



JORNADA DE LOS COMITÉS DE ÉTICA DE LA INVESTIGACIÓN DEL SSPA - 2022



Ética e inteligencia artificial

Evaluaciones de Impacto en proyectos de investigación con IA

Juan Díaz García

Delegado de Protección de Datos del SSPA

JORNADAS DE COMITÉS DE ÉTICA DE LA INVESTIGACIÓN DE ANDALUCÍA

24 y 25
noviembre
2022

#ÉticaInvestigaciónAndalucía

Estrategia de Bioética
del Sistema Sanitario Público de Andalucía

Junta de Andalucía
Consejería de Salud y Consumo
Escuela Andaluza de Salud Pública





INDICE:

Marco de protección de datos en investigación

Las aplicaciones en inteligencia artificial en sanidad

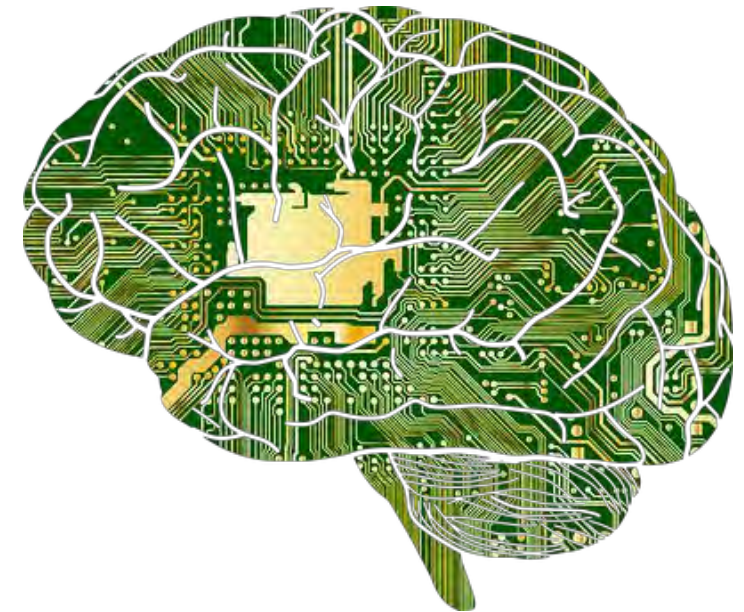
Riesgos derivados para los pacientes

Riesgos para los proyectos



**Estrategia
de Bioética**

del Sistema Sanitario
Público de Andalucía





Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción

La perspectiva ética de la IA, como una parte de la “ética digital”, es uno de los aspectos que más inquietud despierta.

La ética de la IA persigue proteger valores como la dignidad, la libertad, la democracia, la igualdad, la autonomía del individuo y la justicia frente al gobierno de un razonamiento mecánico.

La Comisión Europea trabaja en la definición de una **Inteligencia Artificial confiable**, y establece que para ello, ha de cumplir con siete requisitos clave: **acción y supervisión humanas, solidez técnica y seguridad, gestión de la privacidad y los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y ambiental y rendición de cuentas.**



BASES JURIDICAS

El **artículo 6** del RGPD establece las seis bases jurídicas por las cuales el tratamiento de datos personales se puede considerar lícito.

Las bases jurídicas más habituales que legitimarán el tratamiento en una solución de IA son:

- El tratamiento es necesario para la **ejecución de un contrato** en el que el interesado es parte, o para la aplicación de medidas precontractuales a petición de este. Podría ser el caso de desarrolladores que contraten a sujetos para hacer uso de sus datos personales en la etapa de entrenamiento del sistema. También podría ser que el responsable del tratamiento, y que proporciona un servicio a terceros interesados que incluye la solución de IA, utilizara los datos de estos en el marco del contrato del servicio.
- El **interés legítimo**, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
- El **consentimiento de los interesados**, que, como establece el artículo 4.11 del RGPD, es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Y en ciertos casos más especiales desde el punto de vista de soluciones IA, también pueden ser bases jurídicas: • Protección de intereses vitales. • Razones de interés público o ejercicio de poderes públicos. • Cumplimiento de obligaciones legales.



Decisiones automatizadas

Las decisiones basadas únicamente en el tratamiento automatizado representan la capacidad de tomar decisiones por medios tecnológicos sin la participación del ser humano.

El RGPD, en su Considerandos 71 y así como en su artículo 22, limita y establece derechos con relación a que los sujetos de los datos no sean sometidos a decisiones exclusivamente automatizadas que tengan efectos jurídicos o que afecten significativamente al interesado.

La elaboración de perfiles de forma automática se incluye en este marco de decisiones automatizadas. El Grupo del Artículo 29 ha analizado las implicaciones de este derecho en las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 del WP29.



TOMA DE DECISIONES BASADAS ÚNICAMENTE EN UN TRATAMIENTO AUTOMATIZADO

Las aplicaciones que ofrecen o soportan un servicio basado en soluciones IA pueden tomar decisiones que afectan a los individuos, sus vidas privadas, su seguridad física, su posición social y su interacción con otras personas.

El RGPD garantiza el derecho a no ser sometido a decisiones automatizadas incluidas la elaboración de perfiles cuando:

- No hay intervención humana. Para que pueda considerarse que existe participación humana, la supervisión de la decisión ha de ser realizada por una persona competente y autorizada para modificar la decisión, y para ello ha de realizar una acción significativa y no simbólica.
- Produzcan efectos jurídicos.
- O afecte de forma similar y significativa al interesado.

Se permiten las siguientes **excepciones** cuando el tratamiento:

- Esté basado en el **consentimiento explícito** y se apliquen garantías para proteger derechos y libertades.
- Sea necesario para la **celebración o ejecución de un contrato**, no afecte a categorías especiales de datos y, además, se apliquen garantías para proteger derechos y libertades.
- Esté basado en el derecho de la UE o de España y **no afecte a categorías especiales de datos**.
- Esté basado en el derecho de la UE o de España **y sea necesario para proteger un interés público esencial**



EVALUACIÓN DE LAS SOLUCIONES IA

Tanto el modelo de IA incluido en un tratamiento, como el tratamiento en sí, ha de tener el propósito de dar respuesta a una necesidad real de la empresa y la industria. Estamos hablando de soluciones que trascienden el ámbito experimental y se van a someter a las leyes del mercado, un mercado regulado y que está obligado a cumplir con unas normas y estándares de calidad.

