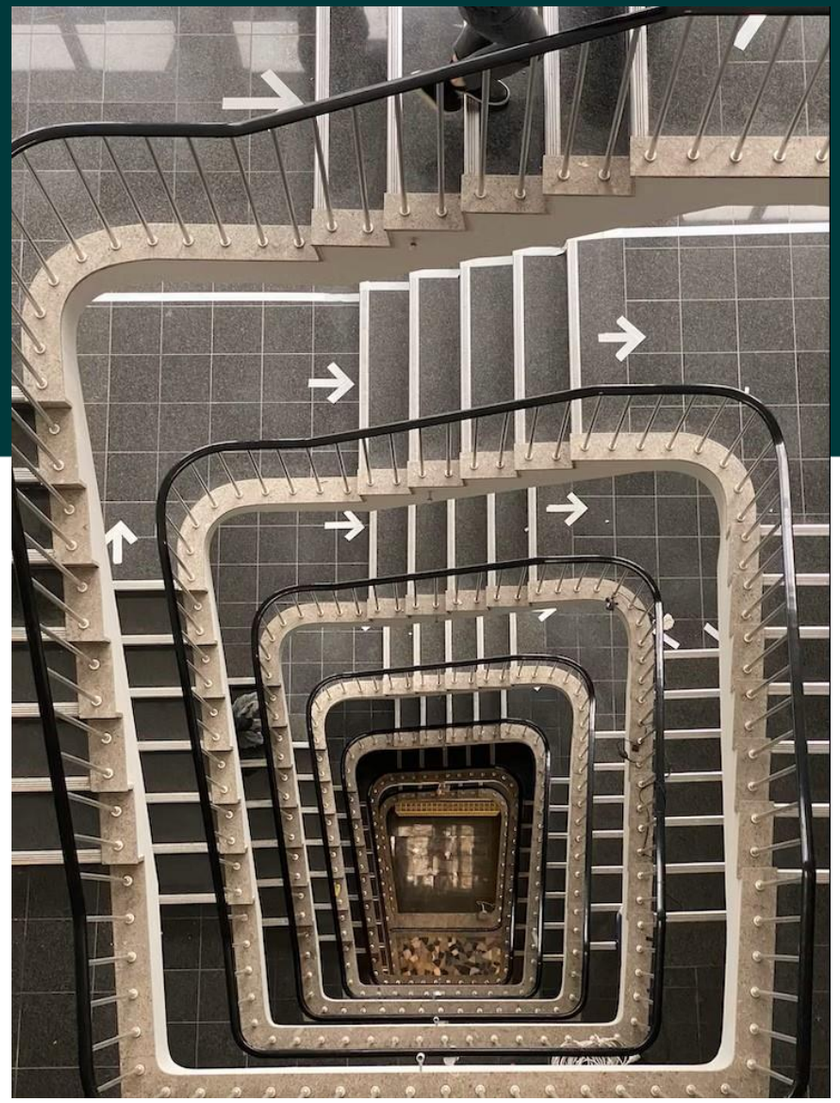
Universidad Internacional de Andalucía

Septiembre 2023

Amenazas para la privacidad y medidas de seguridad en el ámbito de los nuevos paradigmas tecnológicos

