Organiza

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Foro GRC
Privacidad · IA · Ciberseguridad

Insight Foro GRC

Datos seudonimizados y su impacto en Inteligencia Artificial

Mesa debate: Caso de uso IA – Intervención de equipos de cumplimiento (DPD, CISO, Equipos IA)

Taller práctico: Categorización de casos de uso según RIA.

Foro GRC
Privacidad
Ciberseguridad
IA

Miércoles 22 octubre - 16:00 - streaming

Partners Estratégicos

Telefónica Tech

GOUERTIS
Part of Telefónica Tech

CANAL AEC

CLUB DPD AEC

CLUB CISO AEC

Foro GRC IA

¡Bienvenidos al INSIGHT 2025 FORO GRC!

- Una ponencia sobre los datos seudonimizados y su impacto en la IA
- Una mesa de debate sobre un caso de uso IA: la intervención de equipos de cumplimiento
- Un taller práctico exclusivo para los miembros del Foro GRC sobre la categorización de casos de uso según RIA
- Especialistas y expertos de primer nivel:
  - Alberto Casaseca
  - Óscar Labella
  - Mª Concepción Campos
  - Francisco Lázaro
  - Víctor Martínez
  - Marta de Luis Diez

16:00h – 16:05h **Apertura y bienvenida**

16:05h – 16:45h **Ponencia | Datos seudonimizados y su impacto en la IA**
Alberto Casaseca - DPO | Gobierno, Riesgo y Cumplimiento en Privacidad, Ciberseguridad e Inteligencia Artificial, CLECE

16:45h – 17:35h **Mesa Debate | Caso de uso IA: Intervención de equipos de cumplimiento**

Moderador: **Óscar Labella -** Consultor GRC, Govertis, parte de Telefónica Tech

Mª Concepción Campos Acuña - Doctora en Derecho, Directiva Pública profesional, Experta en Compliance, Transformación digital e IA.
Francisco Lázaro - Gerente de Área de Ciberseguridad y Privacidad (CISO | DPO), Grupo Renfe
Víctor Martínez Calvo - Software Manager y Líder de Productos de Compliance, Lefebvre

*(Finaliza la sesión en abierto y comienza el **taller exclusivo para los miembros del Club DPD**)*

17:40h – 18:20h **Taller para socios | Categorización de casos de uso según RIA**
Marta de Luis Diez - Consultora GRC, Govertis, parte de Telefónica Tech

18:25h – 18:30h **Clausura**

Organiza AEC

Partners estratégicos Telefónica Tech GOVERTIS Part of Telefónica Tech

Foro GRC
Gobierno, Riesgo y Cumplimiento

FORO GRC AEC

En un escenario disruptivo, marcado por **desafíos tecnológicos y regulatorios sin precedentes**, surge **la necesidad de unir voces**, perspectivas y conocimientos en un **espacio común** para los profesionales del GRC (Gobierno, Riesgo y Cumplimiento).

El Foro GRC es un **nuevo ecosistema pionero** en España, impulsado por la AEC junto a sus partners estratégicos: Telefónica Tech y Govertis, parte de Telefónica Tech.

PROTECCIÓN DE DATOS Y PRIVACIDAD – CIBERSEGURIDAD – INTELIGENCIA ARTIFICIAL

CLUB DPD AEC

CLUB CISO AEC

Foro GRC IA

Organiza AEC

Partners estratégicos Telefónica Tech GOVERTIS Part of Telefónica Tech

Foro GRC
Gobierno, Riesgo y Cumplimiento

VENTAJAS FORO GRC AEC

Insights todo el año
Para conectar, conocer las mejores prácticas y estar en vanguardia.

Comunidad y Networking
Comparte tu experiencia, resuelve dudas al instante y multiplica tu red.

Congreso Anual
Líderes y profesionales de ámbitos del GRC para debatir las cuestiones más actuales y las claves de futuro

Premios Foro GRC
Reconocimientos a la excelencia y la trayectoria profesional en el ámbito

Talleres exclusivos
Aprende y descubre lo último, desde la práctica, con los mejores

Blogs y actualidad
Permanentemente actualizado con artículos relevantes

Formación especializada
Para ti y tus equipos. -20% en toda la Formación AEC en la materia

Certificación Profesional
Certificamos los conocimientos y habilidades de los profesionales desde 1997

ACTUALIZACIÓN CONTINUA

Más de 4.200 profesionales han confiado en nuestra formación

PROTECCIÓN DE DATOS

275 ediciones con más de 2.950 alumnos

- Programas para el acceso a la certificación DPD-AEPD
  - Programa Superior DPD
  - Programa Avanzado DPD
  - Curso de preparación examen DPD
- Formación complementaria y sectorial (formación válida para la renovación de la certificación)
  - Educativo
  - Público
  - Sanitario
  - Relaciones Laborales
  - Publicidad Digital
  - Procedimiento sancionador
  - Videovigilancia
  - Desconexión digital
  - Brechas de seguridad
  - Continuidad de negocio
  - Canal de denuncias
  - EIPD en Transferencias Internacionales
  - ISO 27701, EIPD

CIBERSEGURIDAD

85 ediciones con más de 900 alumnos

- Gestión de la ciberseguridad industrial
- Programa Executive: Ciberseguridad industrial
- Directiva NIS2
- ISO 27001
- ENS

INTELIGENCIA ARTIFICIAL

30 ediciones con más de 350 alumnos

- Programas para el acceso a la certificación GRC-IA
  - Experto en GRC aplicado a la IA
  - Curso de preparación de examen GRC-IA
- Especialista en el Reglamento IA
- ISO 42001
- IoT y Big Data e IA

Información completa sobre la oferta formativa

Ventajas especiales
miembros FORO GRC
20% descuento

Foro GRC

Gobierno, Riesgo y Cumplimiento

NUEVA CERTIFICACIÓN PROFESIONAL GOBIERNO, RIESGO Y CUMPLIMIENTO EN INTELIGENCIA ARTIFICIAL (CP-GRC-IA)

Perfil: profesional capaz de gestionar de forma integrada los riesgos, la gobernanza y el cumplimiento (GRC) de la inteligencia artificial.