Con relación a su capacidad de dar cumplimiento a los requisitos del tratamiento, hay ciertos parámetros comunes a cualquier solución técnica que deberán quedar especificadas, como, por ejemplo:

- Precisión, exactitud o medidas de error requeridos por el tratamiento.
- Requisitos de calidad en los datos de entrada al componente IA.
- Precisión, exactitud o medidas de error efectivas de la solución IA en función de la métrica adecuada para medir la bondad de esta.
- Convergencia del modelo, cuando nos encontremos con entrenamiento y soluciones adaptativas.
- Consistencia entre los resultados del proceso de inferencia.
- Predictibilidad del algoritmo.
- Y cualquier otro parámetro de evaluación del componente IA



GESTIÓN DEL RIESGO PARA LOS DERECHOS Y LIBERTADES

La **gestión del riesgo para los derechos y libertades** es una actividad continua y forma parte del concepto de Responsabilidad Proactiva o “accountability” que se establece en el RGPD.

Cuando se tratan datos personales y sea proporcional con relación a las actividades de tratamiento, la organización ha de sistematizar las medidas de cumplimiento en una **Política de Protección de Datos**, como se establece en el artículo 24 del RGPD.

Esta política convivirá con una política de calidad, una política de sistemas de información, una de seguridad y una política de toma de decisiones, entre otras. El RGPD no establece de forma específica qué elementos de responsabilidad proactiva hay que implementar de forma obligatoria o la forma de implementarlos, limitándose a proporcionar un amplio grado de flexibilidad para que muy distintos tratamientos se adecúen a la norma.

Sin embargo, sí establece que dichas medidas se han de seleccionar siguiendo un **análisis basado en el riesgo**, y específicamente en el riesgo para los derechos y libertades de las personas con relación al tratamiento de sus datos personales y la elaboración de perfiles.



JORNADA DE LOS COMITÉS DE ÉTICA DE LA INVESTIGACIÓN DEL SSPA - 2022

El **análisis de riesgos** tiene dos fases fundamentales: la primera es la **identificación** de amenazas y evaluación del nivel de riesgo intrínseco existente; y la segunda es la **gestión de este riesgo** mediante la implementación de medidas técnicas y organizativas, adecuadas y proporcionales, para eliminarlo o al menos mitigarlo, reduciendo el impacto o la probabilidad de que se materialicen las amenazas identificadas. Por último, una vez implementadas las medidas seleccionadas, se debe evaluar el riesgo residual remanente y mantenerlo controlado.

Tanto para determinar el riesgo, como para establecer las medidas apropiadas para gestionarlo, es preciso realizar un análisis del tratamiento, dividiendo el mismo en sus distintas fases y administrar las peculiaridades de cada una de ellas.

Para determinar el **nivel de riesgo** de un tratamiento basado o que contiene fases en las que existe un componente IA hay que tener en cuenta:

- Los **riesgos que se derivan del tratamiento en sí mismo**, siendo el más característico el que se deriva del sesgo en los sistemas de toma de decisiones sobre las personas o su discriminación (algorithmic discrimination).
- **Los riesgos que se derivan del tratamiento con relación al contexto social y los efectos colaterales** que se puedan derivar de él, indirectamente relacionados con el objeto de tratamiento.



EVALUACIÓN DEL NIVEL DE RIESGO

Evaluar el nivel de riesgo de un tratamiento es una operación necesaria para determinar el modo en que se van a aplicar las medidas tendentes a suprimirlo o minimizarlo, en particular cuando el riesgo detectado es alto según las condiciones establecidas en la norma, fundamentalmente en:

- El artículo 35.3 del RGPD.
- El artículo 28.2 de la LOPDGDD.
- Las Listas de tipos de tratamientos de datos que requieren EIPD (art 35.4) publicadas por la AEPD.

En cualquier caso, el responsable ha de ser capaz de identificar los riesgos adicionales derivados de la novedad de la solución IA y su modo de implementación como, por ejemplo, en el caso de que el componente IA que se distribuya incluya datos personales.

Hay que recalcar que este análisis trasciende los límites de la entidad responsable, y está orientado a medir el impacto que la actividad realizada pueda tener en el entorno social en el que se realiza o despliega la aplicación.

El responsable del desarrollo, mantenimiento y/o distribución de un componente IA, así como el responsable de un tratamiento que incluya componentes IA, ha de tomar, en cada una de las respectivas etapas y responsabilidades, las medidas oportunas para minimizar o eliminar los factores de riesgo.



LA EVALUACIÓN DE IMPACTO DE LA PRIVACIDAD - EIPD

La EIPD es una obligación establecida en el RGPD cuando los niveles de riesgo asociados al tratamiento son elevados. Esta obligación implica ir más allá de realizar la mera gestión del riesgo del tratamiento, puesto que exige una formalidad adicional a la hora de ejecutar dicha gestión.

La necesidad de que cada responsable lleve a cabo una evaluación de impacto de la protección de datos se establece en el artículo 35 del RGPD cuando, según el apartado 1, “el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas”.

En particular, pero no de forma exclusiva, y tal como establece el artículo 35.3.a , es necesario realizar una EIPD cuando se realice la elaboración de perfiles, basados en tratamientos automatizados (pero no necesariamente exclusivamente automatizados), sobre los que se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente.



