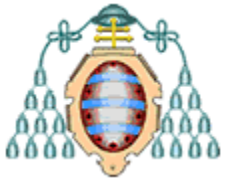
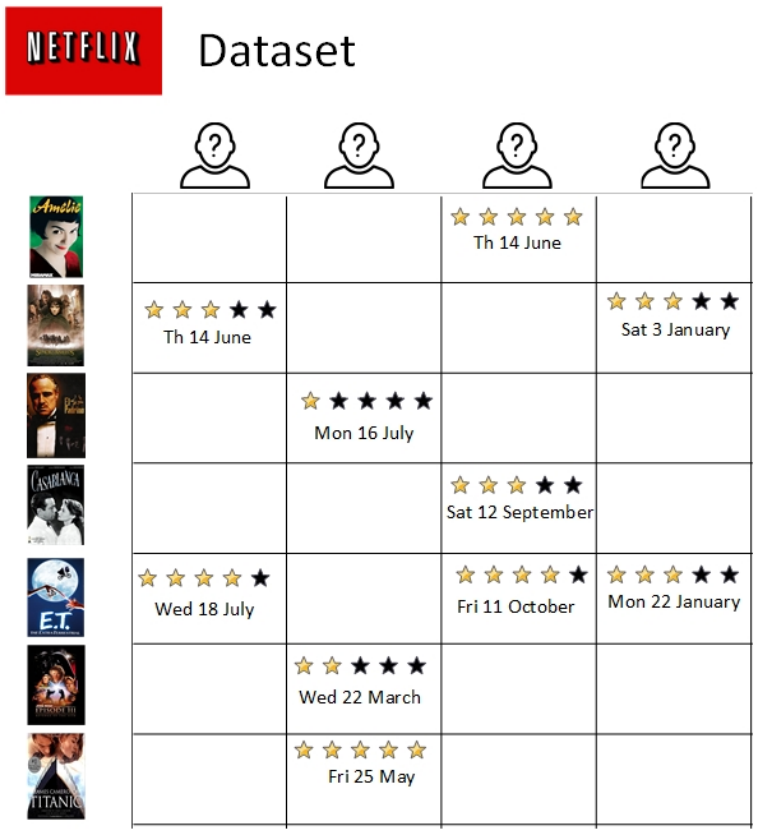
Este trabajo ha sido realizado bajo el proyecto de investigación TestEAMos (TIN2016-76956-C3-1-R), financiado por el Ministerio Español de Economía y Competitividad junto con fondos FEDER

Anonimización de datos guiada por pruebas para aplicaciones inteligentes

Cristian Augusto, Jesús Morán, Claudio de la Riva and Javier Tuya
Grupo de Investigación en Ingeniería del Software
http://giis.uniovi.es
Universidad de Oviedo

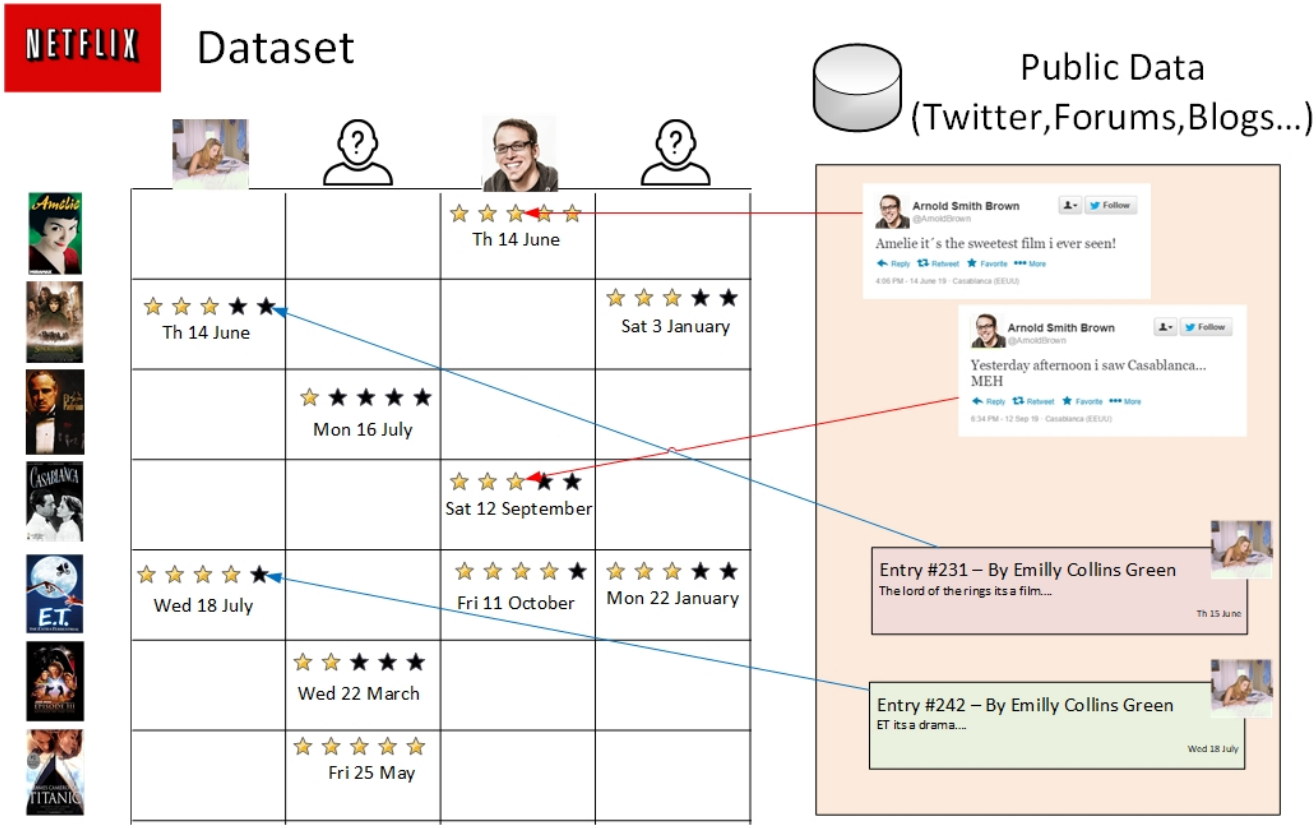


Dataset del concurso de Netflix (I)



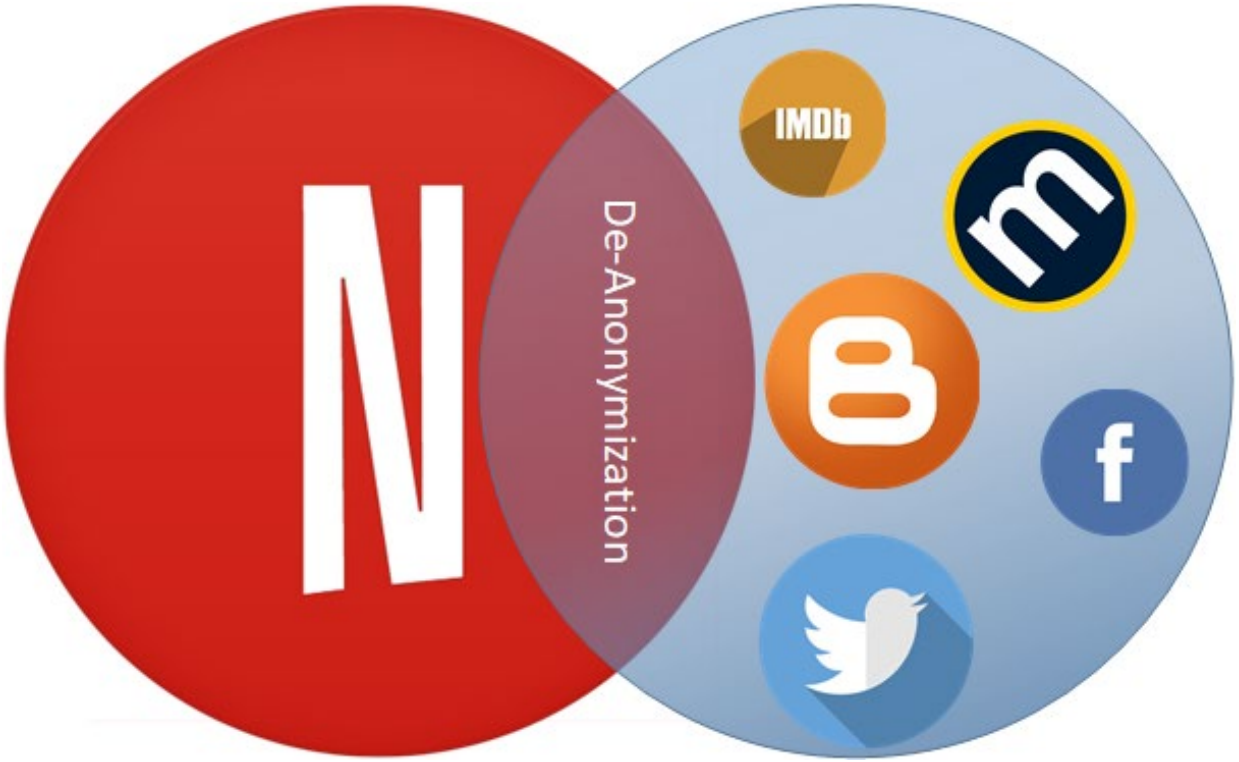
- En 2009 Netflix libero un dataset sin identificadores de los usuarios explícitos, para que desarrolladores compitiesen por mejorar su algoritmo de recomendación