Dominios de conocimiento:

PARTE GENERAL Fundamentos GRC	PARTE ESPECÍFICA GRC aplicado a la IA
D1: Fundamentos IA	**D1: Fundamentos avanzados de la IA**
D2: Fundamentos PD	**D2: Cumplimiento Legal y Normativo de la IA**
D3: Fundamentos SI	**D3: Marco Organizativo y Gobierno Corporativo de la IA**
D4: Fundamentos SG	**D4: Gestión de Riesgos de IA y Evaluación de Impacto**

Acceso al examen:

A. Estándar: Prerrequisitos + examen

Opciones	Prerrequisitos (se ha de cumplir al menos uno)	Detalle prerrequisito
Opción 1.	**3 años de experiencia profesional acreditable**	**En al menos 2 de los dominios recogidos en la PARTE GENERAL: Fundamentos GRC**
Opción 2.	**140 horas formación**	**En al menos 2 de los dominios recogidos en la PARTE GENERAL: Fundamentos GRC**
Opción 3.	**Formación especializada GRC IA**	**Formación “Experto en GRC IA” de la AEC (incluye simulaciones de examen)** **- Curso online tutorizado (110 horas)**

B. Méritos extraordinarios (excepcional y por tiempo limitado)

CERTIFICACIÓN PROFESIONAL
GRC IA
AEC
CERPER

Certificación Profesional GRC en Inteligencia Artificial (CP-GRC-IA)

FORMACIÓN

Curso de Preparación

- ✓ Online a tu ritmo, temario descargable y más de 240 preguntas de simulación para el examen.
- ✓ Recomendado para la opción 1 y 2 de los prerequisitos de acceso.

Programa Experto GRC IA

- ✓ Formación completa de 110 horas con tutorías y clases en directo.
- ✓ Acceso directo a la certificación.
- ✓ Formación bonificable.

EXAMEN

80 preguntas tipo test. Puntuación mínima: 70% global y 50% por cada parte. Dos oportunidades.

CONVOCATORIAS

- ➢ **25 de noviembre de 2025**
- ➢ **16 de diciembre de 2025**
- ➢ **29 de enero de 2026**

MANTENIMIENTO

Validez de 3 años. Renovación con 30 horas de formación continua (mínimo 10h formación específica IA).

VENTAJAS CERTIFICACIÓN

Reconocimiento Profesional

Te posiciona como referente en gestión ética y responsable de la IA.

Empleabilidad

Altamente valorado en mercado emergente, incrementando oportunidades laborales.

Red de Contactos

Integración en comunidad de expertos para compartir experiencias.

Impacto Organizacional

Aportas valor estratégico, mitigando riesgos y asegurando cumplimiento.

Partners estratégicos

AEC

Telefónica Tech

GOVERTIS
Part of Telefónica Tech

CLUB DPD AEC

CLUB CISO AEC

Foro GRC IA

¡Súmate!

Organiza

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Foro GRC
Privacidad · IA · Ciberseguridad

Insight Foro GRC

Datos seudonimizados y su impacto en Inteligencia Artificial

Mesa debate: Caso de uso IA – Intervención de equipos de cumplimiento (DPD, CISO, Equipos IA)

Taller práctico: Categorización de casos de uso según RIA.

Miércoles 22 octubre - 16:00 - streaming

Partners Estratégicos

Telefónica Tech

GOOERTIS
Part of Telefónica Tech

CANAL AEC

"Seudonimización, anonimización y su impacto en la inteligencia artificial"

Alberto Casaseca

DPD, GRC en Privacidad e IA

https://www.linkedin.com/in/acasaseca/

Seudonimización vs. Anonimización

SEUDONIMIZACIÓN

Se ha **reemplazado el identificador directo** (ej. nombre, DNI) por un código o pseudónimo.

- Existe una **clave de correspondencia** que permitiría volver a identificar
- Los datos **siguen siendo personales** bajo el RGPD
- El proceso es **reversible** con la clave adecuada
- Conserva la **estructura relacional** de los datos

ANONIMIZACIÓN

Los datos han sido tratados de forma **irreversible** para que ninguna persona pueda ser identificada directa ni indirectamente.

- **No existe clave** de reidentificación posible
- En principio, **dejan de estar bajo el RGPD**
- El proceso es **irreversible**
- La anonimización **absoluta e irreversible** no es tan sencilla de lograr

La confusion habitual sobre la anonimización

- La anonimización debe cumplir los **tres criterios acumulativos** del Grupo de Trabajo del Artículo 29 (GT29). Si no se cumplen todos, **NO estamos ante una verdadera anonimización**.

a) Individualización

Imposibilidad de aislar a un individuo dentro del conjunto de datos

b) Correlación

Imposibilidad de vincular registros del mismo individuo en diferentes bases de datos

c) Inferencia

Imposibilidad de deducir información adicional sobre el individuo

La confusion habitual sobre la anonimización

⚠ Ejemplo de "Falsa Anonimización"

Dataset de candidaturas (supuestamente anonimizado):

- Edad: 34 años
- Género: Mujer
- Formación: Máster en IA, Universidad X
- Experiencia: 8 años en sector tech
- Localidad: Madrid (generalizada)
- Fecha entrevista: marzo 2023

¿Por qué NO es anonimización real?

✗ **Individualización:** La combinación de atributos es muy específica

✗ **Correlación:** Cruzable con LinkedIn, redes sociales o bases públicas

✗ **Inferencia:** Permite deducir información sensible adicional

Los atributos quasi-identificadores permiten la singularización indirecta del individuo

Cuando cabe la posibilidad de inferencia o singularización mediante atributos quasi-identificadores, NO estamos ante una anonimización válida

Directrices 1/2025 sobre seudonomización: más sombras que luces

Las Directrices 1/2025 del EDPB actualizan la implementación de la seudonimización bajo el RGPD, pero carecen de alineación con la última doctrina del TJUE.