MARTA BELTRÁN PARDO

marta.beltran@urjc.es
@MBeltranPardo

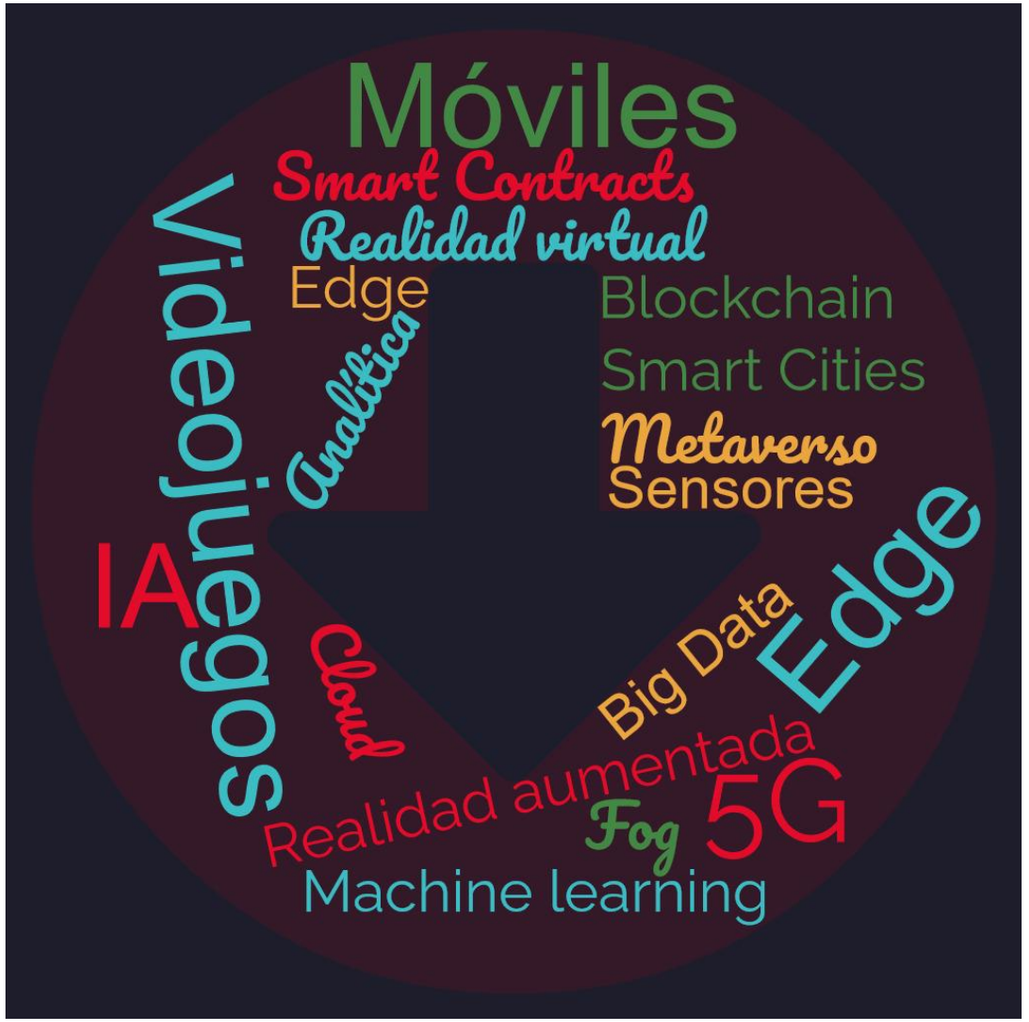


Agenda

01. Nuevos tratamientos de datos
02. Amenazas para la privacidad
03. Big Data
04. Inteligencia Artificial
05. Conclusiones