Dataset del concurso de Netflix (II)



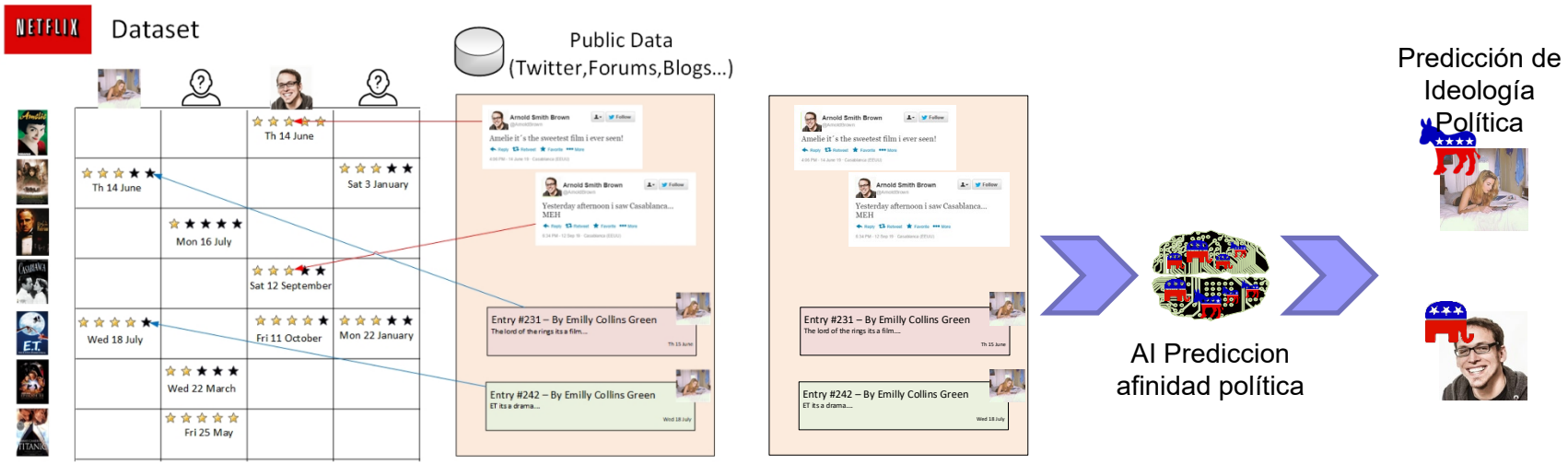
- La información compartida por Netflix cruzada con datos de otras fuentes como Tweets o Posts en Blogs permitía reidentificar a los usuarios

Dataset del concurso de Netflix (III)



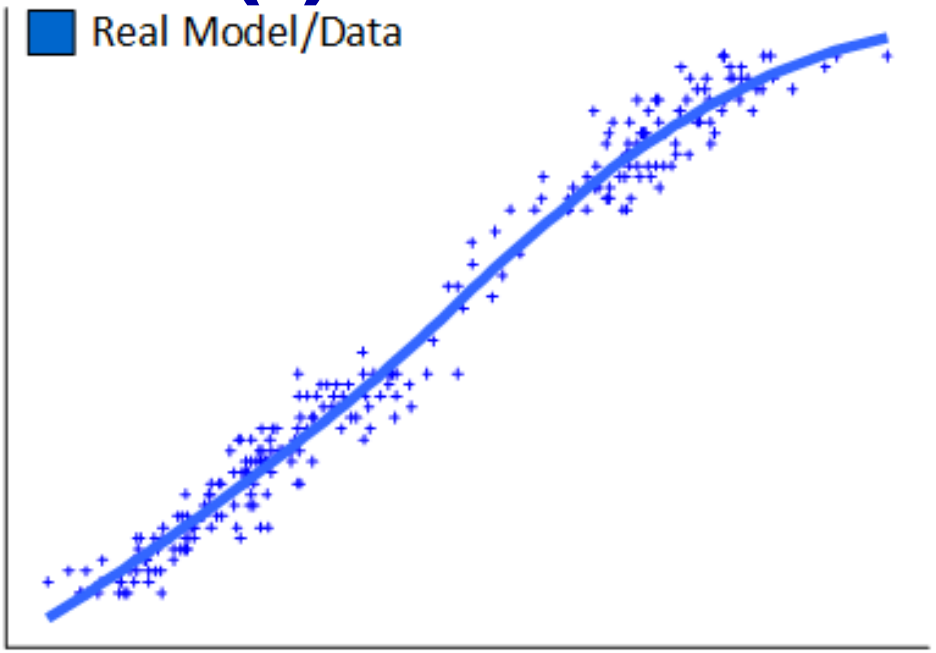
- Cruzando informacion de multiples fuentes se puede llegar a adquirir nuevos conocimientos que no se encontraban originalmente

Dataset del concurso de Netflix (IV)



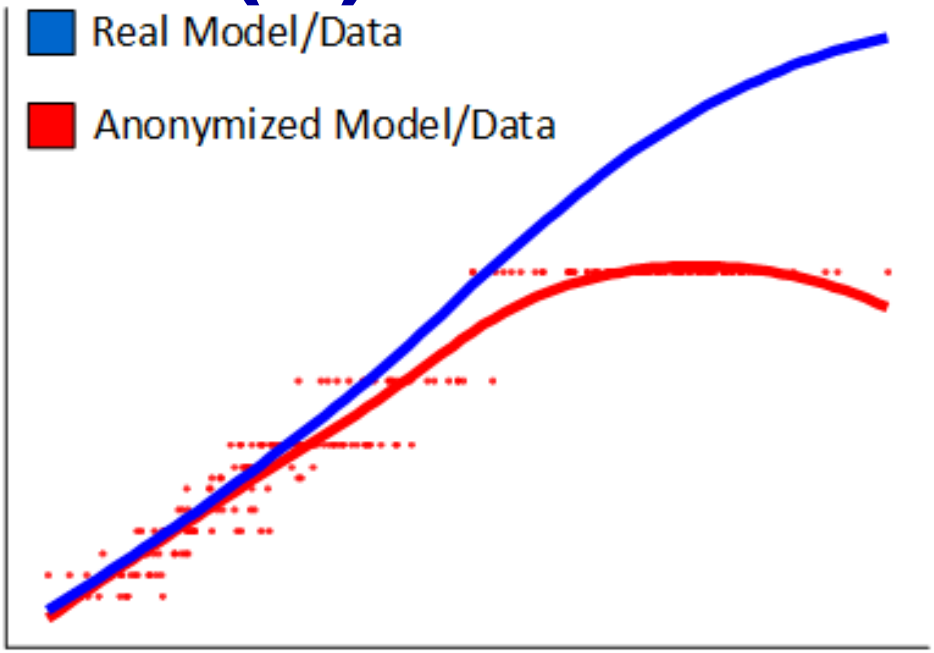
- Algo tan “Inofensivo” puede ser empleado para predecir la ideología política de los usuarios (dato sensible)

Contexto (I)



- Efectos de la anonimizacion
  - Mejora la privacidad → Se pierde información
  - Altera los datos afectando a aquellos desarrollos altamente dependientes de los mismos (p.ej. Modelos de inteligencia artificial

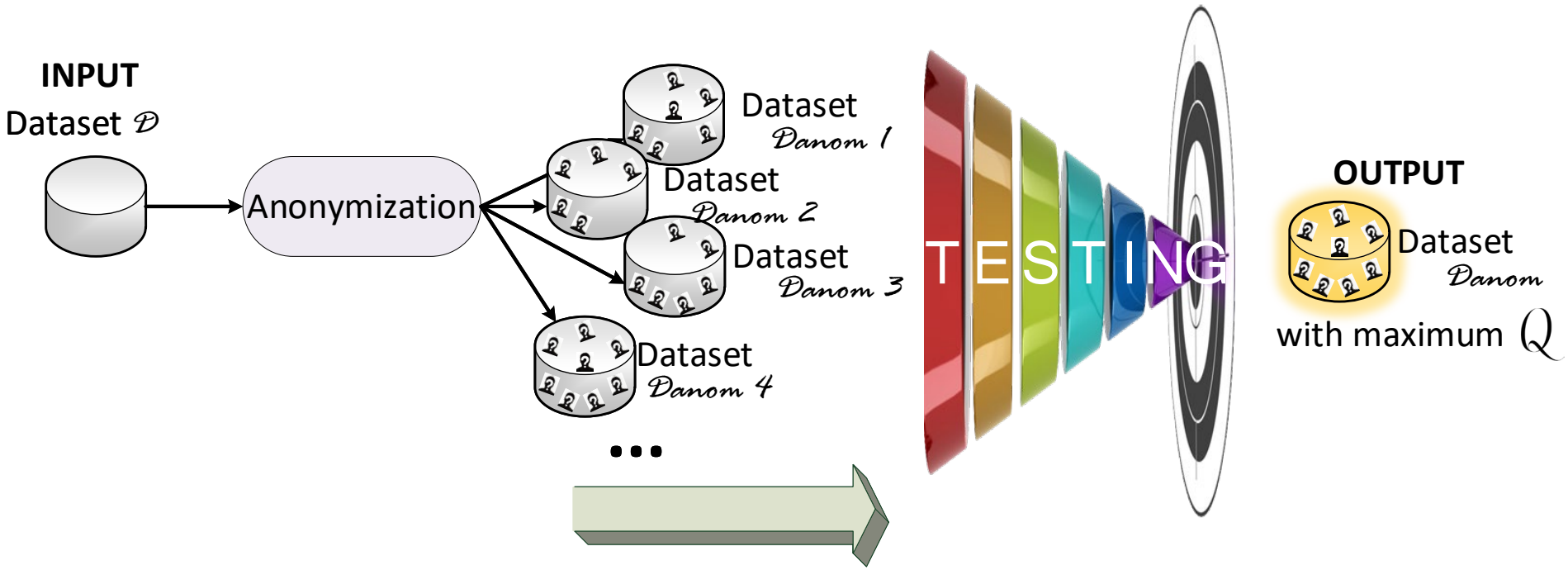
Contexto (II)



