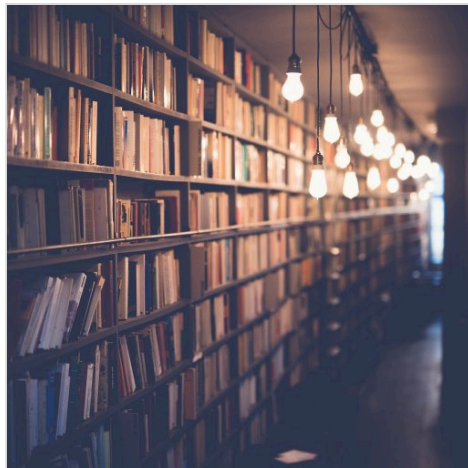


L U M B R E



Anonimización y seudonimización

Materia: Privacidad y Seguridad de Datos · Responsabilidad Profesional

11/10/2026

Antes de empezar

Antes de publicar o analizar datos personales hay que desvincularlos de las personas. La seudonimización reduce el riesgo conservando utilidad; la anonimización pretende eliminarlo, pero la reidentificación recuerda que es difícil.

QUÉ APRENDERÁS

- Aplicar técnicas de seudonimización y anonimización para reducir la identificabilidad de los datos, entendiendo sus límites frente a la reidentificación.

Anonimización y seudonimización

Anónimo no significa irrencontrable

Quitar el nombre no basta para anonimizar. Con suficientes detalles, alguien puede volver a saber quién eres cruzando los datos. Seudonimizar y anonimizar son herramientas valiosas, no promesas de invisibilidad.

VIDEO

Técnicas de anonimización de datos

Un repaso a los métodos para desvincular los datos de las personas y cuánto protegen de verdad frente a la reidentificación.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=cG68mtLg0KA>

Identificadores directos e indirectos

- Directos: nombre, DNI, teléfono: delatan al instante.
- Indirectos: código postal, fecha de nacimiento, género: juntos pueden identificar.
- El peligro está en la combinación de los indirectos.

Seudonimización

Sustituir identificadores por seudónimos reversibles con una clave aparte. Reduce el riesgo pero sigue siendo dato personal, porque se puede revertir.

Anonimización

Transformar los datos de modo que la persona ya no sea identificable, razonablemente. Es irreversible y, de lograrse de verdad, saca el dato del ámbito de la protección personal.

Supresión de cuasi-identificadores

- Borrar o generalizar campos que ayudan a identificar.
- Generalizar: convertir edades exactas en rangos.
- Reduce la especificidad que permite reidentificar.

k-anonimato

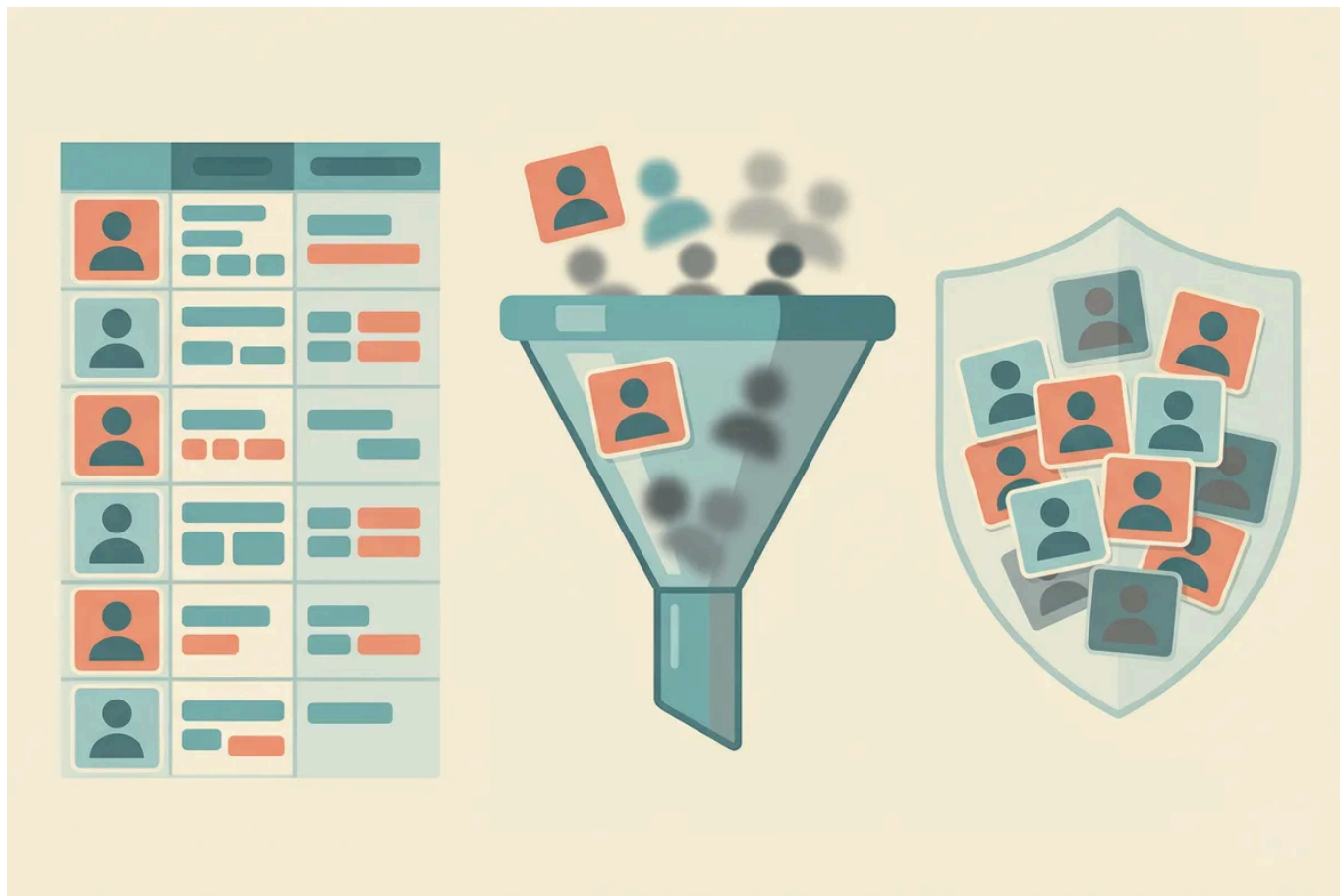
Garantiza que cada registro sea indistinguible dentro de al menos k registros respecto a los cuasi-identificadores. Nadie queda solo en un grupo pequeño y reconocible.