Existen dos problemas significativos con estas directrices

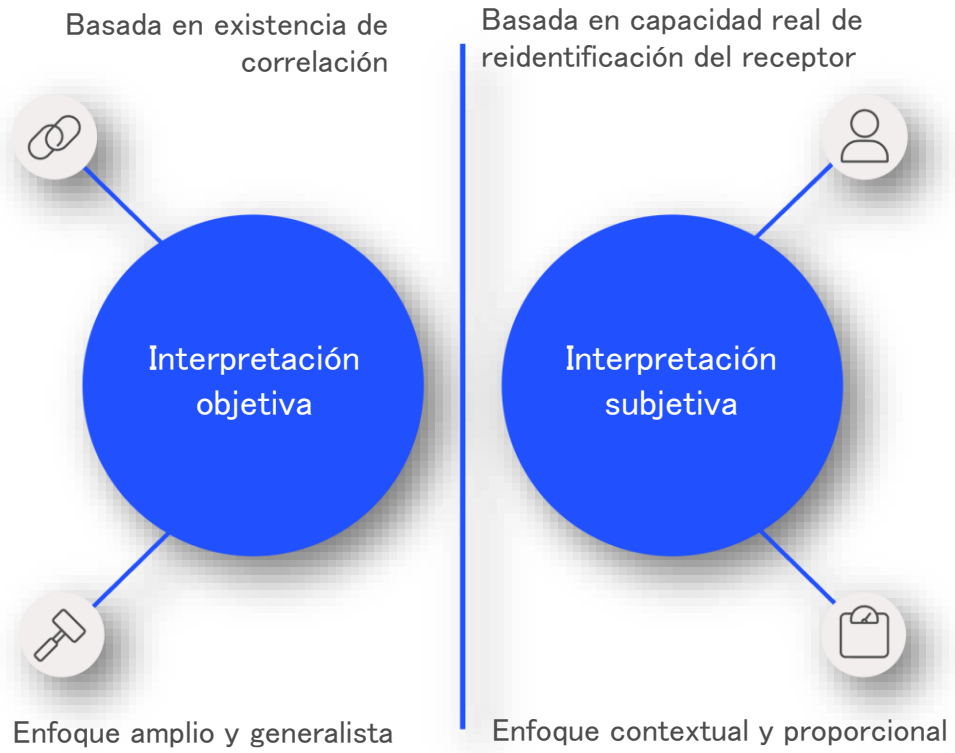
Ignora la jurisprudencia del TJUE sobre la interpretación subjetiva de los datos seudonimizados(Doctrina Scania)

No abordan la valoración de tratamientos **desde el punto de vista de terceros que reciben o acceden** a datasets seudonimizados.

Interpretación objetiva vs. subjetiva del dato seudonimizado

La interpretación objetiva (mayoritaria hasta 2023) sostenía que los datos seudonimizados son personales si existe información adicional en alguna parte para reidentificarlos, aunque el tercero no la tenga.

La interpretación subjetiva del TJUE reconoce que un mismo dato seudonimizado puede ser personal para el la entidad que dispone de las tablas de correlación pero no para el receptor, ya que **dependerá de la capacidad real de reidentificación** de cada parte.



Doctrina del TJUE Sentencia Scania (2023)

En la **sentencia Scania**, el **TJUE** estableció que el **número de bastidor (VIN)** solo es **dato personal** para las entidades que **pueden vincularlo con una persona física** (por ejemplo, el propietario o conductor del vehículo).

Para **otras entidades** (como talleres o agentes independientes) que solo acceden al VIN para fines técnicos y **no pueden identificar al titular**, **no tiene carácter de dato personal**.

El **TJUE** reitera que la definición de dato personal se aplica cuando, por su **contenido, finalidad o efectos**, la información se relaciona con una persona física **teniendo en cuenta los medios razonablemente disponibles** para identificarla.

El **VIN**, en sí mismo, **no es personal**, pero **adquiere ese carácter** cuando alguien dispone de medios razonables para **vincularlo con el propietario o usuario del vehículo.**

Doctrina del TJUE Sentencia IAB Europe (2024)

El **"TC String"** era una cadena de texto generada por plataformas de gestión del consentimiento cuando un usuario acepta o rechaza cookies

El marco que regula este sistema fue creado por **IAB Europe**

IAB Europe alegaba no poder identificar a los usuarios.

El **TJUE** recuerda que **no es necesario que toda la información identificativa esté en manos de una sola entidad**; puede estar repartida entre varios actores y seguir siendo dato personal.

En este caso, aunque IAB no pueda por sí misma combinar el **TC String** con una IP o acceder directamente a los datos de los usuarios, **sí puede solicitar información adicional a sus miembros para identificar a los usuarios**

Por tanto, el **TC String es un dato personal también para IAB Europe**, porque el marco jurídico que diseñó le otorga **posibilidad razonable de identificación indirecta** a través de la información de sus miembros.

Doctrina del TJUE Sentencia SRB–EDPS (2025)

1. La Junta única de resolución del Banco Popular (SRB) encarga a Deloitte un informe sobre comentarios de afectados (accionistas y acreedores del Popular). **Entrega lista con códigos alfanuméricos pero sin tabla de correlación.**

2. Cinco denuncias ante la EDPS alegando que la Junta incumplió su obligación de transparencia al **no mencionar a Deloitte como destinatario de datos.**

3. EDPS sanciona al SRB por transmitir comentarios a Deloitte sin informar debidamente. Infracción del artículo 15.1.d del Reglamento 2018/1725.

4. **TJUE concluye que si Deloitte no puede reidentificar con sus medios, el dataset no es personal para Deloitte**, si bien ello **no exime de cumplir la obligación de información** a los interesados

Criterios de evaluación contextual / test de reidentificabilidad

1 Evaluación Subjetiva

La valoración de identificabilidad debe realizarse desde la **perspectiva de cada parte implicada**, determinando si para esa parte específica se trata de datos personales o no.

2 Medios Razonables

Deben considerarse los **recursos técnicos, jurídicos y prácticos** de que dispone cada parte para identificar a la persona, y la posibilidad razonable de recurrir a terceros.

3 Proporcionalidad

El riesgo de reidentificación debe aparecer como **insignificante** para considerar los datos como no personales. Se evalúan costes, tiempo y tecnología disponible.

Carácter "líquido": El estatus de los datos seudonimizados puede variar según el contexto técnico, contractual y desarrollos tecnológicos futuros.

Responsabilidad: El responsable debe evaluar y documentar que el riesgo de reidentificación es insignificante, no eludirlo alegando ilegalidad.

Considerando 26 del RGPD - Fundamento Legal

"Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta **todos los factores objetivos**, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos."

Recomendaciones practices antes de transferir un dataset seudonimizado

Verificación y Documentación Rigurosa

Documentar la imposibilidad de reidentificación por terceros antes de transferir o compartir datos seudonimizados.

Cláusulas Contractuales Claras

Regular el uso de información adicional y establecer mecanismos si cambian las circunstancias técnicas y jurídicas.