Evaluación de impacto

- Deberá realizarse cuando sea probable que el tratamiento previstos presente **un alto riesgo específicos para los derechos y libertades** de los interesados, entre otros casos, cuando:
 - elaboración de **perfiles** sobre cuya base se tomen **decisiones** que produzcan **efectos jurídicos** para las personas físicas o que les afecten significativamente de modo similar;
 - tratamiento a **gran escala** de las **categorías especiales de datos**
 - **observación sistemática a gran escala** de una zona de acceso público
- Las APD **deberán** establecer listas adicionales de tratamientos de alto riesgo y **podrán** establecer listas que no requieren EIPD
- El RGPD prevé un **contenido mínimo** de la evaluación
- **Como novedad, se prevé que habrá de recabarse “cuando proceda” la opinión de los interesados**



EVALUACIÓN DE LA PROPORCIONALIDAD Y NECESIDAD DE DICHO TRATAMIENTO

El artículo 35.7.b del RGPD establece que, a la hora de realizar una EIPD, se ha de llevar a cabo una **evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad**. El empleo de soluciones basadas en IA sitúa a responsables y encargados en un escenario en el que el tratamiento, por sus características y, en particular, por la tecnología elegida, puede conllevar un alto nivel de riesgo.

Por lo tanto, debería valorarse si el objeto del tratamiento no puede ser conseguido utilizando otro tipo de solución que alcance la misma funcionalidad, con un margen de rendimiento aceptable y un nivel de riesgo menor.

Es decir, la disponibilidad o novedad de una tecnología no justifica, por sí misma, su utilización, sino que debe ser objeto de ponderación, realizando un análisis de si el tratamiento, en la forma en que se plantea, es equilibrado porque se derivan más beneficios y ventajas concretas para el interés general y la sociedad en su conjunto que perjuicios, entendidos estos como los riesgos sobre los derechos y libertades de los sujetos cuyos datos son objeto de tratamiento.



Información significativa sobre la lógica aplicada

En el caso de que el interesado esté sometido a decisiones automatizadas o en la elaboración de perfiles a los que hace referencia el artículo 22 del RGPD, un aspecto importante que se establece en el artículo 13.2.f del RGPD es que éste ha de “disponer de información significativa sobre la lógica aplicada” y “la importancia y las consecuencias previstas”.

La palabra “significativa”, que según la RAE denota “Que da a entender o conocer con precisión algo” se ha de interpretar como información que, proporcionada al interesado, le hace consciente del tipo de tratamiento que se está llevando a cabo con sus datos y le proporciona certeza y confianza sobre sus resultados .



Cumplir con esta obligación ofreciendo una referencia técnica a la implementación del algoritmo puede ser opaco, confuso, e incluso conducir a la fatiga informativa. **Debe facilitarse información que permita entender el comportamiento del tratamiento.**

Aunque dependerá del tipo de componente IA utilizado, un ejemplo de información que podría tener relevancia de cara al interesado, sería:

- El detalle de los **datos empleados** para la toma de decisión, más allá de la categoría, y en particular información sobre los plazos de uso de los datos (su antigüedad).
- La **importancia relativa** que cada uno de ellos tiene en la toma de decisión.
- La calidad de los datos de entrenamiento y el tipo de patrones utilizados.
- **Los perfilados realizados y sus implicaciones.**
- **Valores de precisión o error** según la métrica adecuada para medir la bondad de la inferencia.
- **La existencia o no de supervisión humana cualificada.**
- La referencia a **auditorías**, especialmente sobre las posibles desviaciones de los resultados de las inferencias, así como la certificación o certificaciones realizadas sobre el sistema de IA. En el caso de sistemas adaptativos o evolutivos, la última auditoría realizada.
- En el caso de que el sistema IA contenga información de terceros identificables, la prohibición de tratar esa información sin legitimación y de las consecuencias de realizarlo.



TRANSPARENCIA

Según el Considerando 78 , el **principio de transparencia** es una **medida de privacidad por defecto** para permitir, entre otros, que los interesados puedan supervisar el tratamiento al que están sometidos.

El principio de transparencia se desarrolla en los Considerandos 39 y 58. En estos Considerandos se interpreta la obligación de información a los interesados de un modo que va más allá de lo dispuesto en la letra de los artículos 13 y 14 del RGPD. En particular, los Considerandos comentan la obligación de que “toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente **accesible y fácil de entender**”, “sea **concisa**”, “se utilice un lenguaje sencillo y claro”, que “en su caso, se visualice”, que “podría facilitarse en forma electrónica”, que se proporcione “información añadida para garantizar un tratamiento leal y transparente” y que los interesados “deben tener conocimiento de los riesgos, las normas, las salvaguardias” del tratamiento.

La transparencia no se reduce a un instante puntual, sino que debe ser entendida como un principio en torno al que orbita de forma dinámica el tratamiento realizado y que afecta a todos y cada uno de los elementos y participantes que intervienen en la solución.



EXACTITUD

El término “exactitud” se define en el artículo 5.1.d del RGPD como uno de los principios de protección de datos de carácter personal. En el caso de tratamientos que incorporan soluciones IA, la existencia de sesgos en los modelos de inferencia está íntimamente ligado con la exactitud o calidad del dato.

Según el segundo párrafo del Considerando 71 del RGPD, los datos asociados a los interesados, ya sean los **datos directamente recogidos o los inferidos, han de ser exactos**. En particular, se hace explícito que el responsable del tratamiento ha de utilizar “procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles” que garanticen que los datos vinculados con el interesado son exactos.

Es obligatorio demostrar y documentar que los procedimientos empleados para la inferencia de información sobre un interesado son precisos y, por tanto, estables y predecibles. Cuando un responsable selecciona el empleo de un componente de IA para un tratamiento ha de tener la **diligencia** de asegurarse que los datos tratados, generados y vinculados con el interesado cumplen con las condiciones anteriores.



Certificación

Uno de los problemas que se plantean a la hora de proporcionar transparencia con relación a los algoritmos de IA es la cuestión de la confidencialidad necesaria para preservar la propiedad industrial. Este problema no es exclusivo de la IA, sino que es común a cualquier desarrollo tecnológico, como, por ejemplo, los módulos criptográficos en sistemas seguros, o los circuitos integrados de las tarjetas de crédito.

Sin embargo, en los sectores en los que se emplean estas soluciones es imperativo no confiar únicamente en las manifestaciones de fabricantes y distribuidores, sino que obligatoriamente se establecen mecanismos basados en terceros confiables para determinar los niveles necesarios de calidad y confiabilidad. Estos mecanismos se materializan bien dando acceso a las autoridades de control a los aspectos internos de dichas soluciones, o bien estableciendo mecanismos de certificación por terceros independientes.

