositivos.
- Integración con servicios de atención sanitaria: las soluciones para la promoción de la autonomía y la vida independiente en el hogar suelen ser desarrollados y desplegados como plataformas independientes, independientemente de los sistemas de atención médica institucionales. Avanzar en la interoperabilidad con la infraestructura tecnológica médica existente y los servicios digitales puede aumentar la eficiencia y efectividad de la prestación de atención sanitaria debido a una clara interrelación: los modelos de IA pueden ser alimentados con registros clínicos y procedimientos existentes de personas usuarias para mejorar la toma de decisiones; a la vez que los profesionales sanitarios podrían ser informados y/o alertados de manera oportuna y más objetiva sobre cambios en el comportamiento o estados de las personas usuarias que son difíciles de observar únicamente en entornos clínicos.
- Generación de soluciones inclusivas: Los modelos de IA tienden a centrarse en personas individuales como una relación persona-sistema, siendo especialmente complejo incluir dinámicas de grupo, como relaciones persona-sistema-clínico o la formación de grupos de pares de personas usuarias similares. Los futuros sistemas deben involucrar y moderar de manera equitativa a múltiples beneficiarios: pacientes, familias, cuidadores y personal de atención sanitaria.

4.3. Necesidades de investigación

- Toma de decisiones explicables: A medida que las capacidades de los modelos de IA aumentan, la ausencia de explicaciones tras los comportamientos automatizados genera incertidumbre en las personas usuarias debido a la falta de comprensión de cómo se toman esas decisiones específicas. Un requisito general para futuros modelos de IA debe ser proporcionar explicaciones comprensibles para personas sin experiencia o conocimiento específico en IA.
- Técnicas de evaluación: Las técnicas de evaluación existentes pueden categorizarse en funcionales (i.e. especializadas) y no funcionales (i.e. médicas y de usabilidad), existiendo además instrumentos para evaluar los algoritmos de los modelos de IA en términos de precisión y rendimiento o resultados médicos y relacionados con las personas usuarias (i.e. escalas estándar para condiciones clínicas particulares, entrevistas y cuestionarios). No obstante, para obtener una evaluación clara y válida

de la eficacia y eficiencia de los modelos de IA es necesario un conjunto más completo y coherente de métricas de evaluación intercategorías que se verifiquen en la práctica.

- Recomendaciones de diseño: Las actuales pautas de diseño actuales son únicamente sugerencias aplicadas a dominios y tecnologías específicos, implicando una elevada dificultad en cuanto aplicación y reproducción y, por ello, suponiendo una clara barrera para su adopción. Avanzar en la definición de procedimientos de presentación y bases de conocimiento estándar podrían ayudar a abordar este problema y proporcionar pautas prácticas generalizables y aplicables.

Tabla 4. Resumen de líneas futuras de trabajo

Líneas futuras de trabajo en la provisión de soluciones innovadoras para la promoción de la autonomía y vida independiente en el hogar IBERUS	
	Toma de decisiones colaborativa
	Fortalecimiento de cuidadores y receptores de las soluciones digitales
	Intervenciones para la creación de entornos inteligentes
	Regulaciones y cumplimiento
	Transparencia y privacidad
	Integración con servicios de atención sanitaria
	Generación de soluciones inclusivas
	Toma de decisiones explicables
	Incremento de técnicas de evaluación
	Recomendaciones de diseño

5. REFERENCIAS

Abdulameer, A., & Oubida, R. (2021). The Impact of IOT on Real-World Decisions in the next Stage.

Afzal, S., & Arshad, A. (2021). Ethical issues among healthcare workers using electronic medical records: A systematic review. *Computer Methods and Programs in Biomedicine Update, 1*. doi:10.1016/j.cmpbup.2021.100030.

Agencia Española de Protección de Datos. (2019). *Guía de Privacidad desde el Diseño.*

Ake-Kob, A., et al. (2021) State of the art on ethical, legal, and social issues linked to audio- and video-based AAL solutions. Alicante: University of Alicante, Available at SSRN: https://ssrn.com/abstract=3994835

Ake-Kob, A., Aleksic, S., Alexin, Z., Blaževičienė, A., Čartolovni, A., Colonna, L., ... & Tamò-Larrieux, A. (2022). Position paper on ethical, legal and social challenges linked to audio-and video-based AAL solutions. Obtenido de: https://futurium.ec.europa.eu/en/active-and-healthy-living-digital-world/library/position-paper-ethical-legal-and-social-challenges-linked-audio-and-video-based-aal-solutions?language=en

Ali, K., & Askar, S. (2021). Security Issues and Vulnerability of IoT Devices. *International Journal of Science and Business, 5*(3), 101-115.

