

**Webinar**

# SEUDONIMIZACIÓN EFICAZ

**DIRECTRICES DE LA COMISIÓN EUROPEA DE  
PROTECCIÓN DE DATOS**

Reduce riesgos de identificación y facilita el cumplimiento normativo.



**22 de mayo de 2025**

# SEUDONIMIZACIÓN EFICAZ

## DIRECTRICES DE LA COMISIÓN EUROPEA DE PROTECCIÓN DE DATOS

Bienvenida:



**Estrella Freire**

Secretaria General Cámaras  
Andalucía

Expone:



**Paola Codón**

Abogada especializada  
en protección de datos.

# SEUDONIMIZACIÓN EFICAZ

DIRECTRICES DE LA COMISIÓN EUROPEA DE  
PROTECCIÓN DE DATOS

Aplicaciones,  
desafíos y mejores  
prácticas

# ¿QUÉ ES LA PROTECCIÓN DE DATOS?

La protección de datos de las personas físicas es un derecho fundamental, en virtud del cual se reconoce al titular de esos datos la facultad de tener el control de sus datos personales, disponer y decidir sobre los mismos.



# LEGISLACIÓN

**Reglamento (UE) 2016/679 (RGPD).**

**Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales (LOPDYGD).**

Esta legislación afecta: a las empresas y organizaciones que tratan datos personales y a los interesados cuyos datos se tratan.

No afecta, a las empresas como entidad jurídica.

# CONCEPTOS BÁSICOS

Cualquier actividad en la que estén presentes datos de carácter personal constituirá un tratamiento de datos, ya se realice de manera manual o automatizada, total o parcialmente, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción

## TRATAMIENTO

# DATOS PERSONALES

## DATO PERSONAL

Toda información sobre una persona física que la identifique o permita identificarla (numérica, gráfica, fotográfica, acústica o de cualquier otro tipo)

Los datos personales se pueden agrupar por categorías en función del tipo de datos que tratemos:

- Datos económicos: cuenta corriente.

- Datos profesionales: profesión, sitios donde se ha trabajado.

- Datos de localización: calle, dirección, teléfono

- Datos de identificación: nombre, apellido, mote. Etc



- Organismo europeo independiente.
- Reúne a las autoridades nacionales de protección de datos (Autoridades Nacionales de Supervisión) de los países del Espacio Económico Europeo, así como al Supervisor Europeo de Protección de Datos (SEPD).
- Vela por que el RGPD se aplique de manera coherente y garantice la cooperación, también en materia de aplicación de la ley.

## COMITÉ EUROPEO DE PROTECCION DE DATOS (CEPD)

# Objetivo de las Directrices 01/2025

- 1.-Aclarar el concepto de seudonimi-zación, diferenciándolo de otros mecanismos.
- 2.-Proporcionar recomendaciones prácticas (ejemplos de medidas técnicas/ organizativas que permiten alcanzar un nivel adecuado de protección)
- 3.- Identificar beneficios y limitaciones
- 4.- Orientaciones sobre cómo integrar la seudonimización en el diseño de sistemas de tratamiento de datos, haciendo énfasis en la necesidad de evaluaciones continuas de su eficacia (Protección desde el diseño y por defecto).



# ¿Qué es la seudonimización?

- Definición del RGPD (Art. 4.5)

- Proceso para tratar datos personales de manera que no se puedan atribuir a una persona sin información adicional

# Objetivos y ventajas de la seudonimización

- 1.- Reduce los riesgos para los titulares de los datos al tiempo que permite el análisis general.
- 2.- Permite mantener el deber de confidencialidad:  
Previene la divulgación de identificadores directos.
- 3.- En caso de brechas de seguridad, ante la divulgación o acceso no autorizado a datos que han sido seudonimizados de manera efectiva, la seudonimización puede reducir la gravedad del impacto.
- 4.- La efectividad de la implementación de la seudonimización facilita el cumplimiento del RGPD, en particular los principios de protección de datos (artículo 5 RGPD), la protección de datos desde el diseño y por defecto (artículo 25 RGPD) y la seguridad del tratamiento (artículo 32 RGPD)

# Objetivos y ventajas de la seudonimización

- 5.- Facilita que las organizaciones puedan realizar investigaciones y estudios sin exponer la identidad de las personas.
- 6.- En casos donde los datos se comparten entre múltiples partes, la seudonimización actúa como una barrera para evitar la reidentificación.
- 7.- En cuanto a las transferencias internacionales, seudonimizar datos antes de transferirlos a terceros países reduce riesgos de accesos no autorizados.
- 8.- Puede servir como una medida adicional en acuerdos de transferencia de datos para garantizar un nivel adecuado de protección.
- 9.- Mejora la confianza de los interesados al reforzar la percepción de seguridad y compromiso con la privacidad por parte de las organizaciones, mejorando además su reputación en la gestión de datos personales.