El RGPD establece en el artículo 42 la posibilidad de desarrollar mecanismos de certificación específicos en materia de protección de datos y de sellos y marcas de protección de datos como herramientas para demostrar el cumplimiento del RGPD. Estos esquemas pueden cubrir distintos aspectos del empleo de la IA y ser herramientas para demostrar diligencia. Tal y como explica el Considerando 100, los mecanismos de certificación sirven también para aumentar la transparencia en los tratamientos de datos de carácter personal.



Verificación vs. Validación

La realización de pruebas y/o **verificación del componente de IA** es una parte capital en el desarrollo de este, así como como un criterio importante para seleccionar uno u otro componente por el responsable del tratamiento.

El responsable ha de tener en cuenta que la inclusión en un tratamiento de un componente IA verificado no implica que **el conjunto del tratamiento esté validado**, ni tampoco la adecuación del componente IA para ese tratamiento específico.

Las pruebas del componente IA aseguran que los resultados del diseño y desarrollo cumplen con los requisitos del componente. La validación del tratamiento llega más lejos, ya que se asegura de que los productos y servicios resultantes satisfacen los requisitos relativos a una aplicación específica o uso previsto. La validación garantiza que el tratamiento, así como la solución IA sobre la que se apoya, **cumple con los resultados planificados para un producto o servicio concreto**. Es decir, la validación del tratamiento que incluye un componente IA ha de realizarse en las condiciones que reflejen el entorno real en el que se pretende desplegar el tratamiento. A su vez, el proceso de **validación exige una revisión periódica**, en la medida que evolucionen dichas condiciones o el tratamiento en sí.



Amenazas específicas en componentes IA

El análisis de las medidas de seguridad comunes a cualquier sistema es igualmente necesario para proteger una solución de IA. Por ejemplo, deben considerarse aquellas que se derivan de que los componentes sean desarrollados por terceros o de las comunicaciones de datos a terceras partes que puedan producirse. Además, hay que tener en cuenta la necesidad de implementar medidas concretas dirigidas a prevenir ataques que son específicos a este tipo de aplicaciones. Existen tipologías estudiadas de ataque y defensa a componentes de IA.

Entre las medidas de seguridad, se recomienda prestar especial atención a aquellas que gestionen estos tipos de amenazas:

- **Acceso y manipulación del conjunto de datos de entrenamiento**, previo a la configuración del modelo, por ejemplo, mediante técnicas de envenenamiento con patrones adversos.
- **Inclusión de troyanos** y puertas traseras durante el proceso de desarrollo de la IA, bien en el propio código o en las herramientas de desarrollo.
- **Manipulación de la API** de usuario para realizar accesos al modelo, tanto a nivel de caja negra como de caja blanca, para la manipulación de parámetros del modelo, filtrado del modelo a terceros, ataques a la integridad o disponibilidad de las inferencias.



- Ataques por “adversarial machine learning” por lo que sería necesario un análisis de la robustez y control de la alimentación con datos al modelo.
- Ataques por imitación de patrones que se conoce serán admitidos por el sistema.
- Reidentificación de los datos personales incluidos en el modelo (inferencia de pertenencia o inversión del modelo) por parte de usuarios internos y externos.
- Fraude o engaño a la IA por parte de los interesados, especialmente en casos que puedan suponer un perjuicio para otros interesados, lo que implica la necesidad de realizar un análisis de la robustez ante dichas actuaciones y la realización de auditorías.
- Filtrado a terceros de resultados de perfilado o decisiones inferidas por la IA (también relacionado con las API’s de usuario).
- Filtrado o acceso a los logs resultado de las inferencias generadas en la interacción con los interesados.



SEGURIDAD

El RGPD establece en su artículo 32 que tanto el responsable, como el encargado, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de los interesados.

Estas medidas se adecuarán a los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como a los riesgos de probabilidad y gravedad variables.

Es decir, no hay una solución estándar para todos los tratamientos, y mucho menos para aquellos que incluyan un componente de IA.

La solución tiene que establecerse mediante un análisis de riesgos que, desde el punto de vista de protección de datos, ha de ser relativo a los riesgos para los derechos y libertades de los interesados.



TRANSFERENCIAS INTERNACIONALES

El desarrollo o despliegue de un componente de IA basado en servicios en **la Nube**, la comunicación de los datos de los usuarios a terceros para evolucionar el modelo de IA, o la distribución de componente de IA en el caso de que existan datos personales inherentes al modelo, pueden implicar flujos transfronterizos de datos a terceros países.

No tienen consideración de transferencia internacional de datos los flujos de datos que se producen dentro del marco del **Espacio Común Europeo** (los Estados de la Unión Europea más Islandia, Noruega y Liechtenstein). Dichas transferencias han de aplicar las garantías que se establecen en el Capítulo V del RGPD “Transferencias de datos personales a terceros países u organizaciones internacionales”.

Especialmente importante es establecer mecanismos para permitir que las contrataciones que se realicen en este contexto de transferencias internacionales se gestionen con fluidez, asegurando al mismo tiempo que el cliente responsable tiene información suficiente sobre los contratistas, o potenciales contratistas, y mantiene la capacidad de tomar decisiones.

Cuando existen transferencias internacionales hay que informar a los interesados en los términos del art. 13 y 14 del RGPD e incluirlo en el registro de actividades de tratamiento.