Nuevos paradigmas tecnológicos

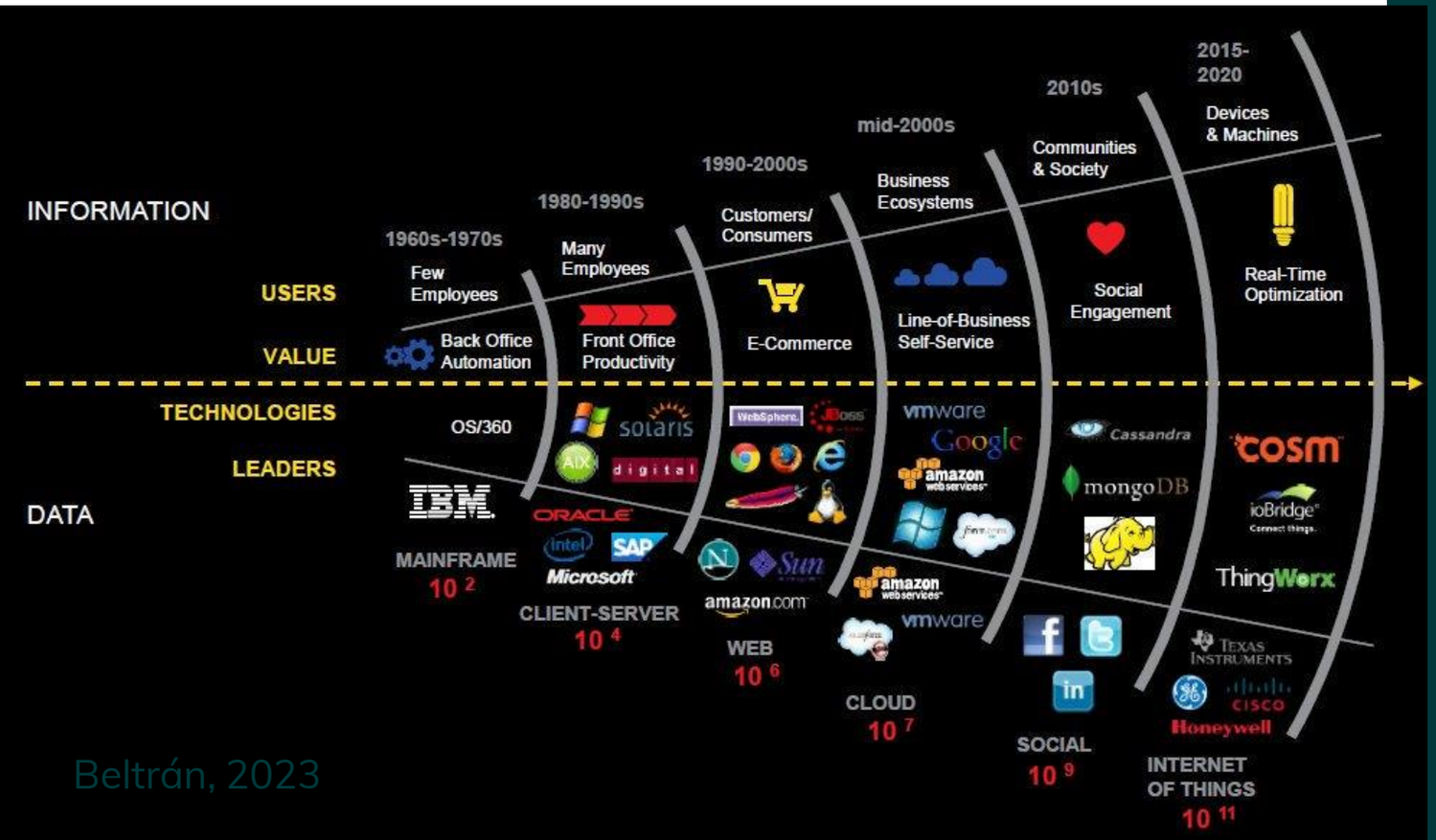
01. Nuevos tratamientos de datos



Beltrán, 2023

Evolución de Internet

Fuente: Informatica, 2013

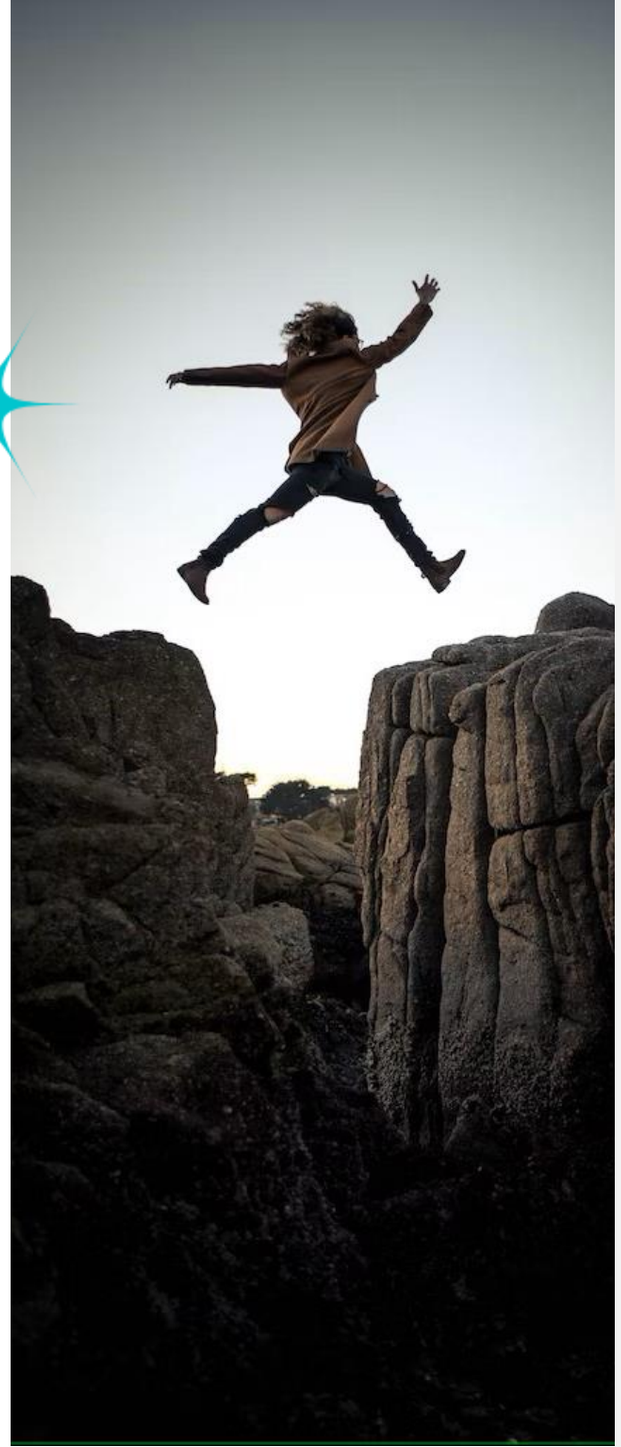


Beltrán, 2023

1. Contenidos
2. Servicios
3. Personas
4. Cosas

Nuevos elementos

1. Usuarios - Escala: De unos pocos a miles de millones, de la esfera profesional a la personal.
2. Valor- Duración: De algo puntual a la conexión constante.
3. Tecnología- Arquitectura: De algo centralizado a algo distribuido/ubicuo, de un proveedor a muchos.
4. Líderes- Modelo de negocio: Cada vez más basado en datos y perfiles.



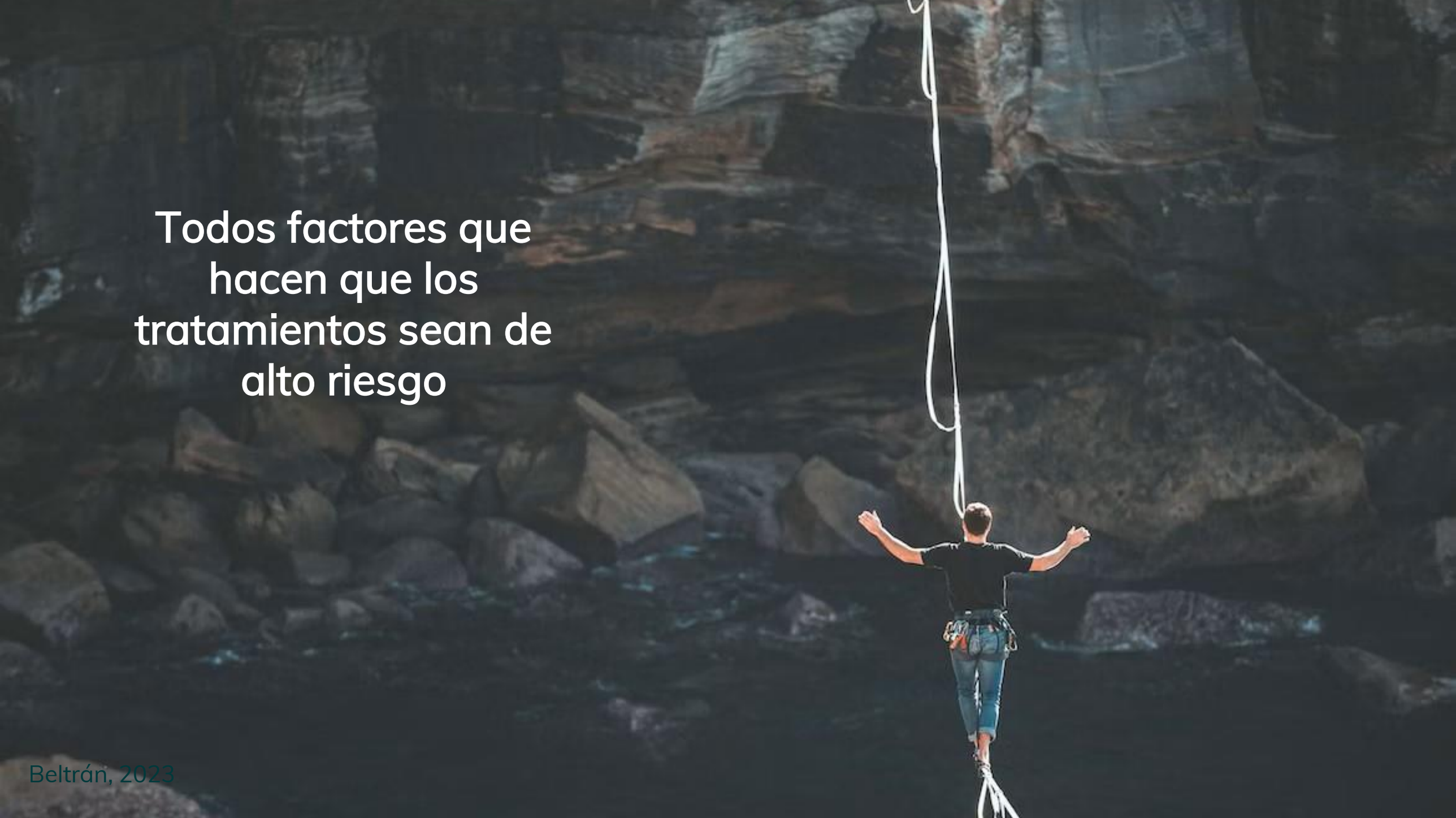
Beltrán, 2023

¿Cómo afecta todo esto al tipo de tratamiento de datos que se realiza?