En las directrices se resalta que la seudonimización tiene que respetar los principios que rigen en protección de datos:

- 1.- Licitud, lealtad y transparencia.
- 2.- Limitación de la finalidad.
- 3.- Minimización.
- 4.- Exactitud.
- 5.- Limitación del plazo de conservación.
- 6.- Integridad y confidencialidad.
- 7.- Responsabilidad proactiva.



# Anonimización

- Considerando 26 RGPD

- Conjunto de datos que no guarda relación con una persona física identificada o identificable

# DIFERENCIAS

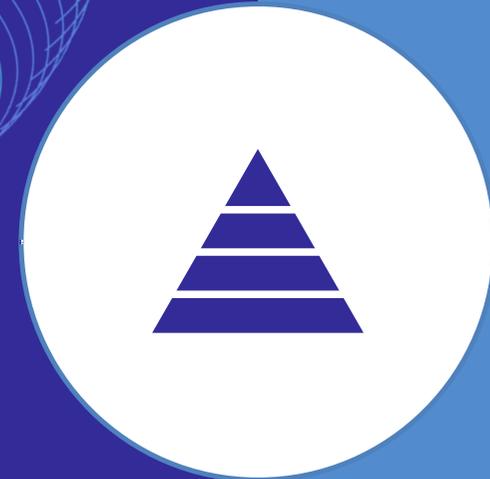
- La anonimización genera un único y nuevo conjunto de datos.
  - No se le aplica el Reglamento General de Protección de Datos

- Seudonimización genera dos nuevos conjuntos de datos: la información seudonimizada y la información adicional que permite revertir la anonimización.
  - Se le aplica el RGPD.

# MEDIDAS TÉCNICAS Y ORGANIZATIVAS

Pueden agruparse en tres grandes bloques:

- 1 – En la transformación seudonimizadora
- 2- Para prevenir la reidentificación indebida
- 3- En la vinculación de datos seudonimizados



# Transformación seudonimizadora

La seudonimización es un proceso que sustituye o elimina identificadores directos, impidiendo la vinculación con los datos originales sin información adicional protegida. Deben almacenarse por separado y estar protegidos con medidas técnicas y organizativas estrictas para evitar accesos no autorizados. Existen dos enfoques principales para llevar a cabo la transformación seudonimizadora: Algoritmos criptográficos. Tablas de búsqueda. \* Los responsables del tratamiento deben evaluar qué atributos modificar, eliminando o sustituyendo identificadores directos y gestionando cuasi-identificadores según el riesgo de reidentificación.



## Ejemplo de seudonimización:

DATOS ORIGINALES	TABLA DE ASOCIACION	DATOS SEUDONIMIZADOS
Nombre: Pedro	Nombre: Pedro – 1aB3e	Nombre: 1aB3e
Apellidos: Pérez	Apellidos: Pérez- 2iF30	Apellidos: 2iF30
Tfno: 111111111	Tfno: 111111- Ac2Ufg	Tfno: Ac2Ufg
Edad: 35	Edad: 35	

# TÉCNICAS BASICAS DE SEUDONIMIZACION

TÉCNICA	GENERADOR DE SEUDONIMOS
Contador	Contador de función monótona que comienza con un determinado valor que se va incrementando cuando se necesita un nuevo seudónimo
Número aleatorio	Valor aleatorio extraído entre un límite mínimo y un límite máximo cuando se necesita un nuevo seudónimo
Función resumen (hash)	Función criptográfica de un solo sentido (no reversible) que transforma los datos personales de entrada en valores de longitud fija
Código de autenticación de mensaje resumido (HMAC)	Función criptográfica de un solo sentido (no reversible) que añade una clave que la hace menos predecible que una función resumen (hash)
Cifrado	Función criptográfica bidireccional (reversible) que transforma los datos personales de entrada en valores que pueden volver a transformarse en su formato original utilizando una clave

# Prevenir la reidentificación indebida

## Medidas técnicas:

- Segmentación de la red.
- Almacenamiento seguro de claves.
- Autenticación segura y sistemas de control de accesos.
- Establecimiento de controles rigurosos y eliminación de copias innecesarias de datos

## Medidas organizativas:

- Contratación de personal capacitado y autorizado para operar los procesos de seudonimización.
- Almacenamiento de los secretos de seudonimización.
- Formación adecuada para empleados que interactúan con interesados y acceden a datos seudonimizados.
- Formalización de acuerdos contractuales cuando intervienen varias entidades.
- Supervisión y auditoría continua de los procesos de seudonimización.