Revisión Periódica de Análisis

Adaptar evaluaciones de identificabilidad a avances tecnológicos y cambios en medios disponibles.

Transparencia y Comunicación

Informar a interesados cuando corresponda y ajustar comunicaciones si el estatus de datos cambia.

Seudonimización vs. Anonimización a la hora de entrenar modelos / sistemas de IA

SEUDONIMIZACIÓN

Ventajas

- **Aprendizaje longitudinal:** mantiene trayectorias individuales completas
- **Mayor eficiencia:** requiere menos datos para detectar patrones
- **Precisión individualizada:** predicciones personalizadas
- **Detección de anomalías:** identifica desviaciones específicas

Riesgos

- Facilidad en la reidentificación
- Requiere medidas de seguridad adicionales

ANONIMIZACIÓN

Ventajas

- **Mayor seguridad:** dificultad en la reidentificación directa si la anonimización es robusta
- **Reducción de riesgos:** minimiza exposición de privacidad
- **Cumplimiento simplificado:** fuera del ámbito RGPD si es robusta

Limitaciones

- Pérdida de relaciones individuales y/o continuidad temporal
- Requiere volúmenes masivos de datos para compensar
- Predicciones solo a nivel poblacional, no individual

La capacidad de Reidentificación de los Sistemas de IA

- Los modelos de IA tienen una **capacidad sorprendente para reconstruir o inferir identidades**, no porque estén diseñados intencionalmente para hacerlo, sino por la propia naturaleza de cómo aprenden a detectar patrones y relaciones en los datos.
- El aprendizaje automático **construye un mapa complejo de conexiones** entre diferentes características, buscando las reglas ocultas que pueden actuar como identificadores únicos.

Unicidad de los Datos Personales

Con solo 3-4 puntos de datos aparentemente inocuos (como fechas de visitas a lugares específicos), se puede identificar de manera única al **95% de las personas** en una base de datos.

Huellas Digitales Conductuales

Nuestras rutinas diarias, combinaciones de preferencias y horarios de actividades crean **patrones únicos** tan distintivos como huellas dactilares físicas.

Correlaciones Profundas

Los modelos detectan **correlaciones sutiles** que serían invisibles para cualquier análisis humano, permitiendo inferir información sensible.

Memorización No Intencionada

Los modelos generativos pueden "memorizar" fragmentos de información que quedan profundamente grabados en sus parámetros, pudiendo **reproducirlos textualmente**.

Mecanismos de Ataques

Ataques de Vinculación

Método: Cruce con bases de datos públicas, redes sociales o registros abiertos.

Ejemplo Dataset:

- Edad: 34 años
- Género: Mujer
- Formación: Máster en IA
- Experiencia: 8 años tech
- Madrid

→ **Combinación única de quasi-identificadores**

Inferencia de Atributos

Método: El modelo de IA aprende correlaciones y deduce información sensible eliminada.

Patrón del Modelo:

```
IF edad > 45 AND
gaps_laborales > 2 AND
sector = "tech"
THEN prob_género_fem = 0.82
```

→ **Sesgo histórico revela datos ocultos**

Inversión de Modelos

Método: Los modelos "memorizan" características del training set.

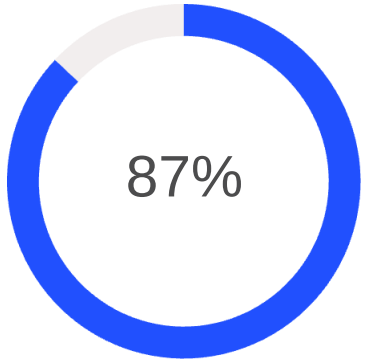
Proceso:

1. Acceso al modelo (API)
2. Consultas estratégicas
3. Observación de predicciones
4. Reconstrucción de datos

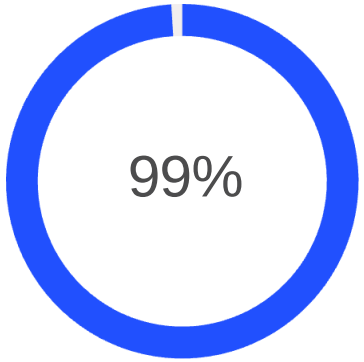
→ **Extracción de training data**

Factores que agravan el riesgo de Re-identificación utilizando IA

- Capacidad de procesamiento masivo
- Deep Learning procesa millones de atributos simultáneamente
- Encuentra correlaciones indetectables por análisis humano
- Cantidades enormes de datos en RRSS
- Bases públicas y data brokers
- Web scraping automatizado



Población identificable con 3 atributos básicos



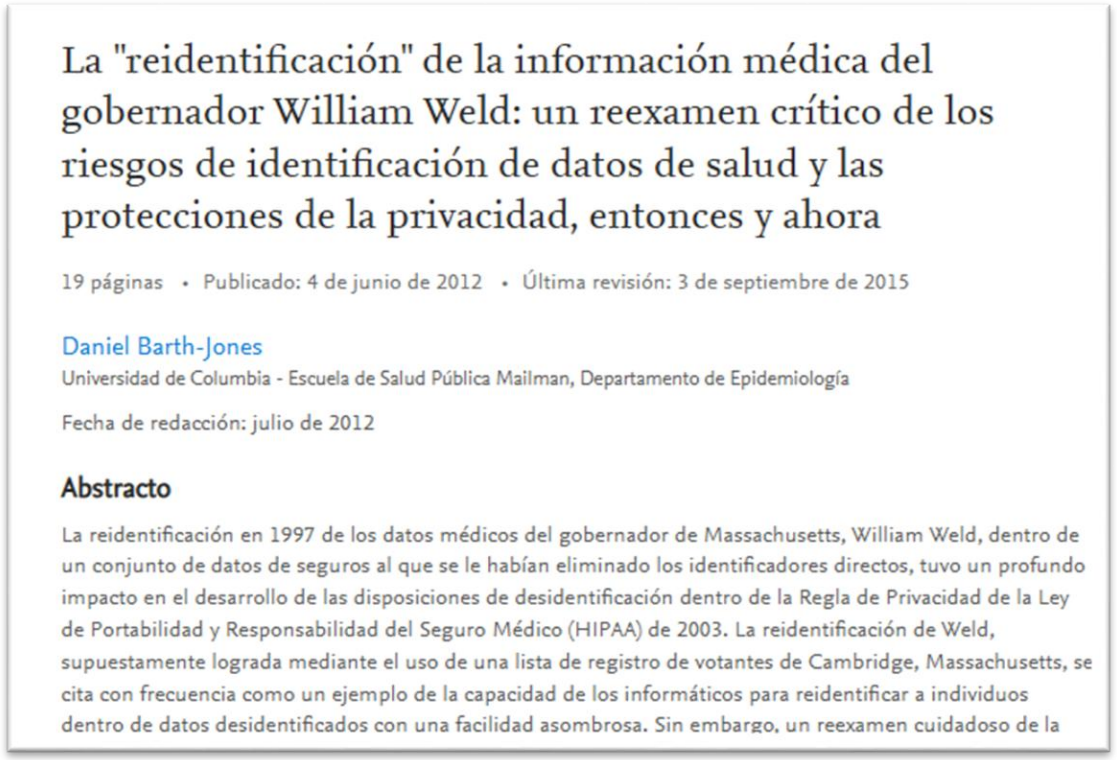
Re-identificación con 8 datos de comportamiento