Andrejevic, M. (2014). Big data, big questions the big data divide. *International Journal of Communication, 8*, 17.

Anmulwar, S., Gupta, A., & Derawi, M. (2020). Challenges of IoT in Healthcare. En *IoT and ICT for Healthcare Applications. EAI/Springer Innovations in Communication and Computing.* Springer, Cham. doi:10.1007/978-3-0

Miller, D.D. y Brown, E.W. (2018). Artificial intelligence in medical practice: the question to the answer? *Am J Med.*, 129–33. doi:10.1016/j.amjmed.2017.10.035.

Awad, A., Trenfield, S., Pollard, T., Ong, J., Elbadawi, M., McCoubrey, L., . . . Basit, A. (2021). Connected healthcare: Improving patient care using digital health technologies. *Adv Drug Deliv Rev*(178), 113958. doi: 10.1016/j.addr.2021.113958. doi:10.1016/j.addr.2021.113958

Azer, A., & Ahmed Abo Bakr, M. (2017). Desafíos éticos y cuestiones jurídicas de la IO. *12th International Conference on Computer Engineering and Systems (ICCES).*

Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2016). Ethical design in the internet of things. *Science and Engineering Ethics*. doi:10.1007/s11948-016-9754-5

Batool, A., Loke, S., Fernando, N., & Kua, J. (2021). Towards a Policy Management Framework for Managing Interaction Behaviors in IoT Collectives. *IoT, 2*(4), 633-655. doi:10.3390/iot2040032

Bietz, M., Bloss, C., Calvert, S., Godino, J., Gregory, J., Claffey, M., & et al. (2016). Opportunities and challenges in the use of personal health data for health research. *Journal of the American Medical Informatics Association*, e42-e48.

BOE. (2016). *Reglamento (UE) 679/2016, General de Protección de Datos*. Obtenido de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Brand, D., DiGennaro Reed, F., Morley, M., Erath, T., & Novak, M. (2019). A Survey Assessing Privacy Concerns of Smart-Home Services Provided to Individuals with Disabilities. *Behav Analysis Practice, 13*(1), 11-21. doi:10.1007/s40617-018-00329-y

Burns, S. P., Terblanche, M., Perea, J., Lillard, H., DeLaPena, C., Grinage, N., MacKinen, A., & Cox, E. E. (2020). mHealth Intervention Applications for Adults Living With the Effects of Stroke: A Scoping Review. Archives of rehabilitation research and clinical translation, 3(1), 100095. https://doi.org/10.1016/j.arrct.2020.100095

Burr, C., Taddeo, M., & Floridi, L. (2020). The ethics of digital well-being: A thematic review. *Science and engineering ethics, 26*(4), 2313-2343.

Calvillo-Arbizu, J., Román-Martínez, I., & Reina-Tosina . (2021). Internet of things in health: Requirements, issues, and gaps. *Comput Methods Programs Biomed*, Sep;208:106231.

Chikukwa, G. (2021). A Consent Framework for the Internet of Things in the GDPR Era. *Masters Theses & Doctoral Dissertations. 362*. EEUU: Dakota State University. Obtenido de https://scholar.dsu.edu/theses/362/

Cicirelli, Grazia & Marani, Roberto & Petitti, Antonio & Milella, Annalisa & D'Orazio, T.. (2021). Ambient Assisted Living: A Review of Technologies, Methodologies and Future Perspectives for Healthy Aging of Population. Sensors. 21. 3549. doi: 10.3390/s21103549.

Clarke, A., & Steele, R. (2015). Smartphone-based public health information systems: Anonymity, privacy and intervention. *Journal of the Association for Information Science & Technology, 66*(12), 2596–2608. doi:10.1002/asi.23356

Cortez, N. (2018). The Evolving Law and Ethics of Digital Health. En H. Rivas, & K. Wac, *Digital Health. Health Informatics.* Springer. doi:https://doi.org/10.1007/978-3-319-61446-5_18

Ebersold, K., & Glass, R. (2016). The internet of things: A cause for ethical concern. *Issues in Information Systems, 17*(4), 145-151.

European Patent Office. (16 de 03 de 2021). *Healthcare innovation main driver of European patent applications in 2020.* Obtenido de https://www.epo.org/news-events/news/2021/20210316.html

European Commission. (2019) European Commission Ethics guidelines for trustworthy AI. Futurium - European Commission. Obtenido de: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1

Farahani, B., Firouzi, F., & Chakrabarty, K. (2020). *Farahani, B., Firouzi, F., Chakrabarty, K. (2020). Healthcare IoT. In: Firouzi, F., Intelligent Internet of Things.* Cham: Springer. doi:10.1007/978-3-030-30367-9_11

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoTin medicine and healthcare. *Future GenerationComputer Systems, 78*, 659–676.