- Enmascaramiento de fallos
  - Puede darse el caso de que un modelo de IA que funcione correctamente en desarrollo falle dramáticamente al ser puesto en producción

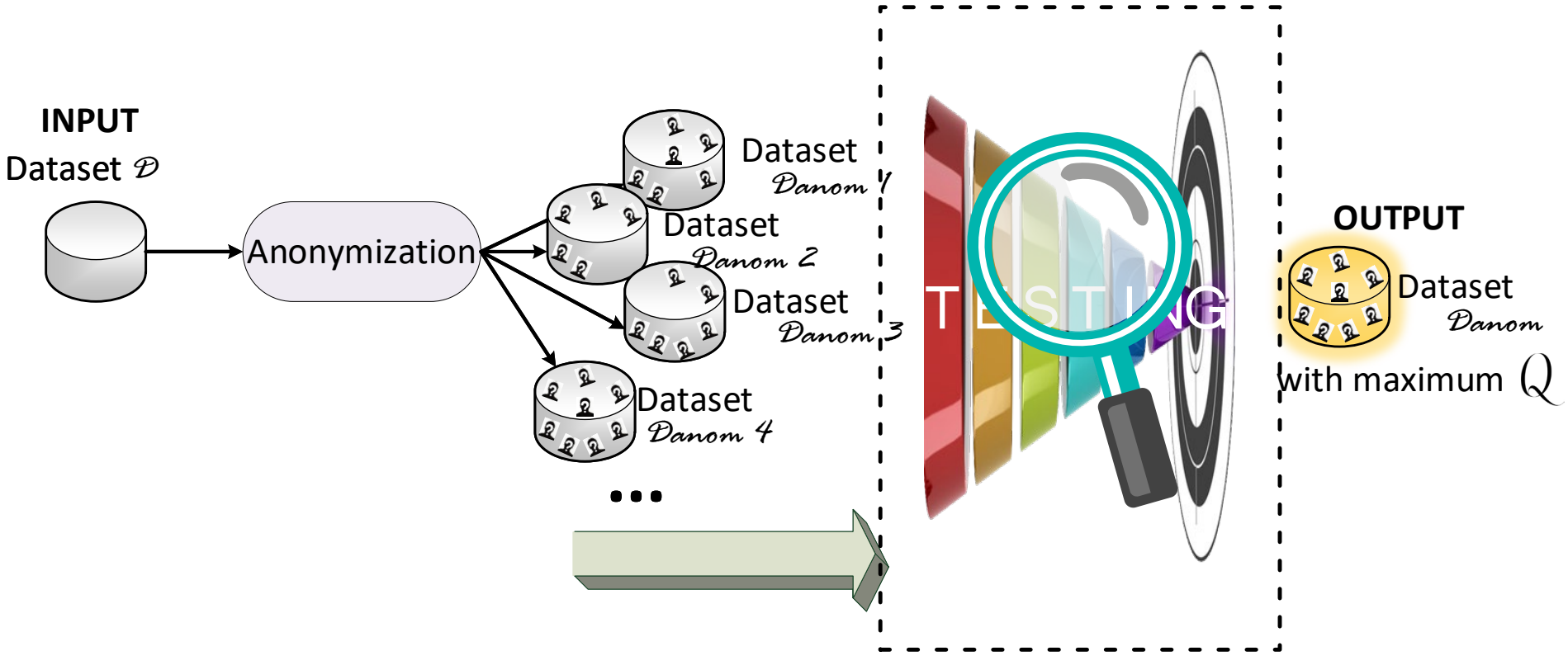
Anonimización de datos guiada por pruebas para aplicaciones inteligentes

Plano general



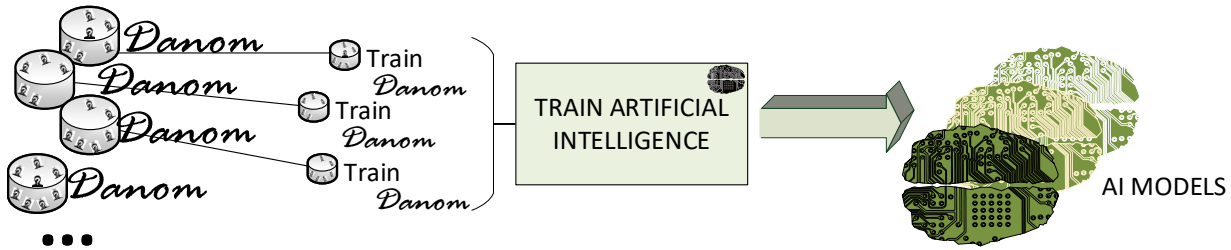
Anonimización de datos guiada por pruebas para aplicaciones inteligentes

Plano general



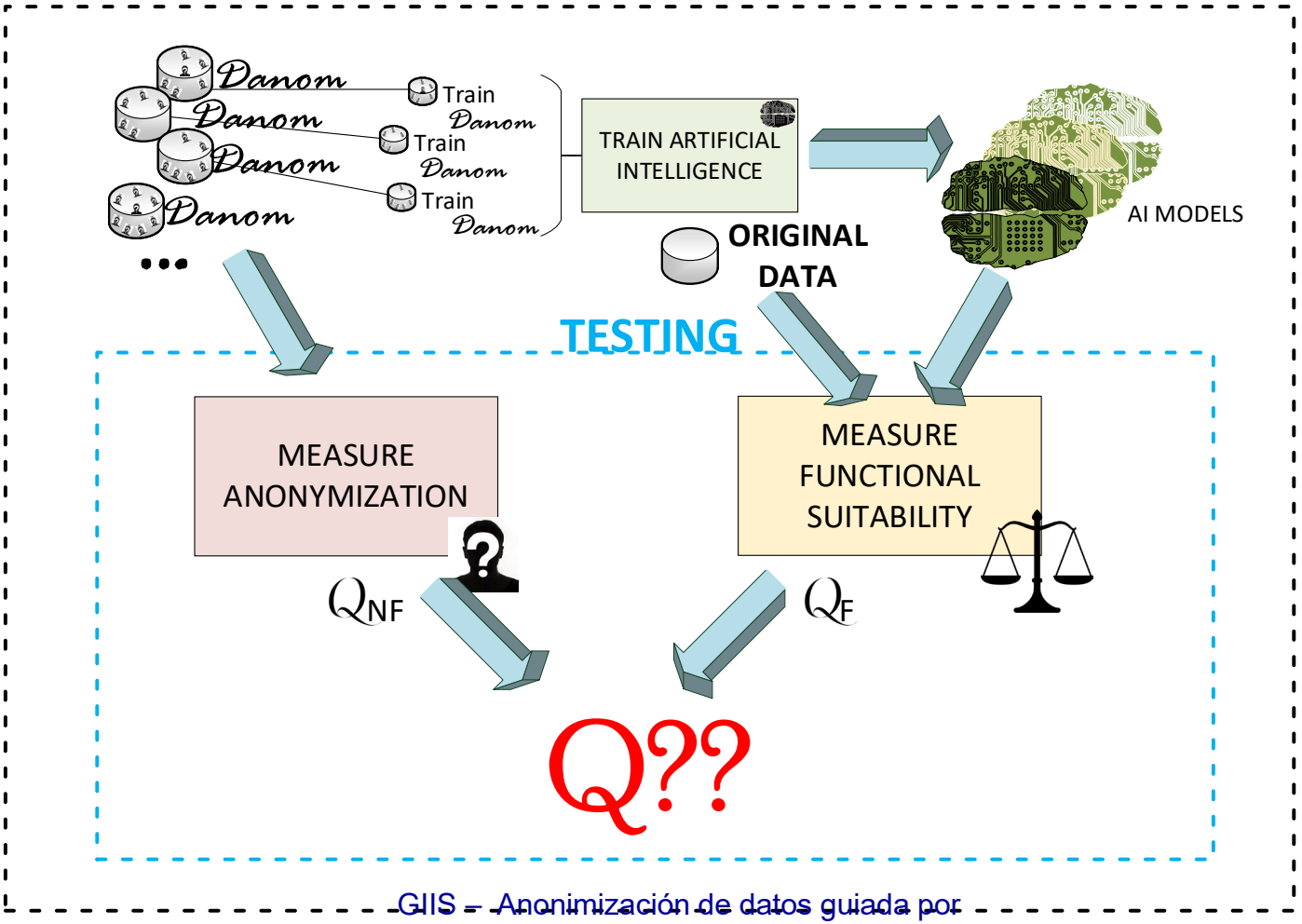
Anonimización de datos guiada por pruebas para aplicaciones inteligentes

