

Principales tecnologías de mejora de la privacidad




 **Herramientas de ofuscación de datos**


Tecnología	Potencial de aplicación	Retos y limitaciones
Anonimización / seudonimización	Almacenamiento seguro	<ul style="list-style-type: none">● Garantizar que la información no se filtre (riesgo de reidentificación)
Datos sintéticos	Aprendizaje automático con preservación de la privacidad	<ul style="list-style-type: none">● Sesgos amplificados, especialmente en datos sintéticos
Privacidad diferencial	Ampliación de oportunidades de investigación	<ul style="list-style-type: none">● Falta de habilidades y competencias suficientes
Pruebas de conocimiento cero (Zero-knowledge proofs)	Verificación de información sin necesidad de divulgarla (por ejemplo, verificación de edad)	Las aplicaciones aún se encuentran en etapas tempranas




 **Herramientas de procesamiento de datos cifrados**

Tecnología	Potencial de aplicación	Retos y limitaciones
Encriptado homomórfico	<ul style="list-style-type: none">● Cálculos sobre datos cifrados dentro de la misma organización	<ul style="list-style-type: none">● Desafíos en la limpieza de datos
Computación multipartita (incluida la intersección de conjuntos privados)	<ul style="list-style-type: none">● Procesamiento de datos privados demasiado sensibles para divulgar● Rastreo o descubrimiento de contactos	<ul style="list-style-type: none">● Garantizar que la información no se filtre● Costes computacionales más elevados
Entornos de ejecución confiables (Trusted Execution Environments)	Computación con modelos que deben permanecer privados	<ul style="list-style-type: none">● Costes computacionales más elevados● Desafíos en seguridad digital



 **Analítica federada y distribuida**

Tecnología	Potencial de aplicación	Retos y limitaciones
Aprendizaje federado	Aprendizaje automático con preservación de la privacidad	<ul style="list-style-type: none">● Se necesita conectividad confiable
Analítica distribuida		<ul style="list-style-type: none">● La información sobre los modelos de datos debe estar disponible para el procesador de datos



 **Herramientas de responsabilidad de datos**

Tecnología	Potencial de aplicación	Retos y limitaciones
Sistemas responsables	<ul style="list-style-type: none">● Establecer y hacer cumplir reglas sobre cuándo se puede acceder a los datos● Seguimiento inmutable del acceso a los datos por parte de los controladores de datos	<ul style="list-style-type: none">● Casos de uso limitados y falta de aplicaciones autónomas● Complejidad de configuración● Riesgos de cumplimiento en privacidad y protección de datos cuando se usan tecnologías de registros distribuidos (DLT)
Compartición secreta umbral (Threshold secret sharing)	Aprendizaje automático con preservación de la privacidad	<ul style="list-style-type: none">● Desafíos de seguridad digital
Almacenes de datos personales / Sistemas de gestión de información personal (PIMS)		<ul style="list-style-type: none">● No se consideran PETs en sentido estricto

Fuente: Informe *‘Emerging privacy enhancing technologies: current regulatory and policy approaches’*.
OECD Marzo 2023.