# Vinculación de datos seudonimizados

Cuando **varios responsables vinculan conjuntos de datos seudonimizados.**

**Tres vías principales:**

- 1.- *Intercambio de secretos de seudonimización* (riesgo de accesos no autorizados y filtraciones)
- 2.- Uso de un proveedor de confianza (Depende de la seguridad del proveedor)
- 3.- Seudonimización en dos niveles (mayor seguridad pero también mayor complejidad)

# Prevenir la reidentificación indebida

## Medidas técnicas:

- Segmentación de la red.
- Almacenamiento seguro de claves.
- Autenticación segura y sistemas de control de accesos.
- Establecimiento de controles rigurosos y eliminación de copias innecesarias de datos

## Medidas organizativas:

- Contratación de personal capacitado y autorizado para operar los procesos de seudonimización.
- Almacenamiento de los secretos de seudonimización.
- Formación adecuada para empleados que interactúan con interesados y acceden a datos seudonimizados.
- Formalización de acuerdos contractuales cuando intervienen varias entidades.
- Supervisión y auditoría continua de los procesos de seudonimización.



# EJEMPLOS RECOGIDOS EN EL ANEXO DE LAS DIRECTRICES

## 1.- Minimización de los datos y confidencialidad en los análisis internos.

Empresa que utiliza una app médica.

## 2.- Minimización y limitación.

Empresa con registro de implantes dentales.

## 3.- Protección de identidad y precisión

Laboratorio médico que utiliza pseudónimos en muestras de **pacientes** para evitar errores en la asignación de resultados y proteger la identidad de los pacientes



# Checklist: Seudonimización Eficaz según el CEPD

Lista de verificación práctica basada en las directrices del Comité Europeo de Protección de Datos (CEPD) para implementar una seudonimización eficaz conforme al RGPD:

- ✓ Separación de datos e información adicional
  - ¿La información que permite la identificación directa está separada físicamente o lógicamente?
  - ¿Se almacena esta información en un entorno seguro y diferente?
  - ¿Existen medidas de control de acceso independientes?
- 🔒 Control de acceso
  - ¿Está restringido el acceso a la información adicional sólo al personal autorizado?
  - ¿Se aplican registros de acceso y auditorías periódicas?
  - ¿Existe un protocolo claro para gestionar solicitudes internas de acceso?
- 🔪 Técnicas criptográficas y transformación de datos
  - ¿Se utilizan mecanismos como cifrado, tokenización o hashing adecuado?
  - ¿Se ha evaluado la robustez del algoritmo utilizado?
  - ¿Se cambian periódicamente las claves o seudónimos utilizados?

# Checklist: Seudonimización Eficaz según el CEPD

Lista de verificación práctica basada en las directrices del Comité Europeo de Protección de Datos (CEPD) para implementar una seudonimización eficaz conforme al RGPD:

## Evaluación continua de riesgos

- ¿Se realiza una evaluación periódica del riesgo de reidentificación?
- ¿Se considera el contexto externo (datos disponibles públicamente)?
- ¿La seudonimización sigue siendo eficaz tras cambios en los datos o en la tecnología?

## Buenas prácticas organizativas

- ¿Existe una política interna sobre seudonimización?
- ¿Se proporciona formación continua al personal sobre su uso correcto?
- ¿Se documentan todas las decisiones técnicas y organizativas adoptadas?

¿Preguntas?

# SEUDONIMIZACIÓN EFICAZ

DIRECTRICES DE LA COMISIÓN EUROPEA DE PROTECCIÓN DE DATOS



CÓDICE PRIVADO  
PERSONAS-DATOS-TECNOLOGÍA

¡GRACIAS!



in

[pcodon@codiceprivado.com](mailto:pcodon@codiceprivado.com)

Paola Codón