Enfoque



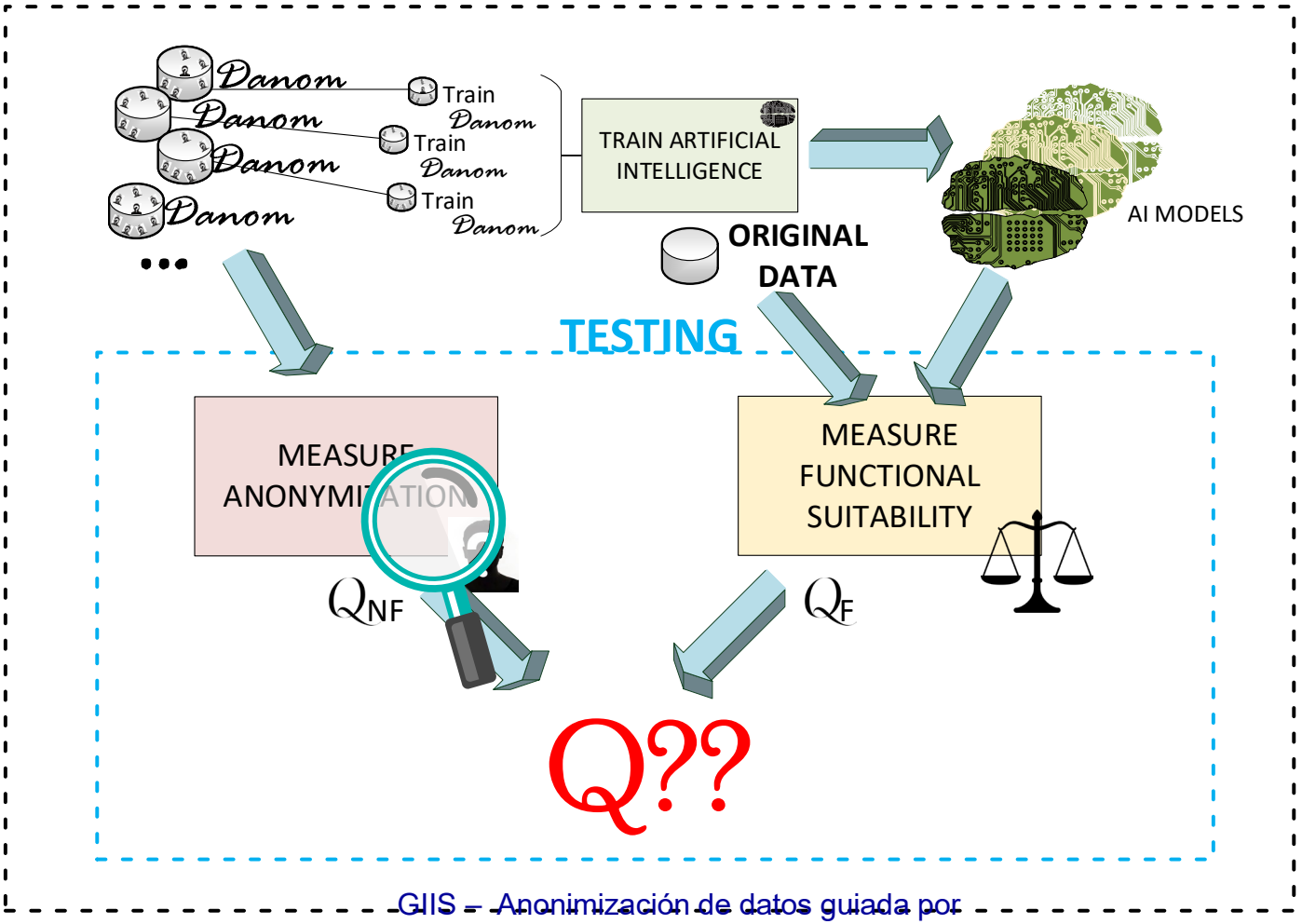
Anonimización de datos guiada por pruebas para aplicaciones inteligentes

Enfoque



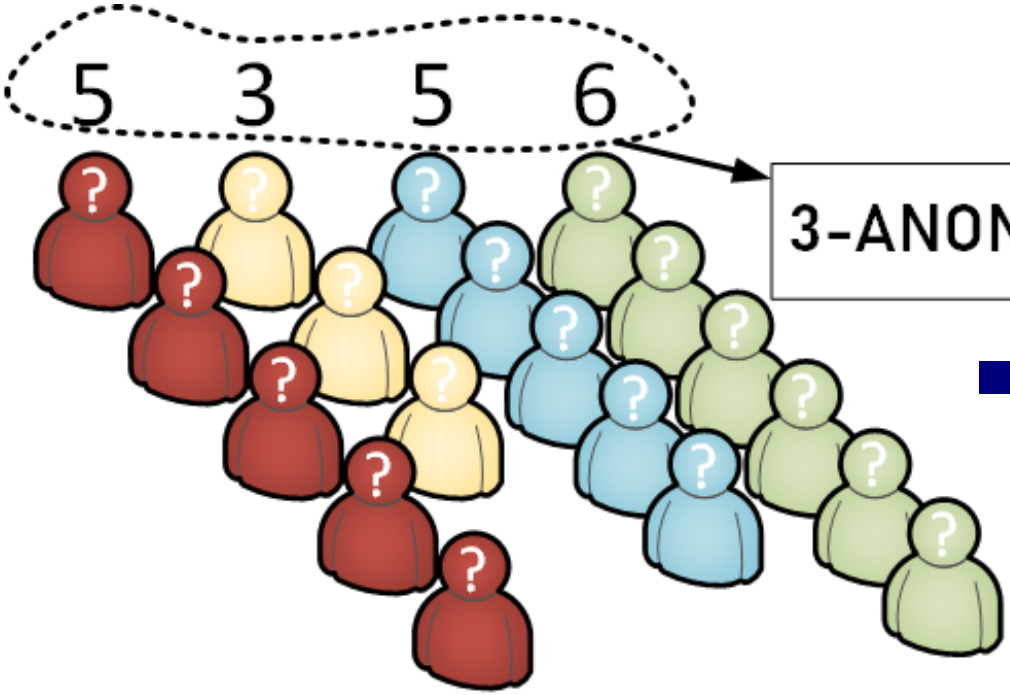
Anonimización de datos guiada por pruebas para aplicaciones inteligentes

Enfoque



Anonimización de datos guiada por pruebas para aplicaciones inteligentes

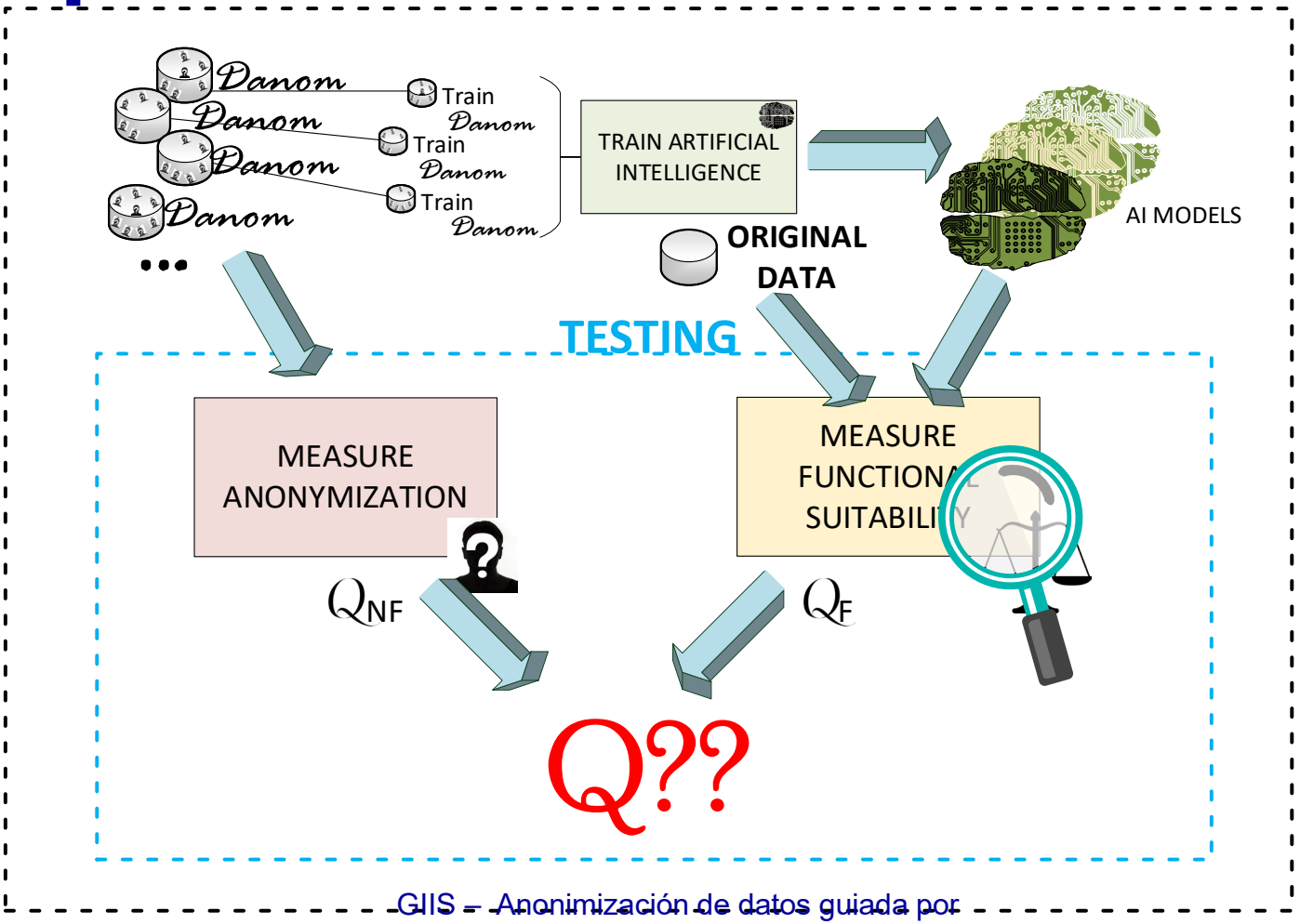
Calidad no-funcional



- K-Anonimidad:
  - Garantiza que al menos existen K-Individuales con la misma combinación de pseudo-identificadores