Beltrán, 2023

Se extienden los tratamientos con determinadas características:

- Observación, monitorización, supervisión, geolocalización o control del sujeto de forma sistemática y exhaustiva.
- Recogida de datos del sujeto en múltiples ámbitos de su vida.
- Recogida de datos de categorías especiales, incluidos biométricos.
- Tratamientos a gran escala.
- Uso innovador de tecnologías.
- Combinación de datos de diferentes fuentes, tratamientos, etc.



Beltrán, 2023

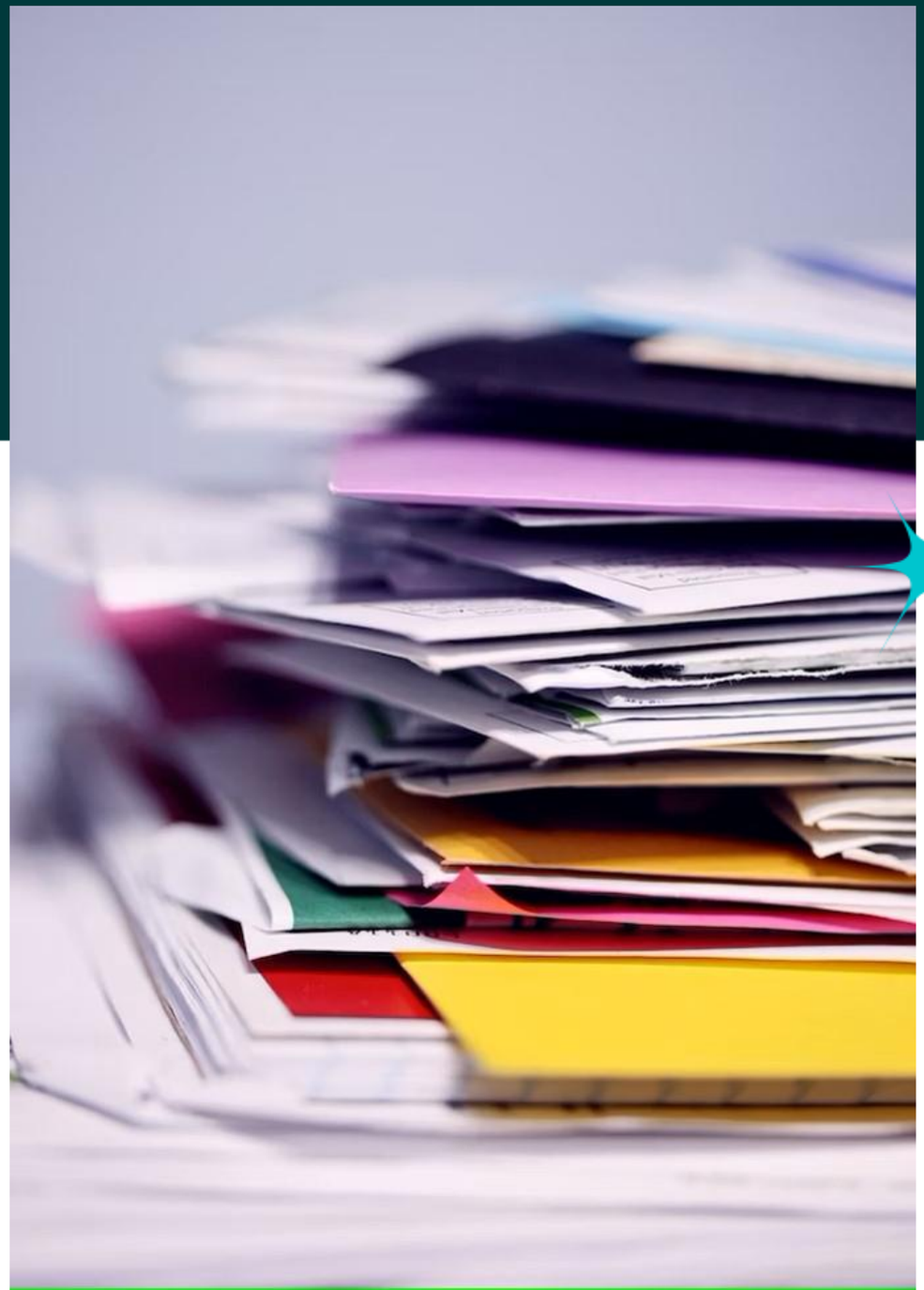
Amenazas relacionadas con el propósito o fin del tratamiento

- ¿Observación, monitorización, supervisión, geolocalización o control del sujeto de forma sistemática y exhaustiva?
- ¿Toma de decisiones automatizadas?
- ¿Se puede llegar a impedir al sujeto el acceso a un bien o un servicio o formar parte de un contrato?
- ¿Puede tener efectos legales?