Fei Wu, P., Vitak, J., & Zimmer, M. (2020). A contextual approach to information privacy research. *Journal of the Association for Information Science & Technology, Association for Information Science & Technology, 71*(4), 485-490.

Group, T. C. (10 de 02 de 2020). *TCG Guidance for Secure Update of Software and Firmware on.* Obtenido de https://trustedcomputinggroup.org/wp-content/uploads/TCG-Secure-Update-of-SW-and-FW-on-Devices-v1r72_pub.pdf

Haney, J., Furman, S., & Acar, Y. (2020). Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges. *International Conference on Human-Computer Interaction, 1.* Copenhaguen. Obtenido de https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=929479

Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., & Wehrle, K. (2016). A comprehensive approach to privacy in the cloud-based internet of things. *Future Generation Computer Systems, 56*, 701-718.

Hutchings, E., Loomes, M., Butow, P., & Boyle, F. (2021). A systematic literature review of attitudes towards secondary use and sharing of health administrative and clinical trial data: a focus on consent. *Systematic Reviews, 10*(1), 1-44.

Emami-Naeini, P., Agarwal, Y. & Cranor, L.F. (2021). *Specification for CMU IoT Security and Privacy Label.* Obtenido de https://www.iotsecurityprivacy.org/downloads/Privacy_and_Security_Specifications.pdf

ISO. (2015). *ISO/IEC 11889-1:2015*. Obtenido de https://www.iso.org/standard/66510.html

Jalali, M., Kaiser, J., Siegel, M., & Madnick, S. (2019). The internet of things promises new benefits and risks: a systematic analysis of adoption dynamics of IoT products. *IEEE Secur Privacy, 17*(2), 39-48. doi:10.1109/msec.2018.2888780.

Jo, T., Ma, J., & Cha, S. (2021). Elderly Perception on the Internet of Things-Based Integrated Smart-Home System. *Sensors, 21*(4), 1284. doi:10.3390/s21041284

Johnson, A. K. (2019). Guide for Security-Focused Configuration Management of Information Systems. *NIST SP*. Obtenido de https://doi.org/10.6028/NIST.SP.800-128

Jovanovic M, Mitrov G, Zdravevski E, Lameski P, Colantonio S, Kampel M, Tellioglu H, Florez-Revuelta F. (2022) Ambient Assisted Living: Scoping Review of Artificial Intelligence Models, Domains, Technology, and Concerns. J Med Internet Res;24(11):e36553, DOI: 10.2196/36553

Khan, F., & Rogers, D. (2019). *IoT cybersecurity.* Obtenido de https://www.caba.org/wp-content/uploads/2020/01/WP_CybersecurityStandards.pdf

Kissel, R. A. (2014). Guidelines for Media Sanitization. *NIST SP*. Obtenido de https://doi.org/10.6028/NIST.SP.800-88r1 .

Kelly, J., Campbell, K., Gong, E., & Scuffham, P. (2020). The Internet of Things: Impact and Implications for Health Care Delivery. *Journal of medical Internet research, 22*(11), e20135. doi:10.2196/20135

Kounoudes, A., & Kapitsaki, G. (2020). A mapping of IoT user-centric privacy preserving approaches to the GDPR. *Internet of Things*. doi:10.1016/j.iot.2020.100179.

KPMG. (2022). *Connected medical device cybersecurity. The competitive advantage of regulatory compliance.*

Loncar-Turukalo T, Zdravevski E, Machado da Silva J, Chouvarda I, Trajkovik V. (2019). Literature on wearable technology for connected health: scoping review of research trends, advances, and barriers. *J Med Internet Res, 21*(9), e14017

Lyon,, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination.* London: Routledge.

Maloy, J., & Bass, P. (2020). Understanding broad consent. *Ochsner Journal, 20*(1), 81-86.

McNeely, C., & Hahm, J. (2014). The big (data) bang: Policy, prospects, and challenges. *Review of Policy Research, 31*(4), 304–310. doi:10.1111/ropr.12082.

Ndiaye, M., Oyewobi, S., Abu-Mahfouz, A., Hancke, G., Kurien, A., & Djouani, K. (2020). IoT in the Wake of COVID-19: A Survey on Contributions, Challenges and Evolution. *IEEE Access*, 186821-186839. doi:10.1109/ACCESS.2020.3030090.