Casos reales documentados de reidentificación

Censo Massachusetts (Latanya Sweeney) 1997

- Conjunto de datos de registros médicos del estado de Massachusetts depurado de identificadores directos
- Cruce con Registro electoral público de la ciudad de Cambridge con solo 3 atributos indirectos (fecha nacimiento, CP, y sexo)
- Se identifico al gobernador William Weld en el data set

Influyó en la modificación de HIPAA incoporando el metodo de desidentificación Safe Harbor



La "reidentificación" de la información médica del gobernador William Weld: un reexamen crítico de los riesgos de identificación de datos de salud y las protecciones de la privacidad, entonces y ahora

19 páginas • Publicado: 4 de junio de 2012 • Última revisión: 3 de septiembre de 2015

Daniel Barth-Jones
Universidad de Columbia - Escuela de Salud Pública Mailman, Departamento de Epidemiología

Fecha de redacción: julio de 2012

Abstracto

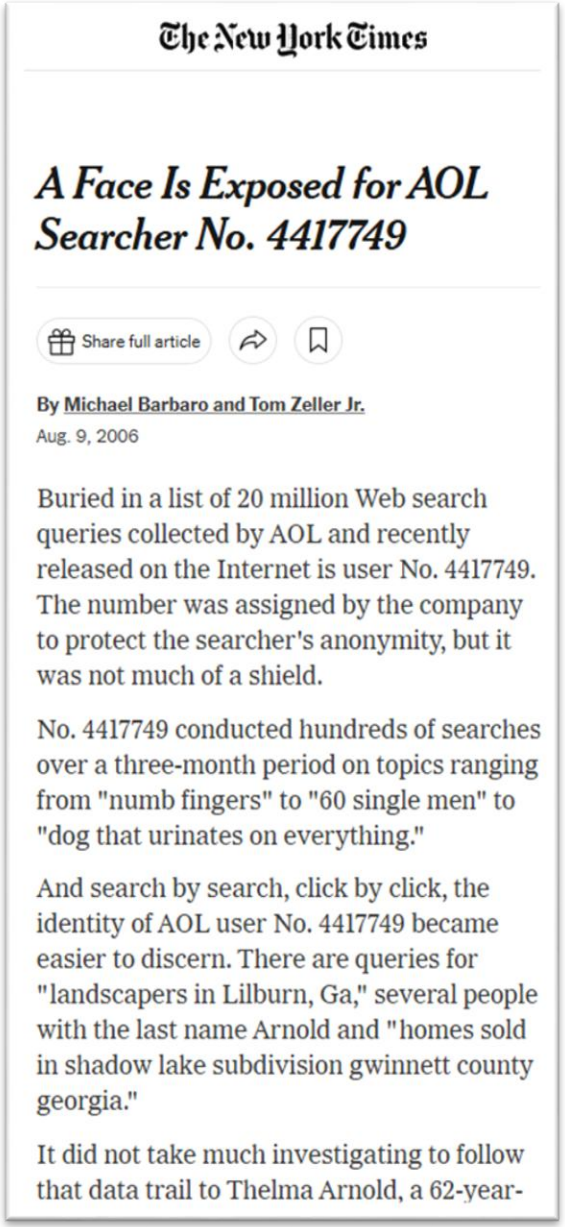
La reidentificación en 1997 de los datos médicos del gobernador de Massachusetts, William Weld, dentro de un conjunto de datos de seguros al que se le habían eliminado los identificadores directos, tuvo un profundo impacto en el desarrollo de las disposiciones de desidentificación dentro de la Regla de Privacidad de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) de 2003. La reidentificación de Weld, supuestamente lograda mediante el uso de una lista de registro de votantes de Cambridge, Massachusetts, se cita con frecuencia como un ejemplo de la capacidad de los informáticos para reidentificar a individuos dentro de datos desidentificados con una facilidad asombrosa. Sin embargo, un reexamen cuidadoso de la

Casos reales documentados de reidentificación

AOL Search Data — 2006

- En 2006. AOL publicó un conjunto de datos con unas 20 millones de busquedas sobre personas , negocios, salud etc. **realizadas por más de 650.000 usuarios**, con el supuesto objetivo de facilitar la investigación académica.
- Aunque los nombres se sustituyeron por identificadores numéricos, la identificación se logró **cruzando las búsquedas con información contextual** que la propia usuaria había introducido en el buscador.
- New York Times identificó "Usuario 4417749" como **Thelma Arnold**

Consecuencia: CTO de AOL dimitió, demandas colectivas presentadas



The New York Times

A Face Is Exposed for AOL Searcher No. 4417749

Share full article

By Michael Barbaro and Tom Zeller Jr.
Aug. 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga," several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