Beltrán, 2023

Amenazas relacionadas con el tipo de datos tratados

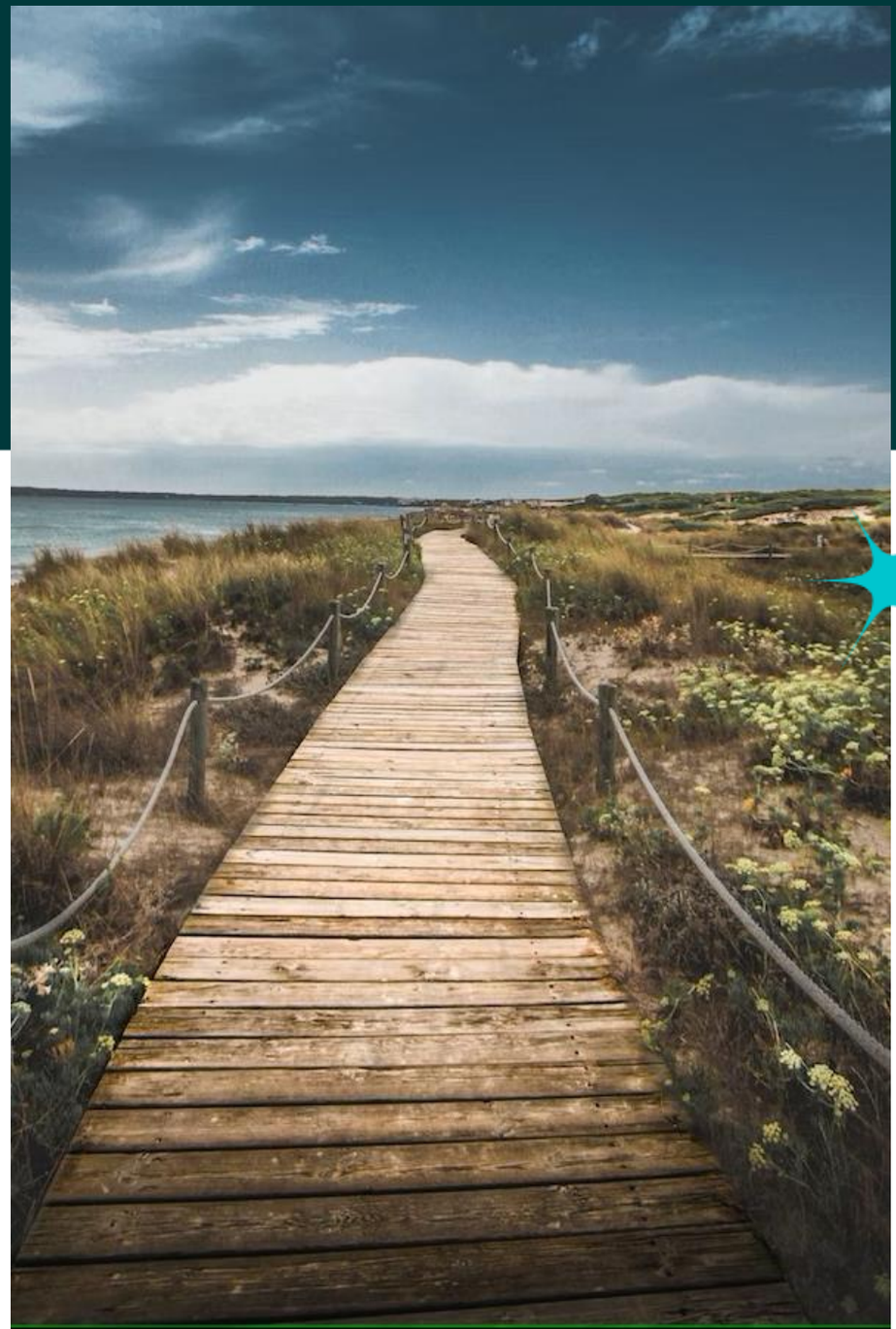
- ✓ Biometría, neurodatos, datos de salud o genéticos, datos de comportamiento.
- ✓ Metadatos, huellas identificativas de dispositivos.
- ✓ Posibilidad de identificación real (en el mundo físico).



Beltrán, 2023

Amenazas relacionadas con el ciclo de vida de los datos

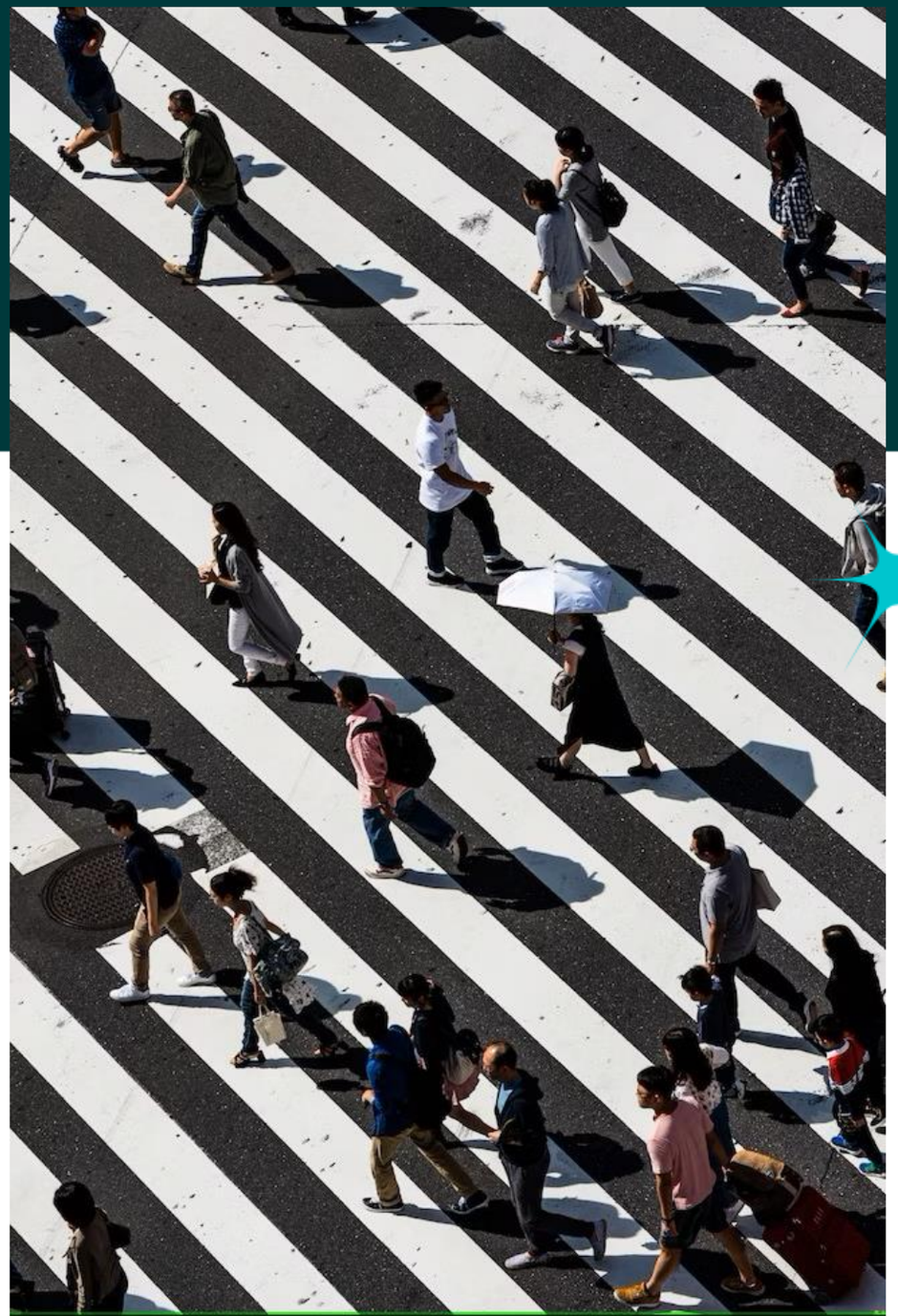
- ✓ ¿Cómo se capturan? ¿Es el sujeto consciente, tiene que hacer algo?
- ✓ ¿Se puede capturar información de más?
- ✓ ¿Cómo/dónde se procesan y almacenan?
- ✓ ¿Cuándo se borran? ¿Se borran de todas las copias (metadatos, copias de seguridad, logs)?