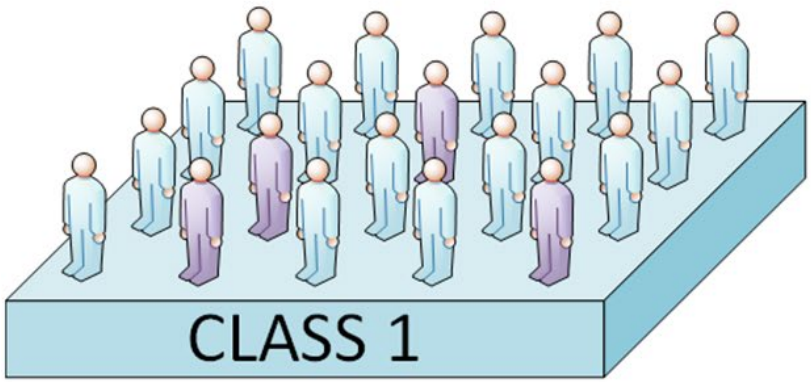
Anonimización de datos guiada por pruebas para aplicaciones inteligentes

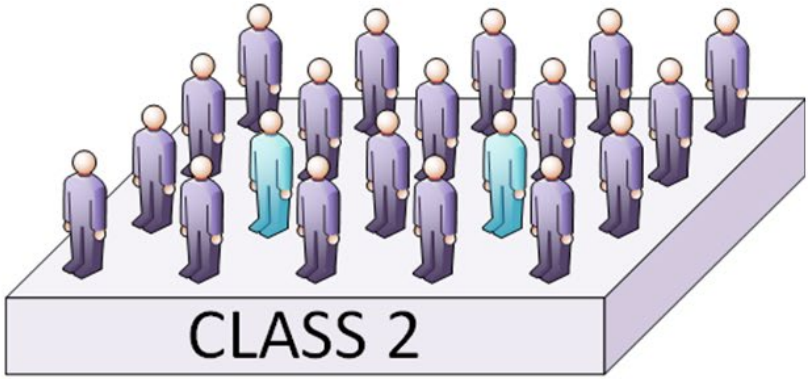
Enfoque



Anonimización de datos guiada por pruebas para aplicaciones inteligentes

Adecuación funcional

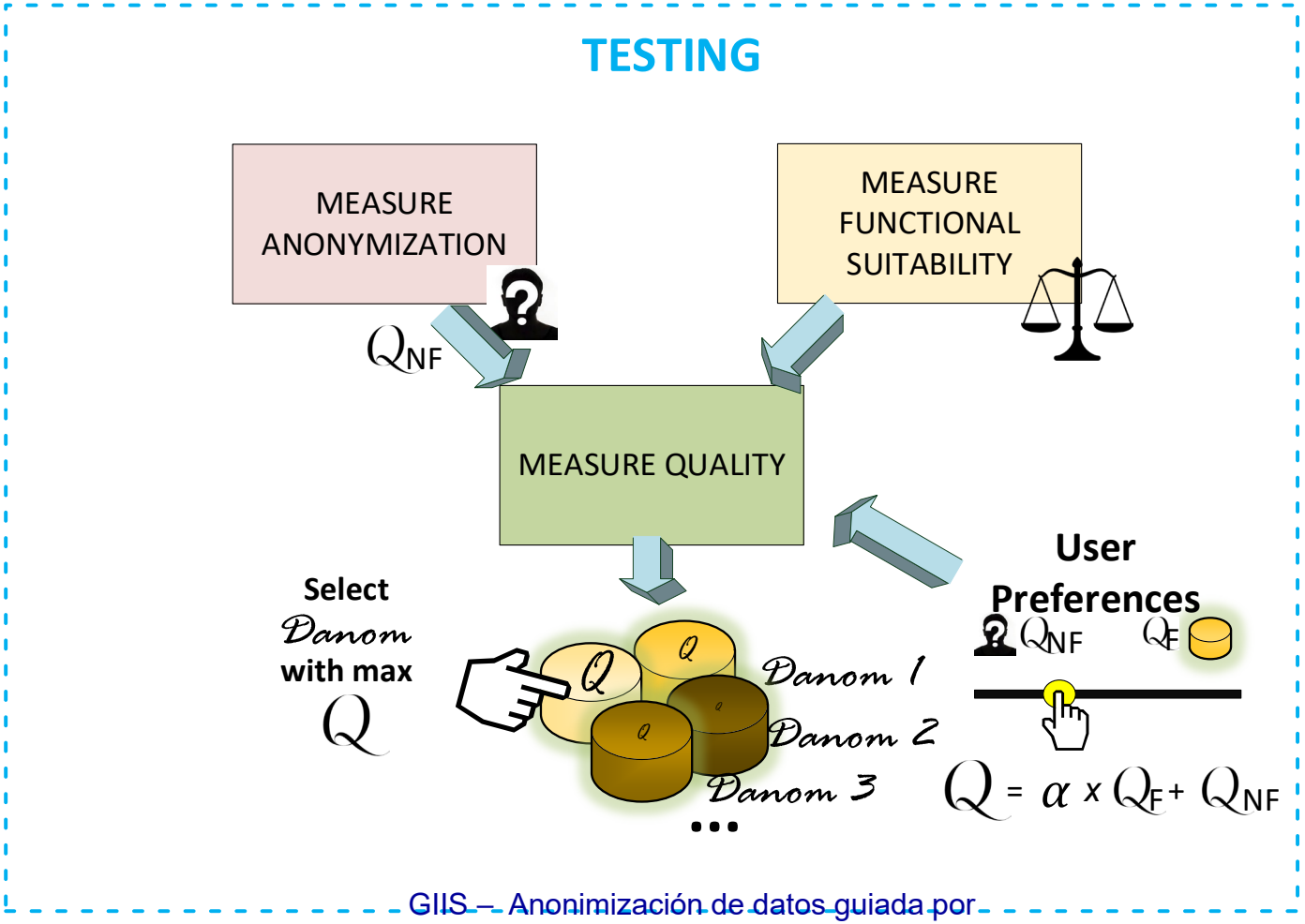




$$Accur = \frac{Nº_{\checkmark} + \checkmark}{Nº_{\,}}$$

Anonimización de datos guiada por pruebas para aplicaciones inteligentes

Metrica de calidad



Conclusiones y trabajo futuro

- Conclusiones
  - Nuestro enfoque logra un punto de compromiso entre la privacidad y la adecuación funcional de los datos.
  - Nuestro enfoque permite a las terceras partes la liberación de datos seguros a la vez de útiles
- Trabajo Futuro
  - Evaluar la técnica en varios conjuntos de datos
  - Automatizar el enfoque
  - Evaluar la dependencia entre el enfoque y los diferentes algoritmos de IA

Este trabajo ha sido realizado bajo el proyecto de investigación TestEAMos (TIN2016-76956-C3-1-R), financiado por el Ministerio Español de Economía y Competitividad junto con fondos FEDER

Preguntas?

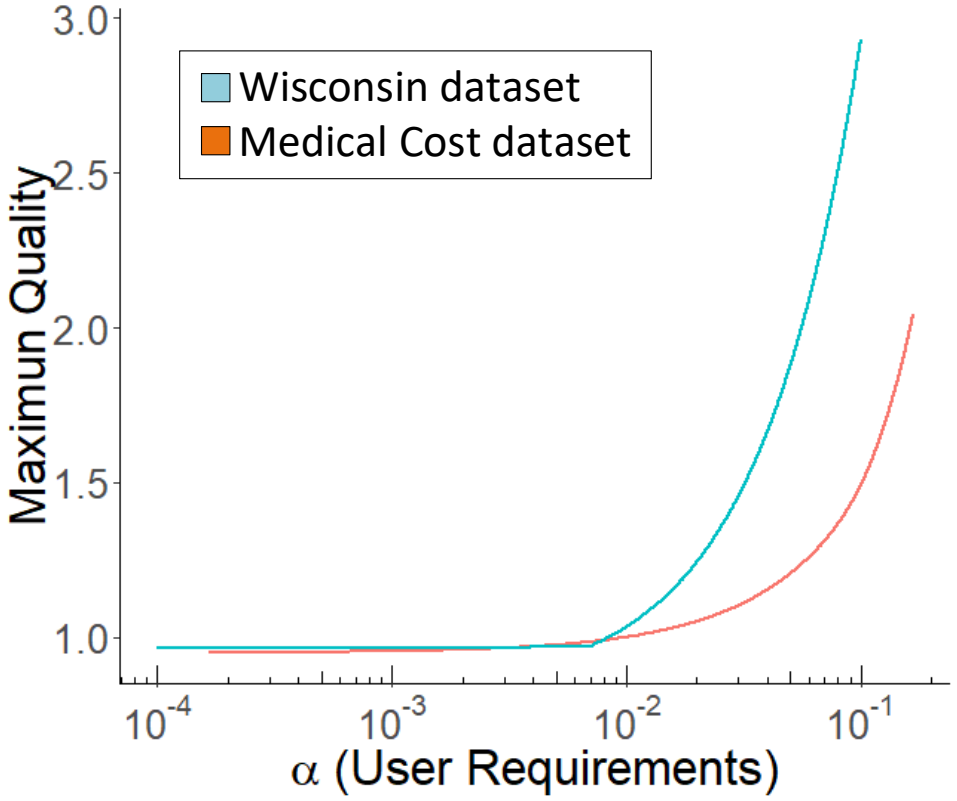
Cristian Augusto, Jesús Morán, Claudio de la Riva and Javier Tuya
Grupo de Investigación en Ingeniería del Software
http://giis.uniovi.es
Universidad de Oviedo