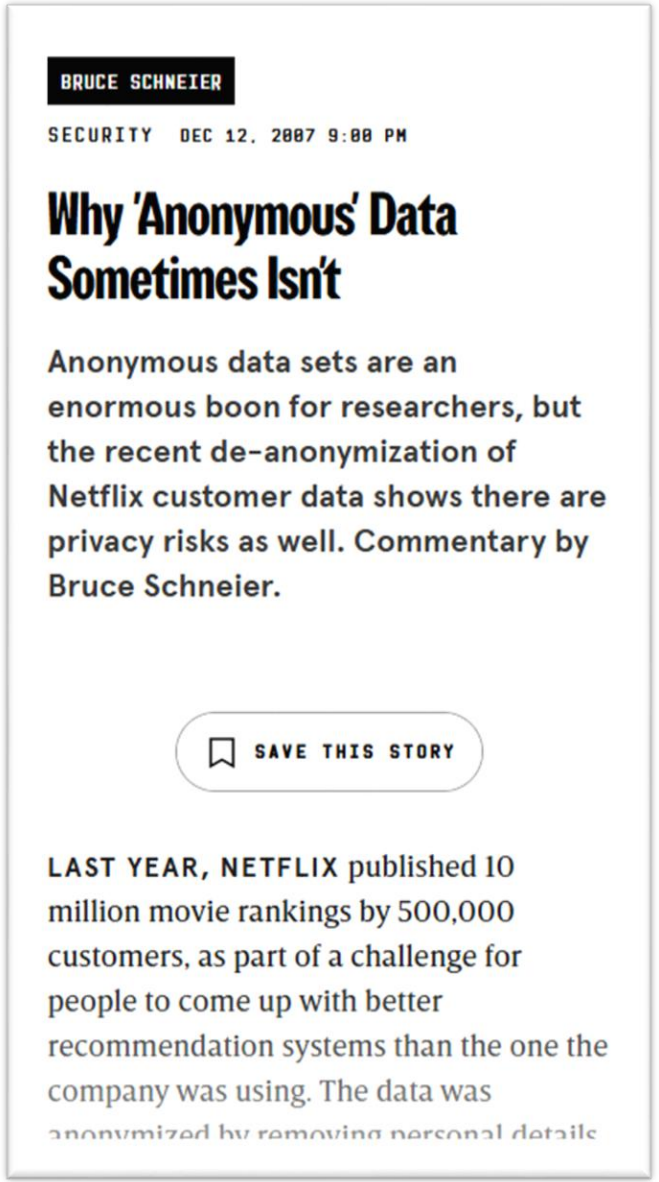
It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-

Casos reales documentados de reidentificación

Netflix Prize 2008

- Netflix publicó un conjunto de datos con millones de valoraciones de películas hechas por unos 500.000 usuarios, para promover la investigación en algoritmos de recomendación. Los datos estaban **seudonimizados** (los identificadores directos (nombre, usuario) fueron reemplazados por números aleatorios, pero incluían **fechas y puntuaciones precisas**.
- **Técnica:** Cruce con con **opiniones públicas en** IMDb (fechas + valoraciones)
- **Resultado:** Al coincidir varias puntuaciones y tiempos, **dedujeron la identidad de usuarios de Netflix (entre 80 y 99 % de los usuarios cuyas valoraciones estaban presentes en IMDb)**, revelando incluso sus gustos o preferencias personales (por ejemplo, películas con contenido sexual o político).

I trabajo demostró que **incluso con datos seudonimizados y parcialmente modificados**, era posible vincular perfiles personales con un altísimo grado de certeza.



BRUCE SCHNEIER

SECURITY DEC 12, 2007 9:00 PM

Why 'Anonymous' Data Sometimes Isn't

Anonymous data sets are an enormous boon for researchers, but the recent de-anonymization of Netflix customer data shows there are privacy risks as well. Commentary by Bruce Schneier.

SAVE THIS STORY

LAST YEAR, NETFLIX published 10 million movie rankings by 500,000 customers, as part of a challenge for people to come up with better recommendation systems than the one the company was using. The data was anonymized by removing personal details

Conclusiones

1. **Frontera difusa entre datos seudonimizados y anonimizados**
   La IA actual puede correlacionar atributos indirectos o quasi-identificadores, difuminando los límites técnicos tradicionales.

2. **Reducción de barreras a la reidentificación**
   Los sistemas de IA existentes reducen drásticamente las barreras prácticas para la reidentificación de personas.

3. **Reconstrucción de identidades sin claves de correlación**
   Los sistemas de IA pueden reconstruir identidades mediante inferencias estadísticas o patrones de comportamiento, incluso sin acceso directo a claves de correlación en el caso de datos seudonimizados.

4. **Datos seudonimizados bajo el RGPD**
   Los conjuntos seudonimizados deben considerarse datos personales mientras exista una probabilidad razonable de reidentificación mediante medios tecnológicos disponibles (lo cuál siempre ocurrirá si se utilizan para el entrenamiento de modelos o sistemas de IA).

5. **Anonimización robusta con enfoques combinados**
   Se requieren técnicas avanzadas: ruido diferencial, agregación dinámica, k-anonimización y otras medidas a la par de la capacidad de reidentificación de la IA.

6. **Evaluación de reidentificabilidad residual**
   No basta con eliminar identificadores directos: es necesario integrar la evaluación de reidentificabilidad residual en cada fase del ciclo de vida del modelo o sistema de IA.

7. **Transparencia y revisión continua**
   Transparencia, documentación y revisión continua del riesgo deben ser requisitos previos al uso de cualquier dataset seudonimizado o desidentificado, e incluso cuando se haya anonimizado.

Organiza

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Foro GRC
Privacidad · IA · Ciberseguridad

Insight Foro GRC

Datos seudonimizados y su impacto en Inteligencia Artificial

Mesa debate: Caso de uso IA – Intervención de equipos de cumplimiento (DPD, CISO, Equipos IA)

Taller práctico: Categorización de casos de uso según RIA.