Beltrán, 2023

Amenazas relacionadas con las categorías de interesados

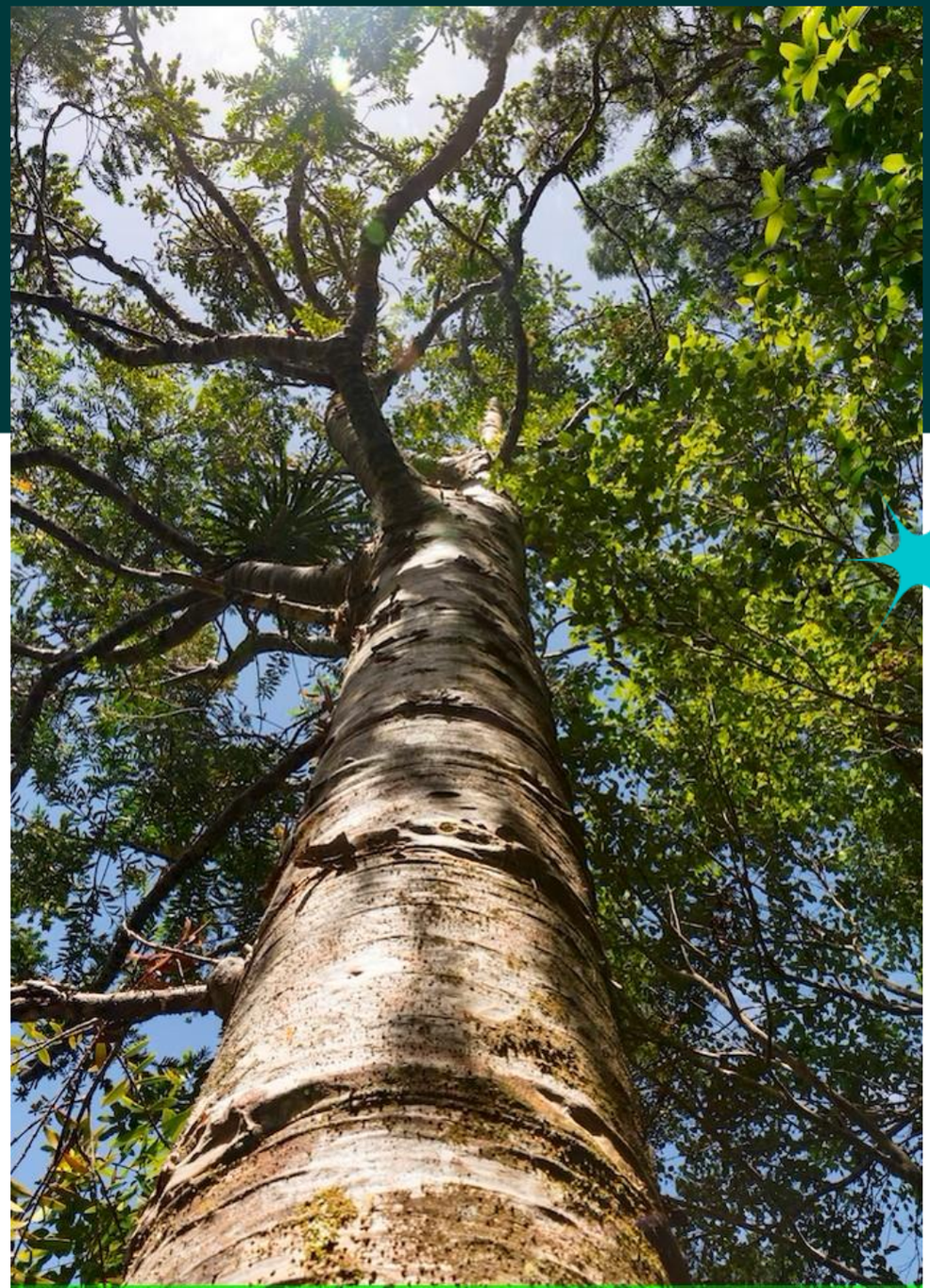
- ¿Menores, víctimas de violencia de género, refugiados?
- ¿Cómo se puede saber o distinguir?
- ¿Existen medidas y mecanismos de protección adaptativos?