Preferencias del usuario

- Representadas por un valor α
  - Prioriza la utilidad de los datos o la privacidad
- Nuestra metrica de calidad:
  - $Q = QF + \alpha \cdot QNF$

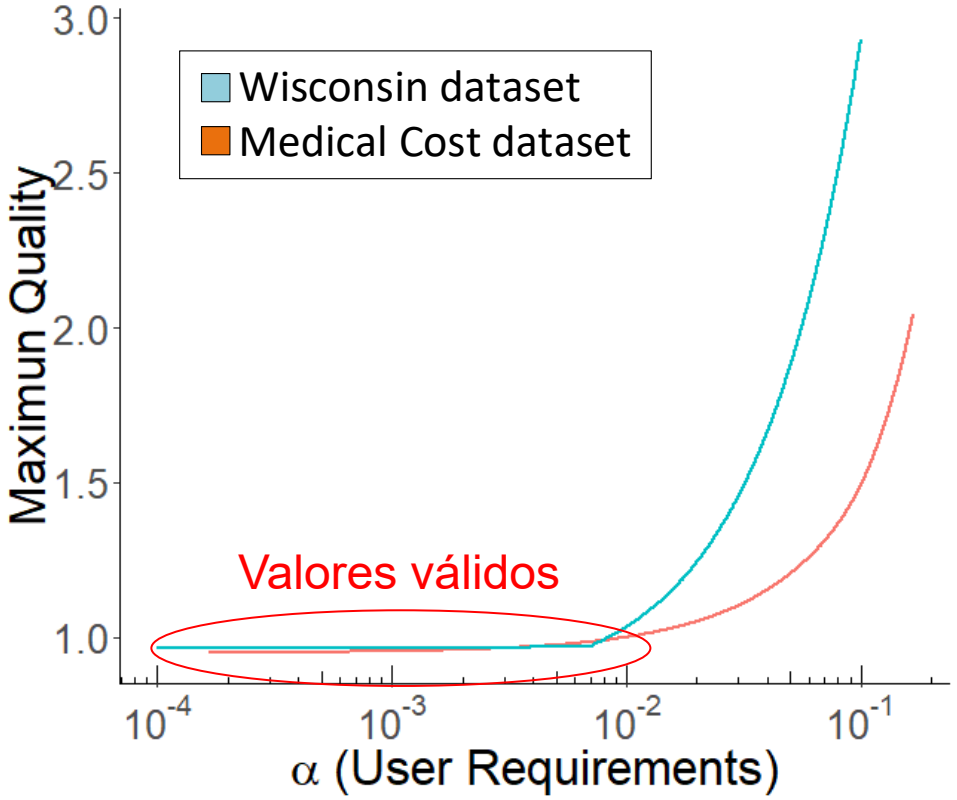
Preferencias del usuario

- Eligiendo el valor :



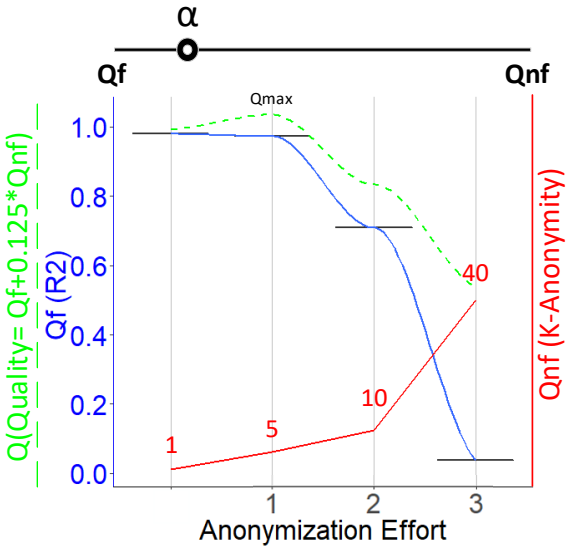
Preferencias del usuario

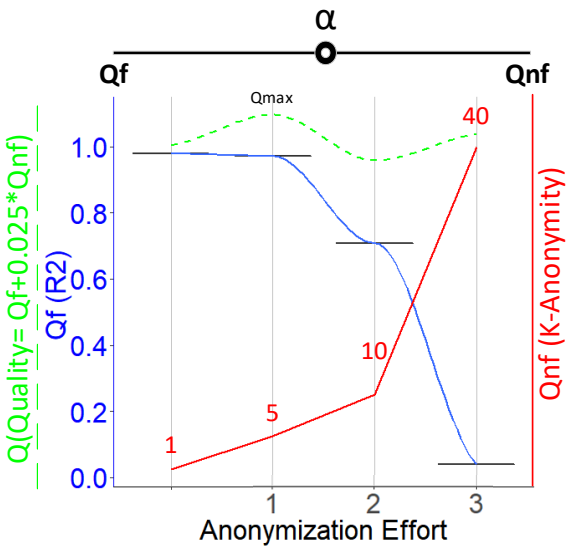
- Eligiendo el valor :

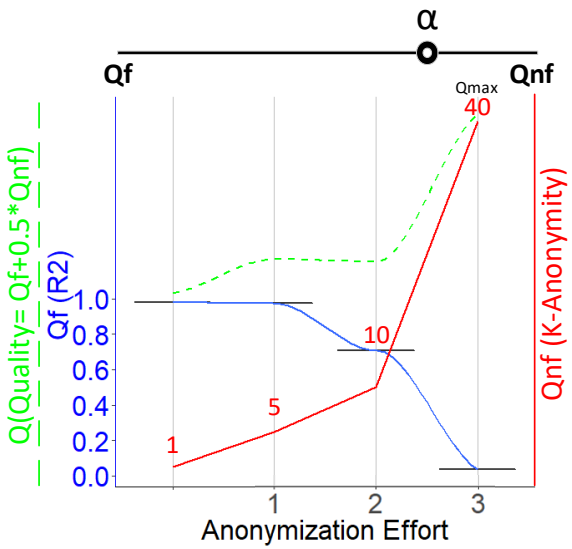


Preferencias del usuario

- Diferentes ponderaciones:

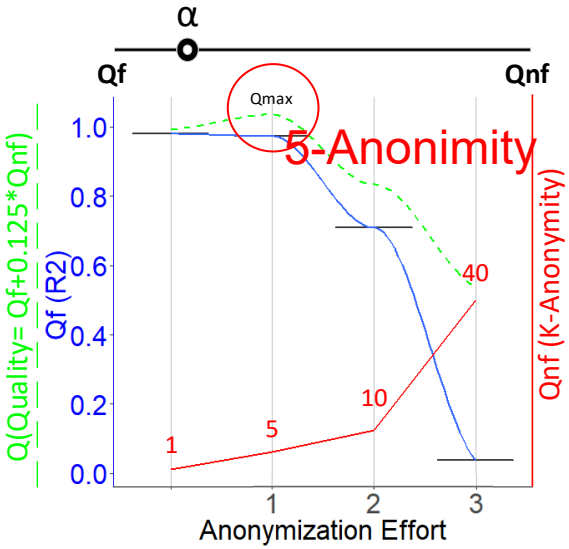


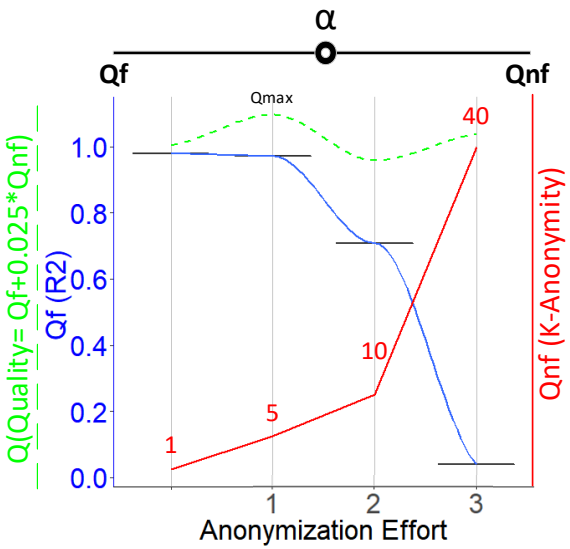


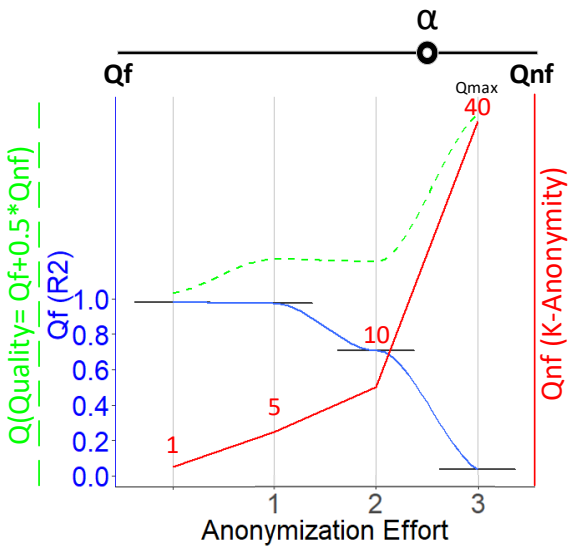


Preferencias del usuario

- Diferentes ponderaciones:

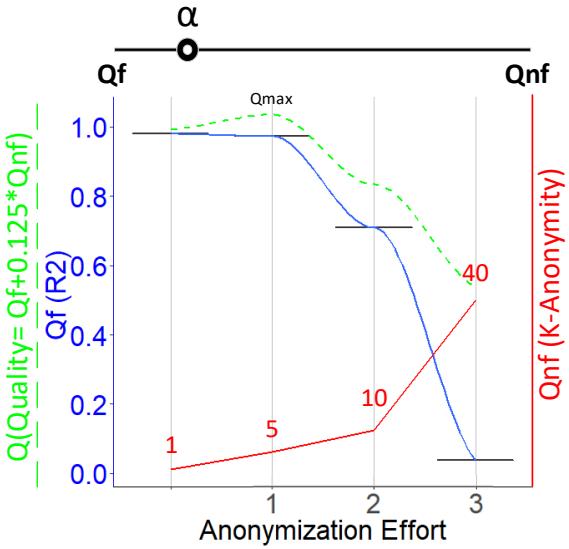


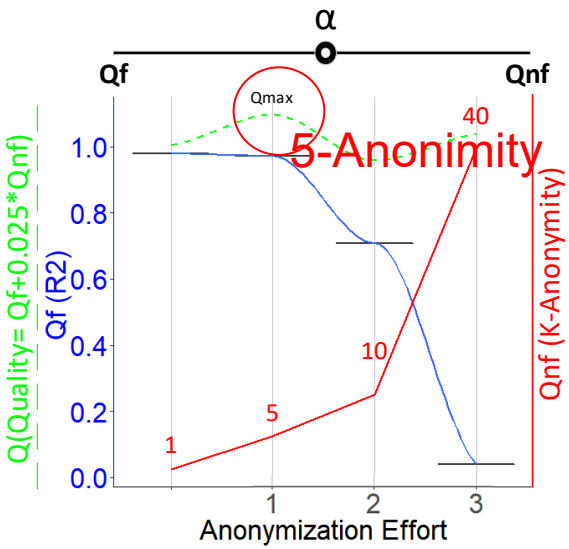


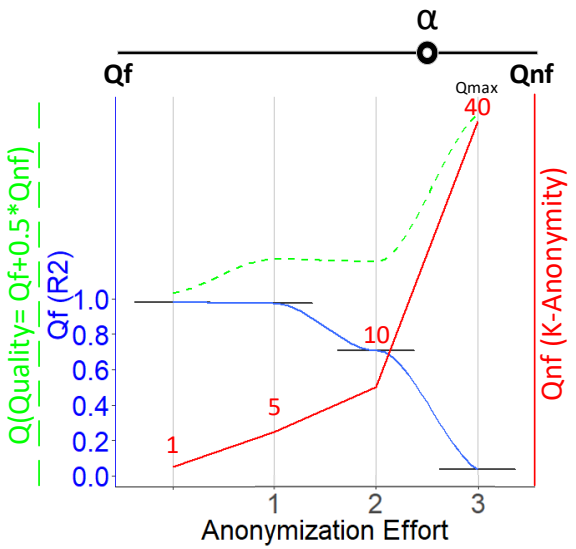


Preferencias del usuario

- Diferentes ponderaciones:

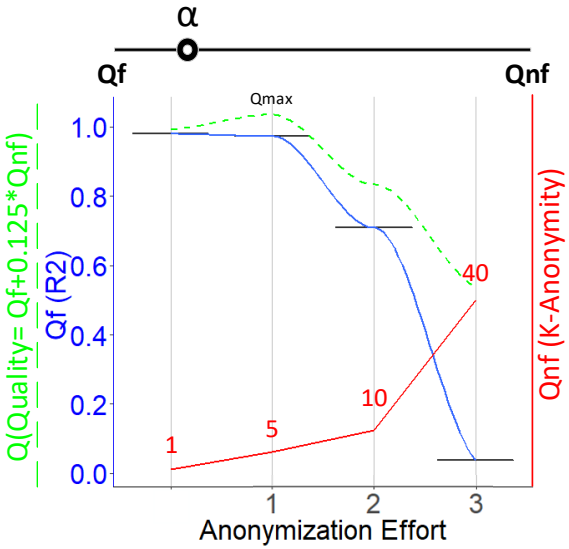


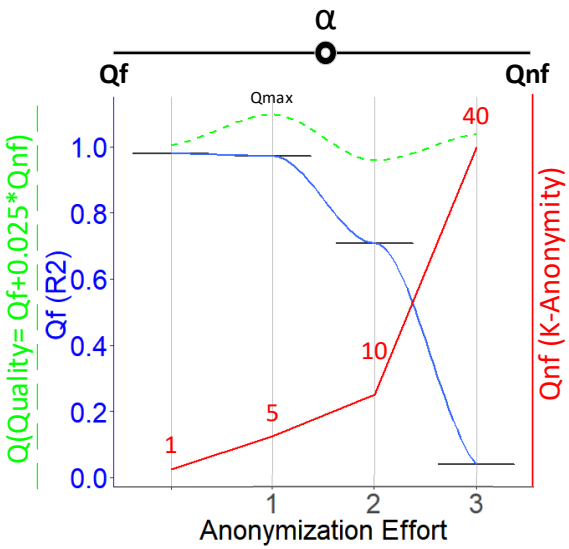


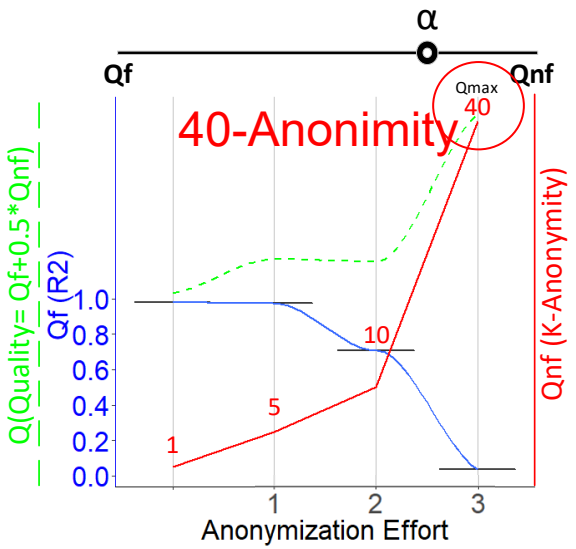


Preferencias del usuario

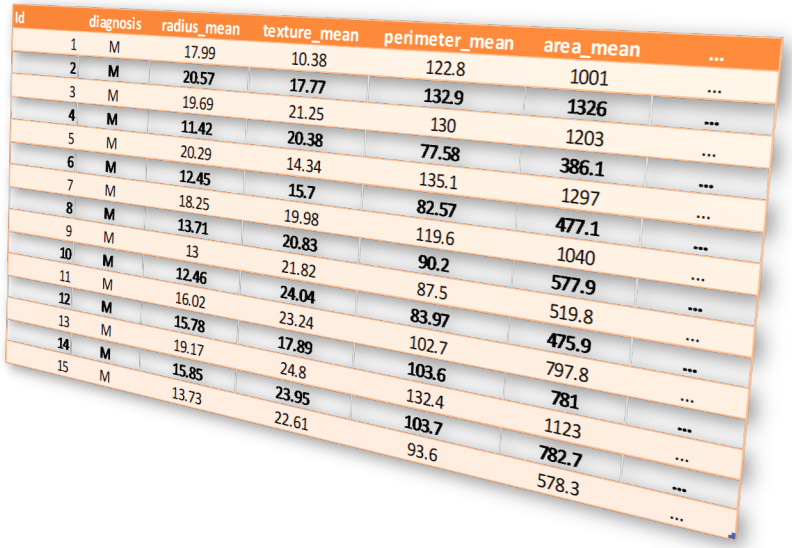
- Diferentes ponderaciones:







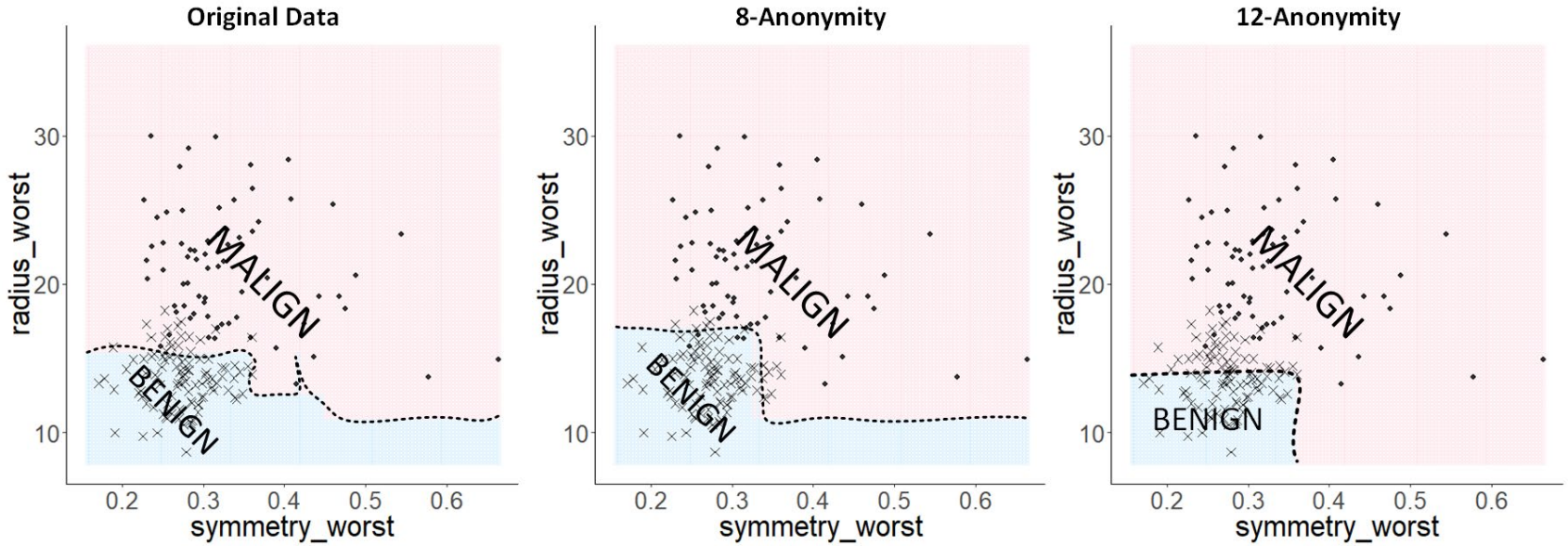
Experimentación (I)



Id	diagnosis	radius_mean	texture_mean	perimeter_mean	area_mean	...
1	M	17.99	10.38	122.8	1001	...
2	M	20.57	17.77	132.9	1326	...
3	M	19.69	21.25	130	1203	...
4	M	11.42	20.38	77.58	386.1	...
5	M	20.29	14.34	135.1	1297	...
6	M	12.45	15.7	82.57	477.1	...
7	M	18.25	19.98	119.6	1040	...
8	M	13.71	20.83	90.2	577.9	...
9	M	13	21.82	87.5	519.8	...
10	M	12.46	24.04	83.97	475.9	...
11	M	16.02	23.24	102.7	797.8	...
12	M	15.78	17.89	103.6	781	...
13	M	19.17	24.8	132.4	1123	...
14	M	15.85	23.95	103.7	782.7	...
15	M	13.73	22.61	93.6	578.3	...

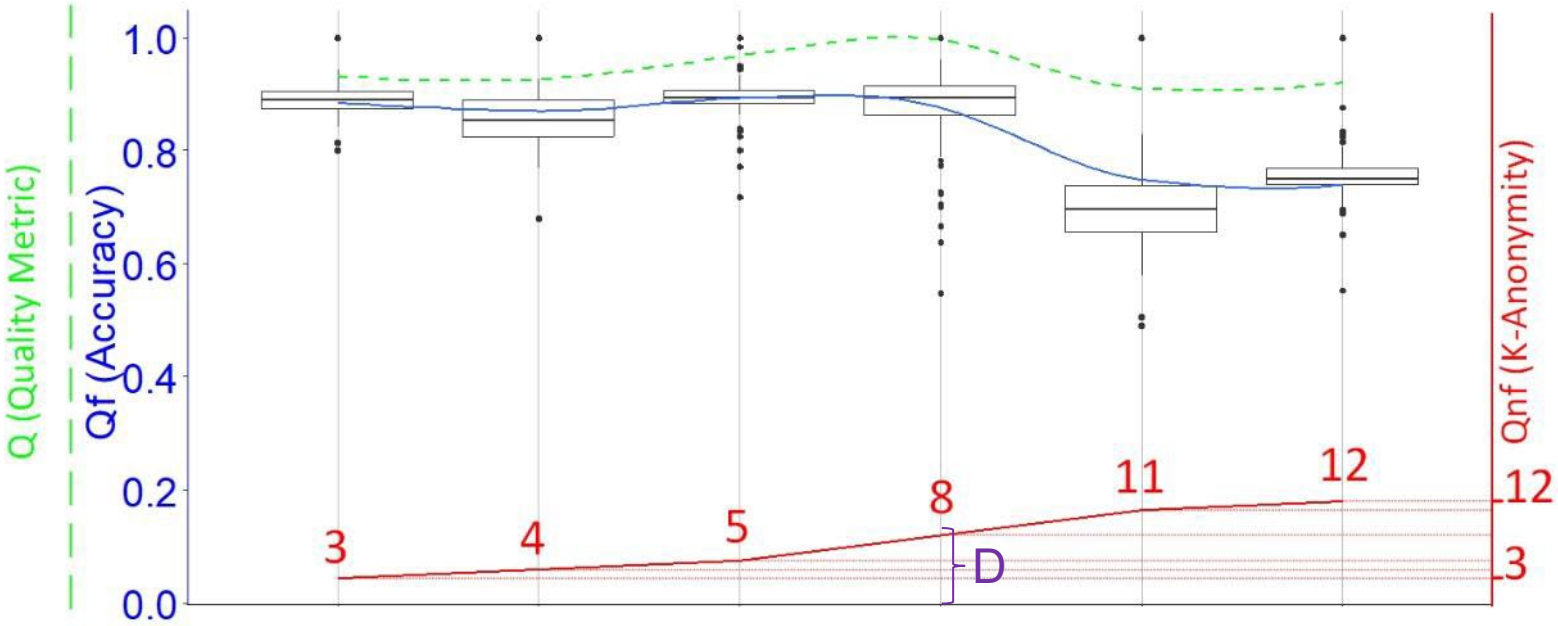
- Dos datasets de dominio publico referents a temas medicos
  - Breast-Cancer(Wisconsin) Dataset
  - Medical Cost Personal Dataset
- Usando tecnicas de generalizacion sobre los pseudo-identificadores numericos

Experimentacion(II)



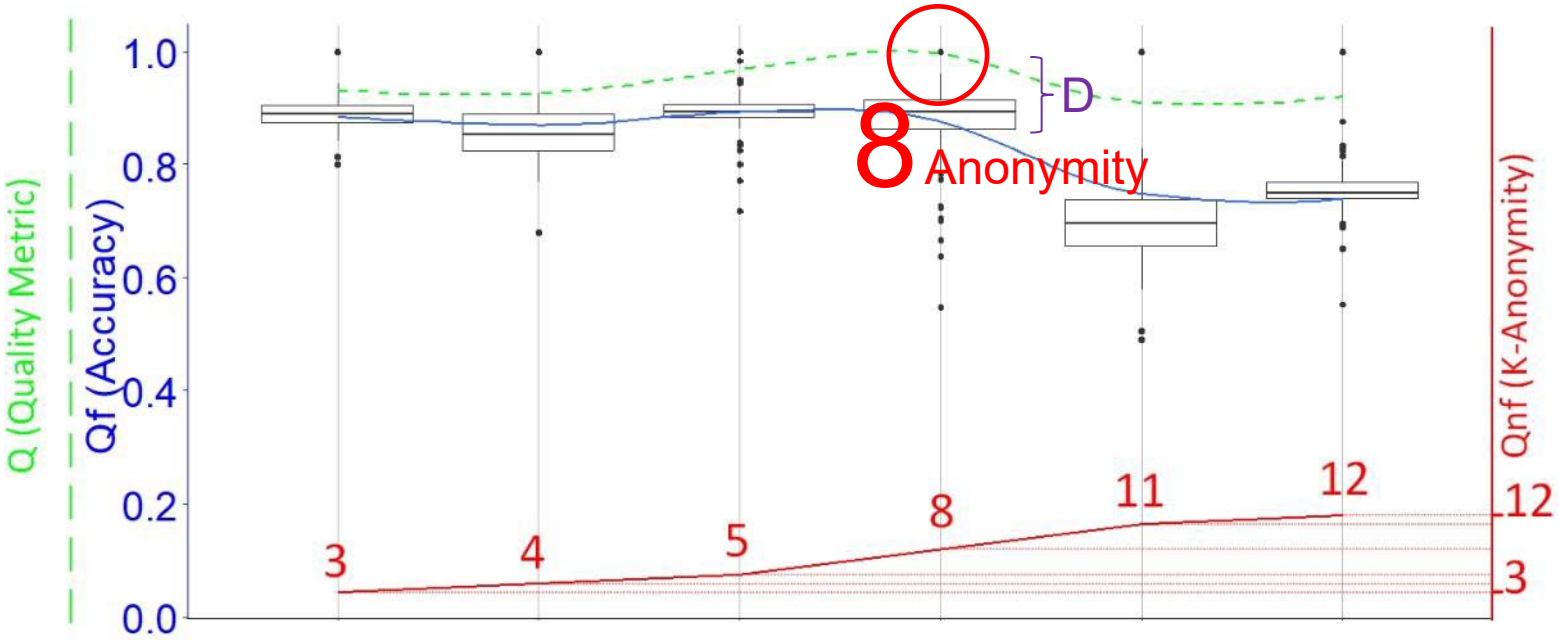
- Wisconsin Dataset:
  - Usa un algoritmo RandomForest Algorithm para clasificar empleando dos metricas de los tumores
  - Trata de predecir la clase del tumor(malign o benigno)

Experimentacion(III)



- Wisconsin Dataset:
  - Alcanza el punto de compromiso entre calidad funcional y no funcional en 8-Anonimidad

Experimentacion (IV)



- Wisconsin Dataset:
  - Alcanza el punto de compromiso entre calidad funcional y no funcional en 8-Anonimidad