Miércoles 22 octubre - 16:00 - streaming

Partners Estratégicos

Telefónica Tech

GOOERTIS
Part of Telefónica Tech

CANAL AEC

"Categorización de casos de uso según el RIA"

Marta A. de Luis Diez

GRC Senior Consultant, Govertis part of Telefónica Tech

Marta de Luis Diez | LinkedIn

@ m.deluis@govertis.com

Organiza:

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Partners Estratégicos:

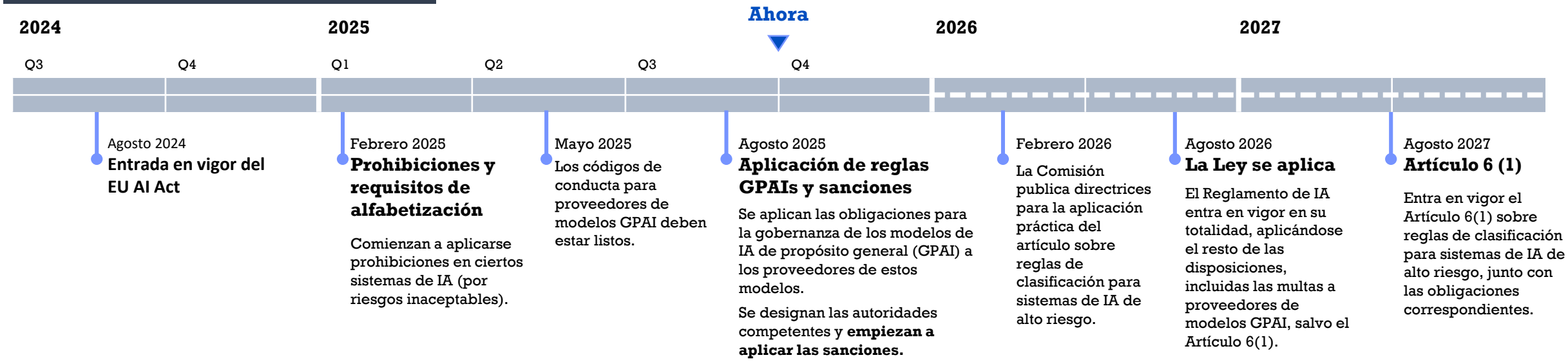
GOVERTIS
Part of Telefónica Tech

Telefónica Tech

Cronograma de aplicación del RIA

El Reglamento de IA de la UE (RIA/ IA Act) es la primera norma integral que regula cómo se desarrollan, comercializan y usan los sistemas de IA en Europa, con obligaciones que dependen del riesgo y del rol en la cadena

Calendario de aplicación de la Ley



Panorama del RIA: lo esencial

Un marco único: extraterritorial, basado en riesgo y con sanciones relevantes

APLICACIÓN AMPLIA Y EXTRATERRITORIAL

Afecta a cualquier sistema de IA **utilizado o comercializado en el mercado de la UE**, sin importar **dónde se hayan desarrollado.**

ENFOQUE BASADO EN RIESGO

Categoriza los **sistemas de IA** por **nivel de riesgo** (prohibidos, alto, transparencia reforzada y mínimo). Riesgos más altos conducen a requisitos y obligaciones más estrictas.

RESPONSABILIDADES DIFERENCIADAS

Las **obligaciones** varían dependiendo de tu rol en la cadena de la IA, se distingue entre: proveedores, responsables de despliegue, representantes autorizados, distribuidores e importadores.

SANCIONES SEVERAS

El **incumplimiento** del Reglamento puede dar lugar a **sanciones** de hasta 35 millones de euros o el 7% de la facturación global, **dependiendo de la gravedad**.

IMPLEMENTACIÓN GRADUAL

En **vigor desde agosto 2024.** Aplicación escalonada con requisitos aplicables en fases: desde los 6 hasta los 24 meses, según el nivel de riesgo del sistema.

IMPORTANCIA E IMPACTO

La IA sin control puede poner en riesgo la seguridad, los **derechos fundamentales** y la confianza social. Esta ley busca garantizar un uso seguro, ético y centrado en el ser humano.

¿Está tu organización lista para cumplir con el AI Act?

Ruta de categorización en 8 pasos

Del marco del RIA a decisiones operativas: cómo categorizar un caso de uso

- PASO 1: ¿Es un sistema de IA? (art. 3.1)
- PASO 2: ¿Queda fuera por exclusiones? (art. 2)
- PASO 3: ¿Qué rol tiene mi organización en este caso?
- PASO 4: Descarta prácticas prohibidas (art. 5)
- PASO 5: ¿Es alto riesgo por integración de un producto regulado? (art. 6.1. + Anexo I)
- PASO 6: ¿Es alto riesgo por área de uso? (art. 6.2 + Anexo III)
- PASO 7: ¿Transparencia reforzada? (art. 50)
- PASO 8: Obligaciones por rol (Según resultado anterior)

Ruta de categorización en 8 pasos

PASO 1 — ¿Qué es un “sistema de IA” (art. 3.1) y por qué es el filtro inicial?

SISTEMA DE IA

Un **sistema de IA** es en sistema basado en máquinas que está diseñado para **funcionar con diversos niveles de autonomía** y que puede mostrar **capacidad de adaptación** tras su despliegue, y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo **generar salidas** tales como predicciones, contenidos, recomendaciones o decisiones que pueden **influir en entornos** físicos o virtuales.

MODELO GPAI

Un **modelo de IA de propósito general** es un modelo entrenado, habitualmente con grandes volúmenes de datos y técnicas como la autosupervisión a escala, que demuestra una **capacidad significativa para desempeñar con competencia una amplia gama de tareas**. Por ello, estos modelos pueden ser reutilizados en múltiples aplicaciones o sistemas de IA distintos.

En el marco del RIA, el foco regulatorio recae sobre **el sistema de IA** en su conjunto, no sobre los modelos individuales que lo conforman. Es el Sistema de IA el que genera impacto real y **debe ser evaluado y supervisado**.

Ruta de categorización en 8 pasos

PASO 2 — ¿Cuándo NO aplica el RIA? Exclusiones (art. 2)

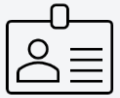
Ruta de categorización en 8 pasos

PASO 3 — Rol de la organización

PROVEEDOR	RESPONSABLE DEL DESPLIEGUE	IMPORTADOR	DISTRIBUIDOR	REPRESENTANTE AUTORIZADO
Desarrolla un sistema de IA y lo introduce en el mercado o lo pone en servicio en la UE	Utiliza un sistema de IA en el marco de una actividad profesional	Introduce en la UE un sistema de IA de una empresa establecida en un tercer país	Comercializa un sistema de IA en la UE	Recibe un mandato del proveedor para cumplir y gestionar en su nombre las obligaciones