Beltrán, 2023

Amenazas relacionadas con la extensión o alcance del tratamiento

- ✓ ¿Número de sujetos?
- ✓ ¿Volumen de datos tratados por sujeto?
- ✓ ¿Duración en el tiempo del tratamiento?
- ✓ ¿Frecuencia?



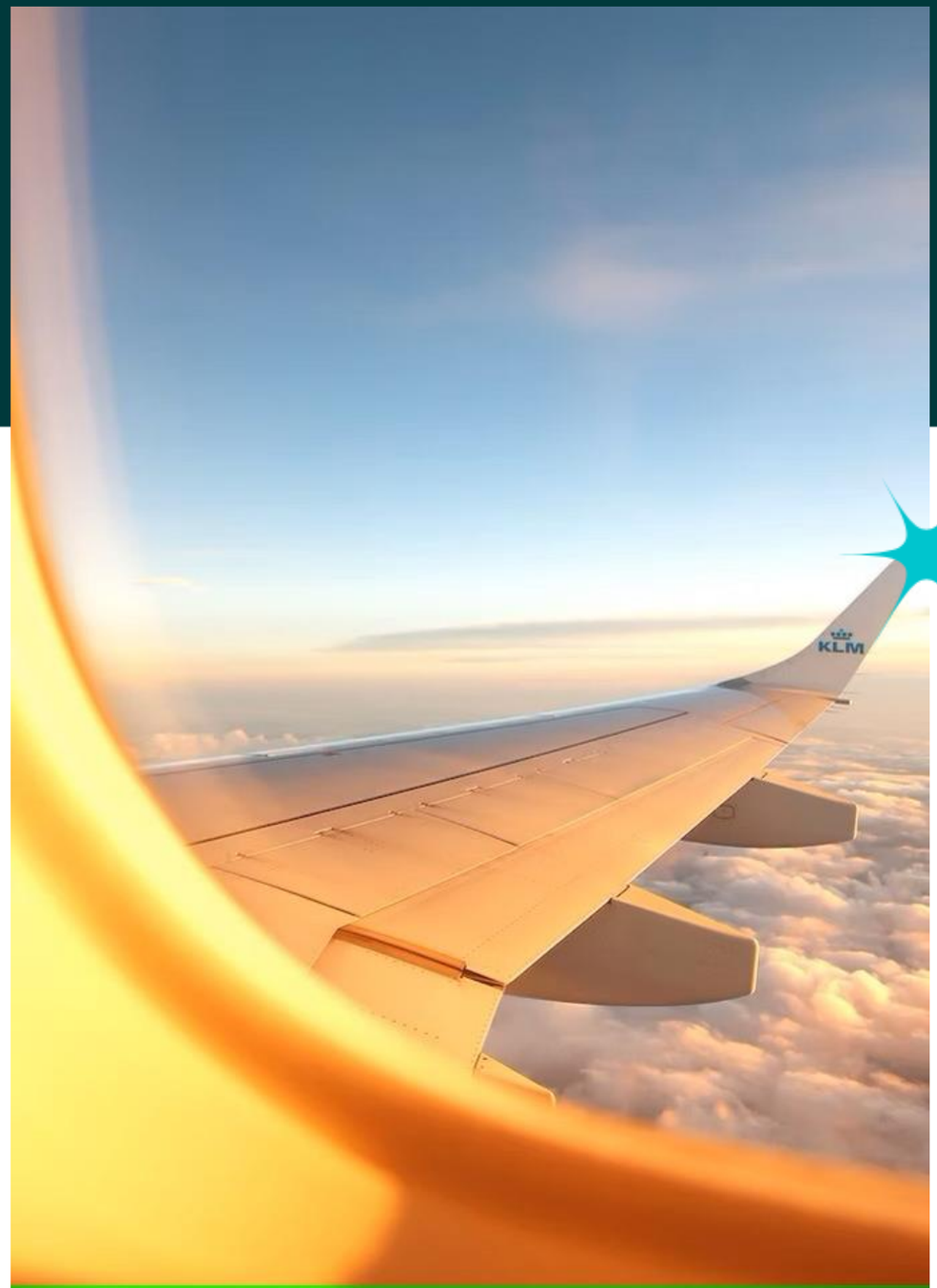
Beltrán, 2023

Amenazas relacionadas con el grado de control de los sujetos

- ¿Tienen alguno? ¿Cómo lo ejercen?
- ¿Se respeta el principio de transparencia?
- ¿Tienen otras alternativas?