r-diversidad y más allá

- El k-anonimato solo protege la identidad, no atributos sensibles.
- La l-diversidad exige variedad de valores sensibles en cada grupo.
- Hay medidas de cercanía que evitan grupos homogéneos.

Ruido diferencialmente privado

La privacidad diferencial añade ruido calibrado a consultas o datos, dando una garantía matemática: la presencia de uno apenas cambia el resultado. Es el estándar más sólido.



Quitar el nombre no basta: anonimizar es generalizar y agrupar hasta que nadie quede solo y reconocible.

El riesgo de reidentificación

- Cruzar datos «anónimos» con otras fuentes disponibles.
- Casos famosos reidentificaron a partir de datos liberados.
- La anonimización debe evaluarse contra ataques plausibles.

Utilidad frente a privacidad

Cuanto más se protege, menos detallado y útil queda el dato. Encontrar el punto justo depende del riesgo y del uso previsto.

Qué no es anonimizar

- Solo quitar el nombre o cifrar de forma reversible no anonimiza.
- Si una clave permite revertir, sigue siendo identificable.
- Confundir ocultar con anonimizar es un error caro.

Errores frecuentes

- Borrar el nombre y el DNI y dar el conjunto por anonimizado.

- Confundir seudonimización con anonimización cuando la clave sigue disponible.
- Publicar datos «anónimos» sin evaluar ataques de reidentificación cruzada.

Ejemplo resuelto: una fuga de datos «anónimos» de movilidad

Una ciudad libera registros de viajes sin nombres pero con fecha, hora y coordenadas precisas. Un investigador cruza esos datos con publicaciones en redes y vuelve a identificar a varios usuarios. El equipo corrige generalizando hora y zona y aplicando k-anonimato antes de republicar.

1. inventariar identificadores directos e indirectos del conjunto
2. generalizar o suprimir los campos que delatan
3. aplicar k-anonimato o ruido de privacidad diferencial
4. medir el riesgo de reidentificación con ataques plausibles
5. publicar solo si el riesgo residual es aceptable

¿Para qué sirve en la realidad?

Publicar datasets abiertos, entrenar modelos con datos sensibles o compartir información entre organizaciones exige desvincular el dato de la persona: la anonimización bien hecha protege la privacidad sin matar la utilidad, y su ausencia acaba en multas y escándalos de reidentificación.

1. La seudonimización se distingue de la anonimización porque:

- ☐ es irreversible
- ☐ mantiene la posibilidad de reidentificar con una clave separada
- ☐ elimina por completo el riesgo
- ☐ no afecta a los identificadores directos

2. Quitar únicamente el nombre de un conjunto de datos garantiza su anonimización completa.

- ☐ Verdadero
- ☐ Falso

ACTIVIDAD INTERACTIVA DISPONIBLE EN LUMBRE

3. Anonimizar



4. Ordena una publicación responsable de datos:

Elementos:

- identificar cuasi-identificadores y sensibles
- aplicar generalización o ruido
- medir riesgo de reidentificación
- liberar si el riesgo es aceptable

Clasificar	. . .
Transformar	. . .
Evaluar	. . .
Publicar	. . .

Privacidad diferencial https://en.wikipedia.org/wiki/Differential_privacy Marco con garantía formal de que un individuo apenas influye en el resultado.

5. Une cada técnica de protección del dato con su idea:

5.	seudonimización	-----
5.	generalización	-----
5.	k-anonimato	-----
5.	privacidad diferencial	-----

Opciones: sustituir identificadores de forma reversible · reducir el detalle de un cuasi-identificador · cada registro mezclado con k-1 similares · añadir ruido con garantía matemática

Anonimizar

Anonimización y seudonimización

Identificadores

directos

indirectos

cuasi-identificadores

Técnicas

supresión

generalización

k-anonimato

ruido diferencial

Riesgos

reidentificación

cruce de fuentes
grupos pequeños
Equilibrio
utilidad
privacidad
riesgo aceptable

El mapa mental interactivo es interactivo en la versión online.



k-anonimato <https://en.wikipedia.org/wiki/K-anonymity> Cada registro indistinguible dentro de al menos k respecto a los cuasi-identificadores.

6. Vas a publicar datos de movilidad «anonimizados». ¿Qué ataque de reidentificación temerías y qué técnica (k-anonimato, ruido) priorizarías?

Referencia curricular

Materia:

Privacidad y Seguridad de Datos · Responsabilidad Profesional

Versión interactiva completa (con actividades, videos y autoevaluación):



<https://univ.lumbre.lat/object/cdia-priv-002-anonimizacion-y-seudonimizacion>

Material educativo generado desde Lumbre · lumbre.lat