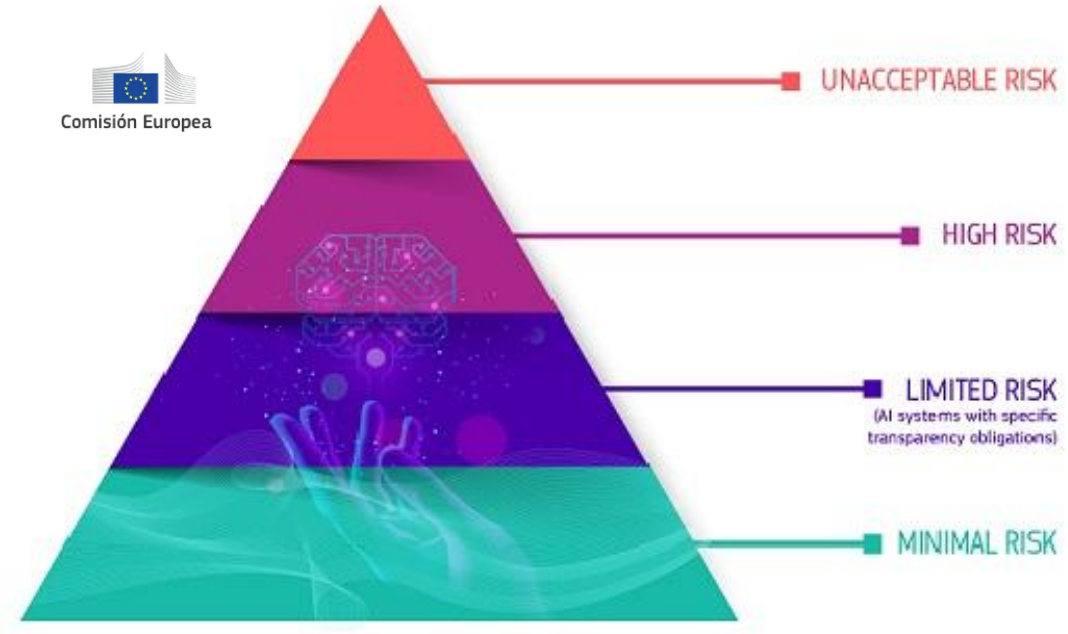




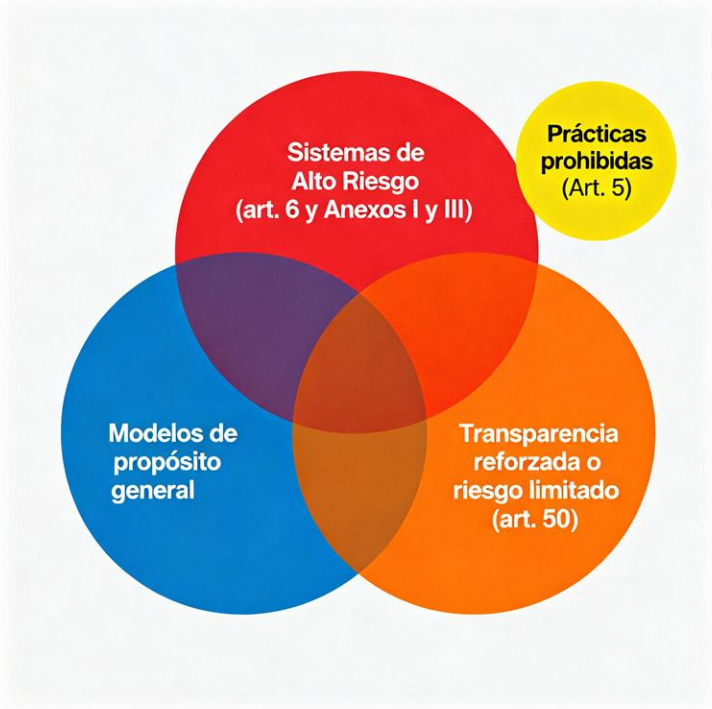


Ruta de categorización en 8 pasos

Pasos 4-7 — Cuidado con el “mito” de los 4 niveles



AI risk-based approach



Ruta de categorización en 8 pasos

Paso 8 — ¿Dónde puedo consultar qué obligaciones me aplican?

Prácticas prohibidas	Sistema de Alto Riesgo	Transparencia reforzada	Modelos de propósito general
Si es PROHIBIDO → Art. 5 	**Si es ALTO RIESGO → Art. 6 + Anexos I/III** **Qué debe cumplir el sistema**: Arts. 8–15 **Según rol:** Arts. 16–27 **Antes de lanzar**: Arts. 43-49 **Después de lanzar**: Arts. 72-73	**Si aplica TRANSPARENCIA → Art. 50** **Proveedor**: 50. 1 y 2 **Responsable del despliegue**: 50. 3 y 4	**Si hay GPAI** → Arts. 53–55 Específicas para el proveedor del modelo.

Ejemplo de caso de uso

Concesión de crédito al consumo online. Somos una fintech que concede **crédito al consumo online** y utilizamos un **SaaS de un tercero** (proveedor). El usuario **interactúa con un asistente/IA** durante la solicitud y, al final, el sistema **genera vídeos explicativos automatizados** (contenido sintético) sobre las condiciones del crédito, tomando una decisión sobre la solvencia crediticia en base a una elaboración de perfiles. **No reentrenamos** el modelo ni cambiamos su **finalidad**; solo **configuramos umbrales y reglas de negocio** y seguimos las **instrucciones del proveedor**.

CATEGORIZACIÓN DE CASO DE USO SEGÚN EL RIA	
Paso 1 ¿Es sistema de IA (art. 3.1)?	Si. infiere riesgo y genera recomendaciones/decisiones de crédito.
Paso 2 ¿Exclusiones (art. 2)?	No (uso profesional en la UE; no es defensa, ni I+D, ni doméstico).
Paso 3 Rol de la organización	Responsable del despliegue (uso conforme del SaaS).
Paso 4 Prácticas prohibidas (art. 5)	Ninguna práctica prohibida.
Paso 5-6 ¿Alto riesgo? (art. 6.1/6.2 + Anexos)	No Anexo I, pero si Anexo III "acceso a servicios esenciales" (Evaluar solvencia / calificación crediticia)
Paso 7 Transparencia reforzada (art. 50)	Interacción con IA y contenido sintético (obligaciones del proveedor)
Resultado	Sistema de Alto Riesgo (art. 6.2 y Anexo III) y Responsable del despliegue
Paso 8 Obligaciones	Art. 26: Obligaciones de los implantadores de sistemas de IA de alto riesgo Art. 27: Evaluación de impacto sobre los derechos fundamentales de los sistemas de IA de alto riesgo

Verificador del cumplimiento de la Ley de IA de la UE - Future of Life Institute (FLI)

MUCHAS GRACIAS