Oficina de Ciencia y
Tecnología del Congreso
de los Diputados

Oficina C

Inteligencia artificial y salud

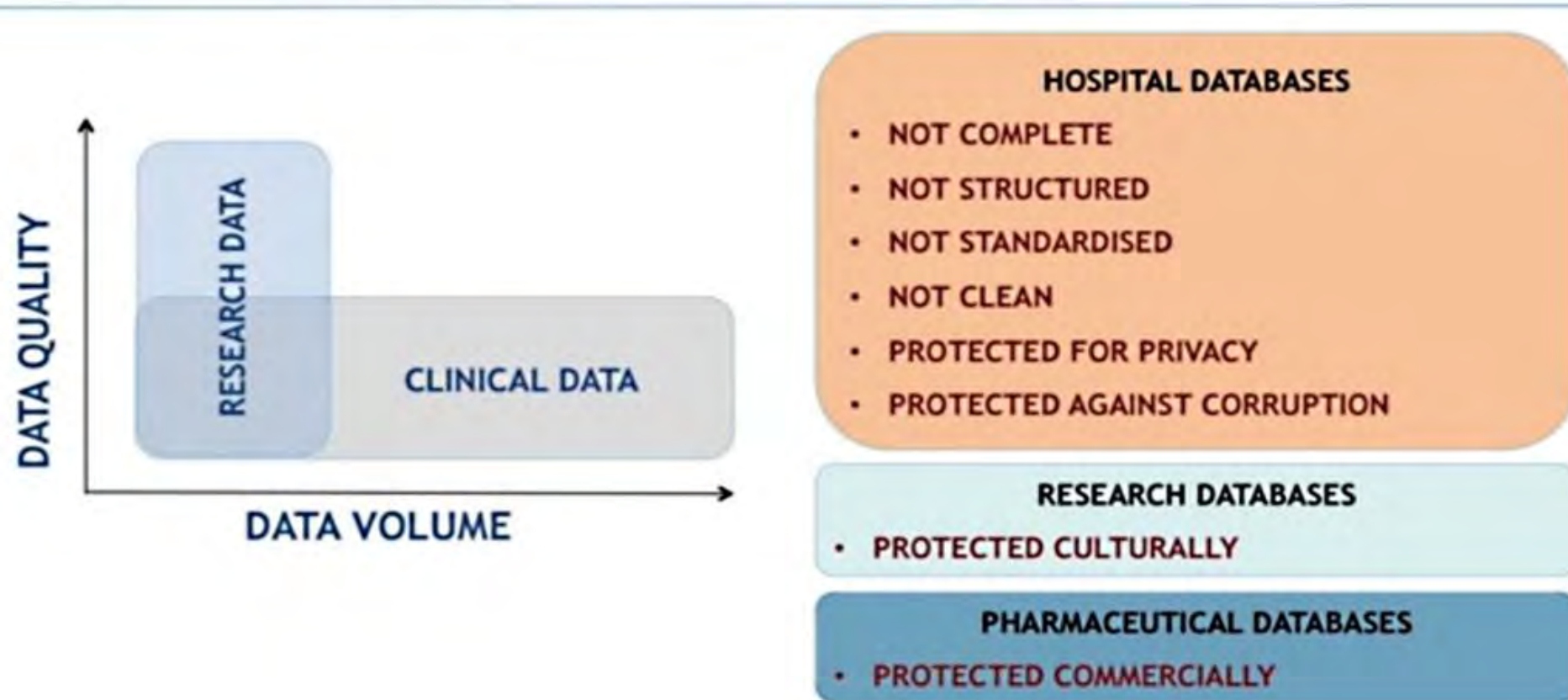
Potencial y desafíos

La salud es uno de los ámbitos **donde se espera una mayor contribución** de la inteligencia artificial (IA), con implicaciones en el coste, calidad y eficiencia de la atención médica, incluida la capacidad de preparación y respuesta ante emergencias sanitarias. No obstante, plantea retos importantes relacionados con su seguridad, la privacidad y el acceso a los datos o la generación de desigualdades. La legislación, regulación, evaluación y supervisión humana son elementos clave para facilitar su implementación en la práctica profesional.



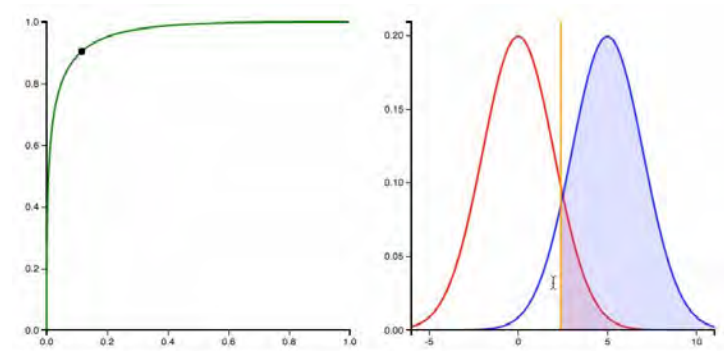
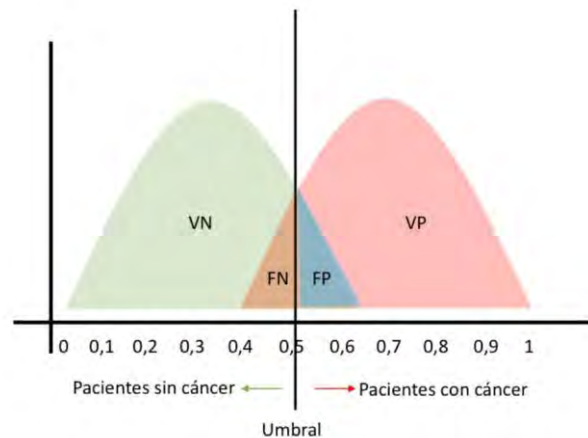
Problemas en los Tratamientos de la Información