NIST. (02 de 2021). *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*. Obtenido de https://csrc.nist.gov/publications/detail/nistir/8276/final

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Artículo 25. "Protección de datos desde el diseño y por defecto" - Reglamento (UE) 2016/679, General de Protección de Datos*. Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3126-1-1

Pasluosta, C., Gassner, H., Winkler, J., Klucken, J., & Eskofier, B. (2015). An emerging era in the management of Parkinson's disease: Wearable technologies and the internet of things. *IEEE Journal of Biomedical and Health Informatics, 19*(6), 1873–1.

Priyadarshini, S., & Swain, S. (2021). Role of IoT and Social Networking in Mental Healthcare of Transgender Community During COVID-19 Pandemic. *Applications of Artificial Intelligence in COVID-19*, 405-419.

Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B. (2020). A survey on access control in the age of internet of things. *IEEE Internet of Things Journal*, 4682-4696.

Rashid, M., Parah, S., Wani, A., & Gupta, S. (2020). Securing E-Health IoT data on cloud systems using novel extended role based access control model. En *Internet of Things (IoT)* (págs. 473-489). Springer.

Rath, D., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level - a literature review. *XIMB Journal of Management, 18*(2), 171-186. doi:10.1108/XJM-08-2020-0096

Ravi, S., Climent-Pérez, P. & Florez-Revuelta, F. (2023). A review on visual privacy preservation techniques for active and assisted living. *Multimed Tools Appl*. https://doi.org/10.1007/s11042-023-15775-2

Rayan, R., Tsagkaris, C., & Iryna, R. (2021). The Internet of Things for Healthcare: Applications, Selected Cases and Challenges. En G. Marques, A. Bhoi, & V. Albuquerque, *IoT in Healthcare and Ambient Assisted Living* (Vol. 933). Singapore, Singapore: Springer. doi:10.1007/978-981-15-9897-5_1

Ruotsalainen, P., & Blobel, B. (2020). Health Information Systems in the Digital Health Ecosystem—Problems and Solutions for Ethics, Trust and Privacy. *International Journal of Environmental Research and Public Health, 17*(9).

Schmietow, B., & Marckmann, G. (2019). Mobile health ethics and the expanding role of autonomy. *Med Health Care Philos*, 623–30. doi:10.1007/s11019-019-09900-y

Schomakers, E., Biermann, H., & Ziefle, M. (2021). Users' Preferences for Smart Home Automation - Investigating Aspects of Privacy and Trust. *Telematics Informatics, 64*, 101689.

Semantha, F., Azam, S., Yeo, K., & Shanmugam, B. (2020). A Systematic Literature Review on Privacy by Design in the Healthcare Sector. *Electronics, 9*(3), 452. doi:10.3390/electronics9030452

Stavropoulos, T., Papastergiou, A., Mpaltadoros, L., Nikolopoulos, S., & Kompatsiaris, I. (2020). IoT Wearable Sensors and Devices in Elderly Care: A Literature Review. *Sensors, 20*(10), 2826. doi:10.3390/s20102826

Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *J. Tech. & Intell. Prop*(239). Obtenido de https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1

Tobore, I., Li, J., Yuhang, L., Al-Handarish, Y., Kandwal , A., Nie, Z., & Wang, L. (2019). Deep learning intervention for health care challenges: some biomedical domain considerations. *JMIR Mhealth Uhealth*, e11966.

Torous, J., Jän Myrick, K., Rauseo-Ricupero, N., & Firth, J. (2020). Digital mental health and covid-19: using technology today to accelerate the curve on access and quality tomorrow. *JMIR Ment Health, 26*(7), e18848. doi:10.2196

Wang, J. L. (2021). The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering*. Obtenido de https://doi.org/10.1016/j.cie.2021.107174

Xin, W., Liu, R., Liu, Y., Chen, Y., Yu, W. y Miao, Q. (2023). Transformer for Skeleton-based action recognition: A review of recent advances. *Neurocomputing, 537*, 164-186. https://doi.org/10.1016/j.neucom.2023.03.001.

Yeh, M. (2020). Participated without consent: Mandatory authorization of government database for secondary use. *Developing World Bioethics, 20*(4), 200-208

IBERUS

www.iberushealth.org

Proyecto (CER-20211003) reconocido como **Red de Excelencia CERVERA**

IBV INSTITUTO DE BIOMECÁNICA DE VALENCIA

CTIC CENTRO TECNOLÓGICO

ITCL CENTRO TECNOLÓGICO

Tekniker MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI INNOVACIÓN