DATA SOURCES AND CHALLENGES

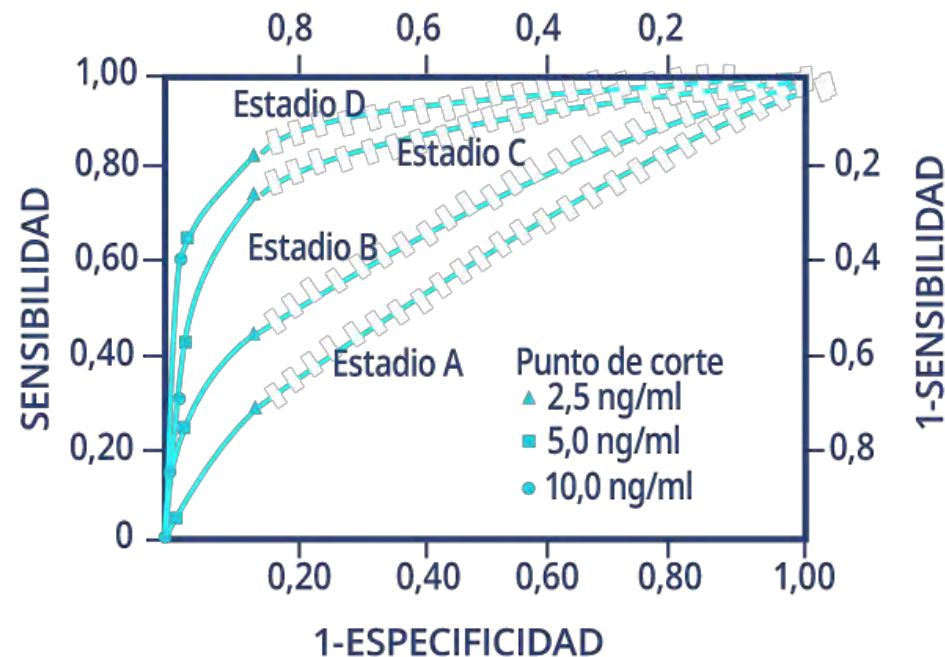
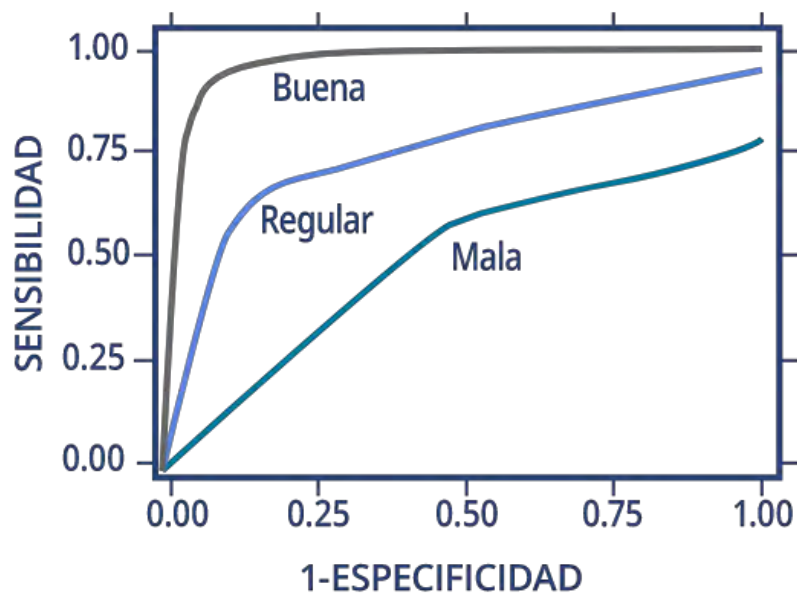




Evaluación Curvas ROC



ESPECIFICIDAD



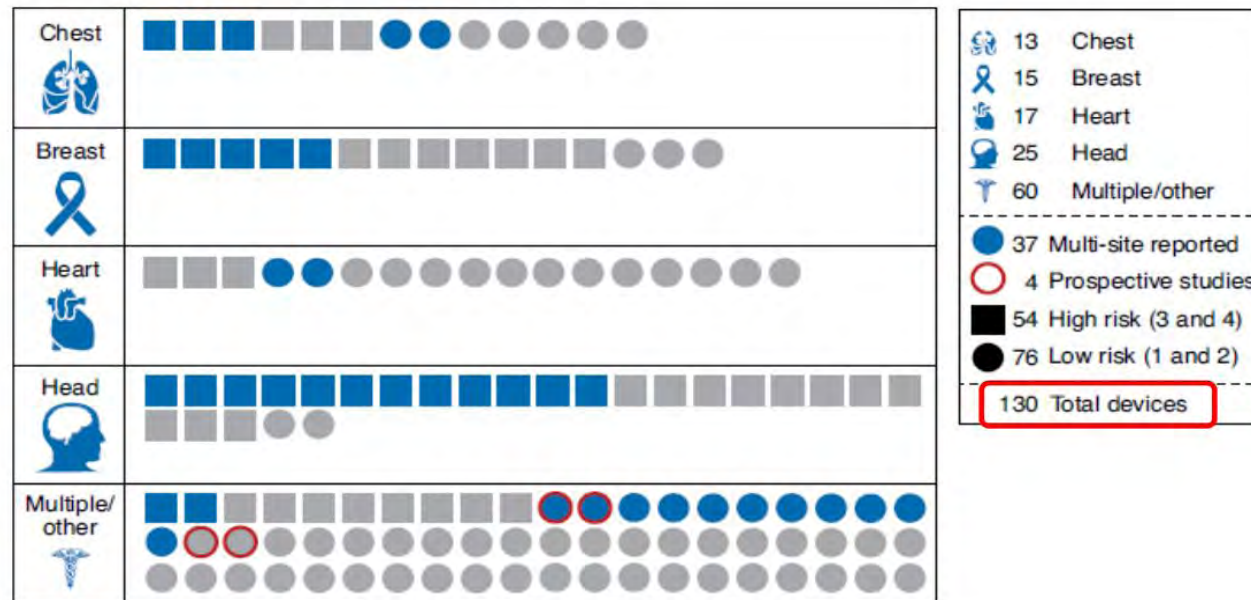
Interpretación de una curva ROC, de acuerdo con los estadios de la enfermedad [imagen]. Tomada de Fletcher, R. y Fletcher, S. (2008). "Diagnóstico", p. 47



How medical AI devices are evaluated: limitations and recommendations from an analysis of FDA approvals

Eric Wu, Kevin Wu, Roxana Daneshjou, David Ouyang, Daniel E. Ho and James Zou

NATURE MEDICINE | VOL 27 | APRIL 2021 | 576-584



- ✓ Validación retrospectiva → 97%
- ✓ No análisis utilidad clínica
- ✓ Nº centros sanitarios ND → 70%
- ✓ Aplicabilidad muy limitada → 10%
- ✓ Nº pacientes ND → 45%
- ✓ Nº pacientes \cong 300 → 55%

Radiology

Deep Convolutional Neural Network–based Software Improves Radiologist Detection of Malignant Lung Nodules on Chest Radiographs

Yongsik Sim, MD • Myung Jin Chung, MD • Elmar Kötter, MD • Sehyo Yune, MD • Myeongeun Kim, MD • Synho Do, PhD • Kyunghwa Han, PhD • Hanmyoung Kim, MS • Seungwook Yang, PhD • Dong-Jae Lee, PhD • Byoung Wook Choi, MD, PhD

Radiology 2020; 294:199–209 • <https://doi.org/10.1148/radiol.2019182465> • Content codes: **CH** **IN**

- ✓ Estudio retrospectivo y multicéntrico
- ✓ Eficacia radiólogos + software vs radiólogos vs software
- ✓ End-points → Sensibilidad y Falsos positivos
- ✓ Detección nódulos pulmonares malignos en Rx tórax (malignidad confirmada por TAC y biopsia)
- ✓ Rx normales → 200
- ✓ Rx patológicas → 600 (704 nódulos)

Table 1: Characteristics of the Radiologists Performing Interpretation of Chest Radiographs

Center and Reader	Experience Level
Center 1	
Reader 1	Radiology resident
Reader 2	Chest radiologist, 5 years
Reader 3	Chest radiologist, > 10 years
Center 2	
Reader 4	Radiology resident, 3rd year
Reader 5	Chest radiologist, 5 years
Reader 6	Chest radiologist, > 10 years
Center 3*	
Reader 7	Chest radiologist, 5 years
Reader 8	Chest radiologist, 15 years
Reader 9	Chest radiologist, 20 years
Center 4	
Reader 10	Radiology resident, 4th year
Reader 11	Chest radiologist, 5 years
Reader 12	Chest radiologist, 12 years

Table 4: Pooled Results of Radiologist Reader and DCNN Performance

Center, Total No. of Nodules, and System	Sensitivity (per Nodule) (%)	FPPI	Readers with DCNN vs Readers without DCNN	Readers with DCNN vs DCNN	Readers without DCNN vs DCNN
Overall (12 readers, 704 nodules)					
Readers without DCNN	65.1 [1375 of 2112] (62.0, 68.1)	0.2 [488 of 2400] (0.18, 0.22)	Sensitivity $P < .001$; FPPI	Sensitivity $P = .006$; FPPI	Sensitivity $P = .12$; FPPI
Readers with DCNN	70.3 [1484 of 2112] (67.2, 73.1)	0.18 [422 of 2400] (0.16, 0.2)	$P < .001$	$P = .13$	$P = .76$
DCNN alone	67.3 [474 of 704] (63.8, 70.7)	0.2 [159 of 800] (0.17, 0.23)			



europapress / andalucía / conocimiento

Publicado 03/08/2021 14:59

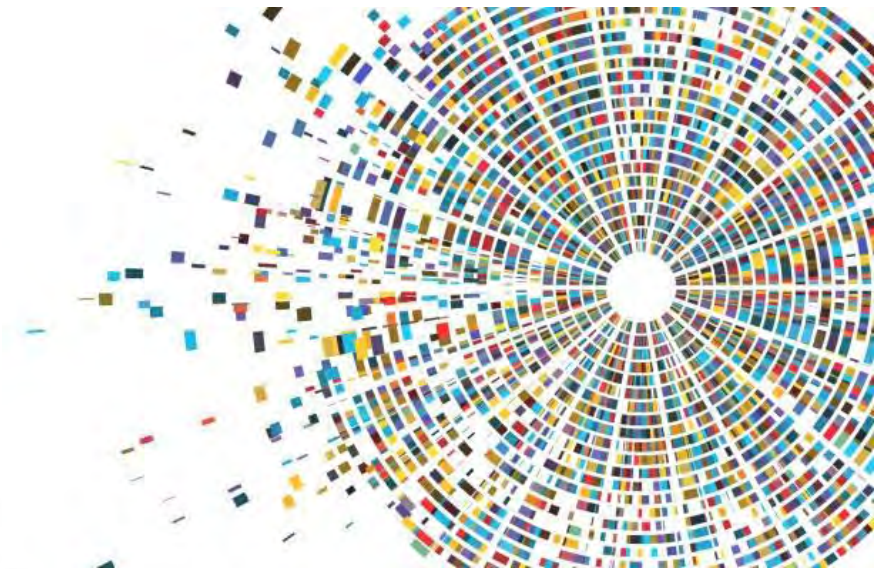
'Red.es' adjudica por 4,6 millones de euros una solución de analítica avanzada para la sanidad pública andaluza



El programa tenía un precio de licitación de 7,7 millones de euros, por lo que la adjudicación supone un ahorro de casi el 40%. - Red.es

SEVILLA, 3 Ago. (EUROPA PRESS) -

'Red.es', entidad pública empresarial adscrita al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, ha adjudicado este martes el 'Servicio para la implantación de una solución corporativa de analítica avanzada', basada en tecnologías 'big data', para el Sistema Sanitario Público de Andalucía a la UTE EY Transforma Servicios de Consultoría por un importe de 4,6 millones de euros.





EU initiative on a European Health Data Space (EHDS)

eHealth Stakeholder Group – towards EHDS acceptance

The eHSG have formed 5 working groups on which concrete solutions the stakeholders identify and actions that could be taken in the area of:



- 1. promoting access to health data and interoperability*
- 2. re-use of health data for research and policy-making*
- 3. promotion of digital health services and products*
- 4. uptake of AI for health*
- 5. sharing of data between public and private partners*

El espacio europeo será clave para tres ejes esenciales de la protección de la salud pública: la prestación de asistencia sanitaria; la investigación y la elaboración de políticas sanitarias; y el sistema de alerta temprana sobre amenazas transfronterizas de salud”.



JORNADA DE LOS COMITÉS DE ÉTICA DE LA INVESTIGACIÓN DEL SSPA - 2022

Termina el juicio a la fundadora de Theranos: Elisabeth Holmes, condenada a 11 años y 3 meses de cárcel con 3 años de libertad supervisada

Historia de Roberto Corrales • sábado

Reaccionar | 1



Elisabeth Holmes, fundadora de Theranos.
© Proporcionado por Business Insider España

Más de 4 años después de que se presentaran cargos contra ella por engañar a los inversores y a los pacientes de la empresa de análisis de sangre Theranos, Elisabeth Holmes ya ha recibido su condena.

Disrupción Tecnológica





[October 2013 press release](#), IBM declared that MD Anderson, the cancer center that is part of the University of Texas, “is using the IBM Watson cognitive computing system for its mission to eradicate cancer.”

IBM Watson Flops For Cancer Treatment: Why Did AI Fail?

MD Anderson Cancer Center recently announced it was dropping IBM Watson’s cognitive-computing system, which was supposed to use artificial intelligence (AI) to expedite physicians’ decision making when treating malignant tumors.

Un informe de los auditores de la Universidad de Texas afirma que el proyecto costó al MD Anderson más de 62 millones de dólares y, sin embargo, no cumplió sus objetivos.



“Artificial intelligence has been suffering from overhype since the 1970s and 80s,” said Steven Salzberg, a professor of biomedical engineering at the Johns Hopkins School of Medicine. “Be skeptical and ask to see some evidence. (Technology companies) need to do more than simply assert that it works.”



Retos de la Investigación

Marco de colaboración grupos de investigación

Convenios – herramientas – plataformas – app de registro

Vis+ Padris – BIG DATA SAS – Integración de fuentes - Heterogeneidad

Data lake – para la investigación - “Data - **Pantano - Ciénaga**”

Evaluaciones de Impacto en Big Data, IA y BD específicas

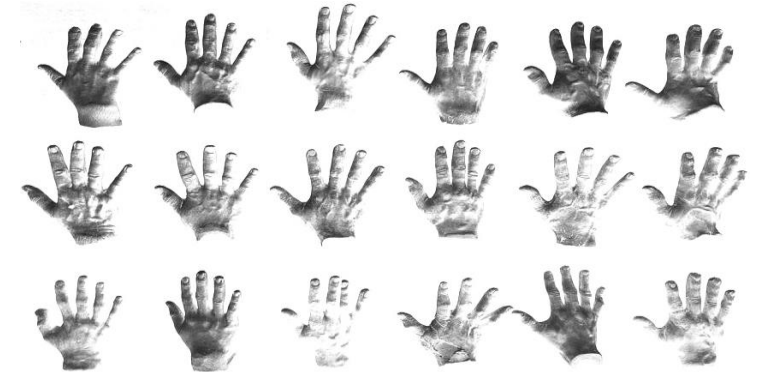
Medidas Técnicas y Organizativas para facilitar la información para Big Data e IA

Trabajo en Red – Modelos distribuidos

Nuevos algoritmos IA – reproducir los resultados con los datos reales y locales

Validación de herramientas IA – Interpretabilidad - Evaluación de Resultados

Aplicabilidad en la Medicina de Precisión





CONCLUSIONES

Uno de los principales problemas de las soluciones de IA no es la IA en sí, sino cómo van a usar las personas la tecnología IA y los nuevos sesgos psicológicos que se derivan de su empleo.

En particular, es necesario prestar especial atención a atribuir responsabilidades a componentes IA sin supervisión y sin adoptar una posición crítica.

La delegación de la toma de decisiones a máquinas no es nueva; ya ocurre con los algoritmos deterministas, pero el sesgo de atribuir una autoridad o peso superior a un resultado inferido por una solución de IA puede hacer incrementar los riesgos derivados de esta delegación de responsabilidad.



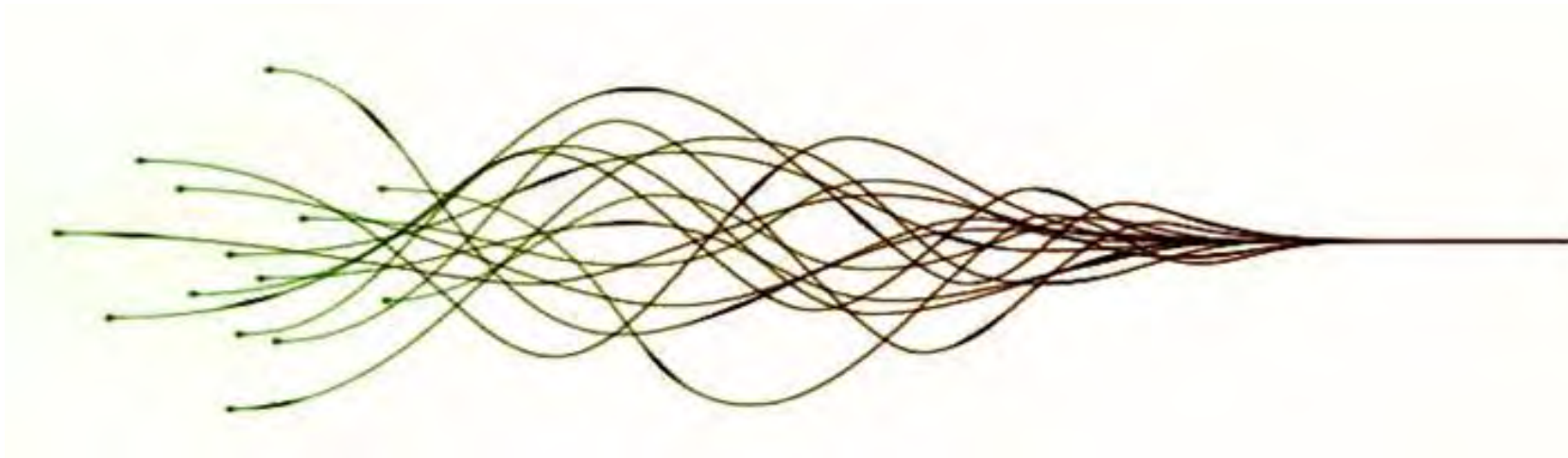
Resumen

Marco legal – nos protege a todos como ciudadanos y pacientes

Ofrecer garantías reales en la metodología de la investigación y en las fuentes de datos

Facilitar medidas técnicas y organizativas para conseguir una investigación de calidad

Compromiso en el manejo de la información clínica que facilite la investigación y en especial facilitando los proyectos de la iniciativa Europea, Española y Andaluza



dpd.sspa@juntadeandalucia.es