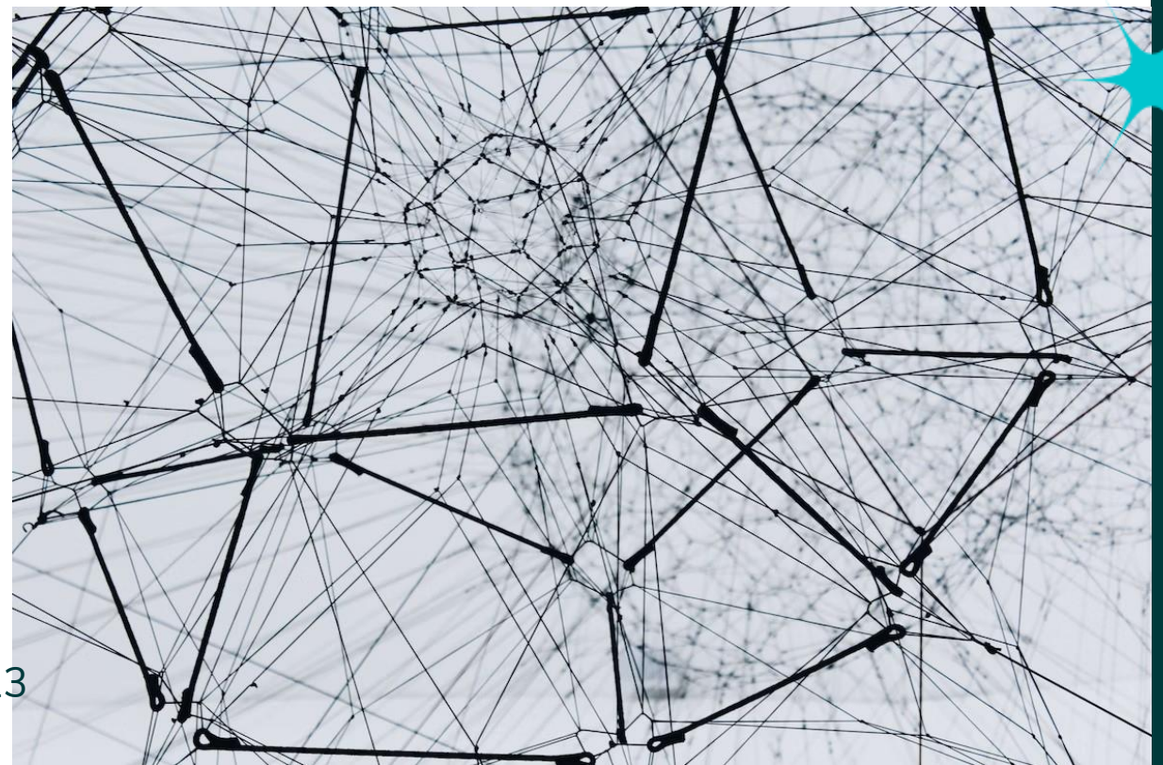
Beltrán, 2023

Amenazas relacionadas con la transferencia de datos a terceros



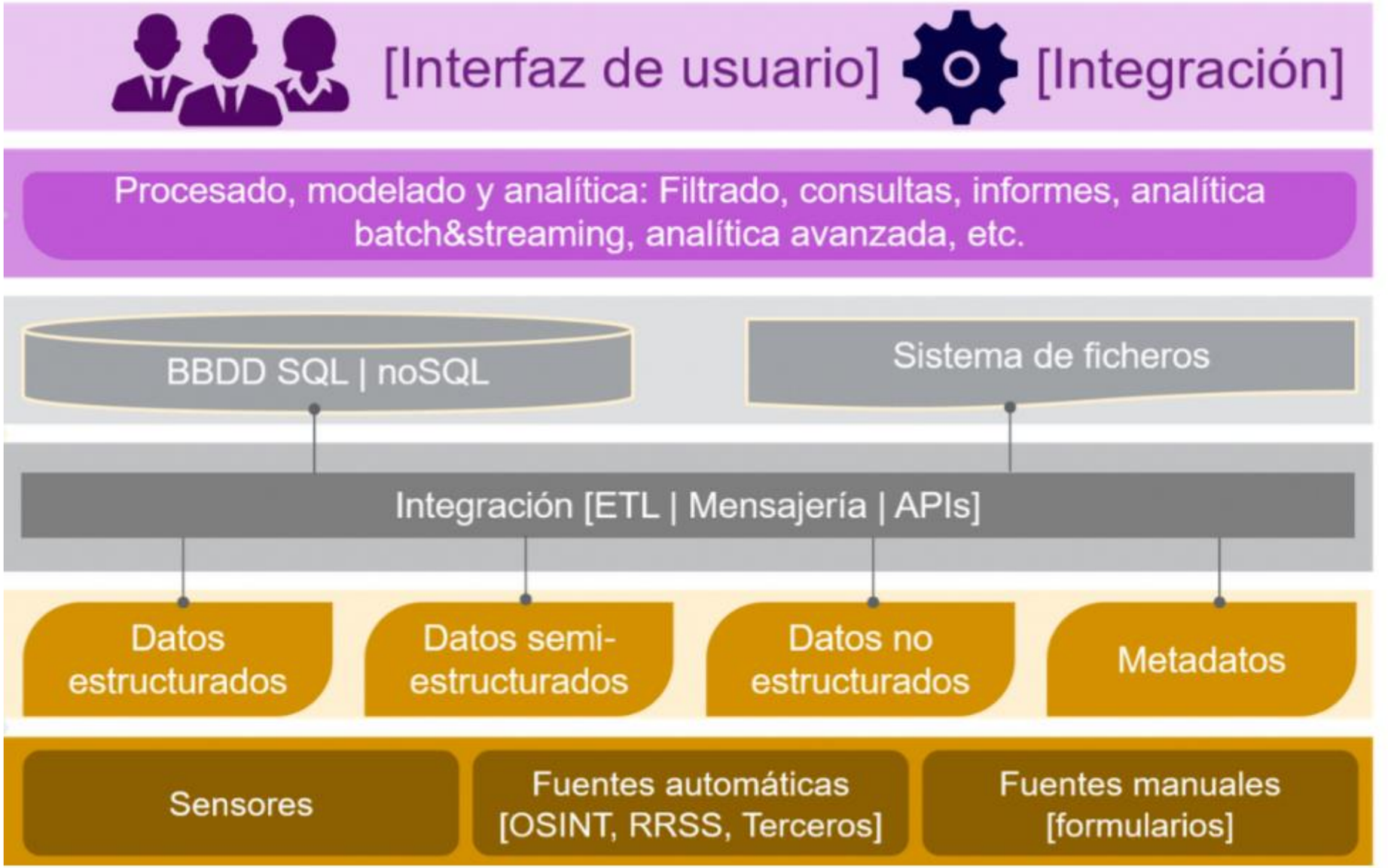
- ✓ ¿Qué datos se transfieren a estos terceros y para qué? ¿Qué obligaciones de cumplimiento tienen? ¿Qué tipo de acuerdos y contratos hay firmados con estos terceros?
- ✓ ¿Se informa adecuadamente de estas transferencias?

¿Qué es “Big” en la actualidad?



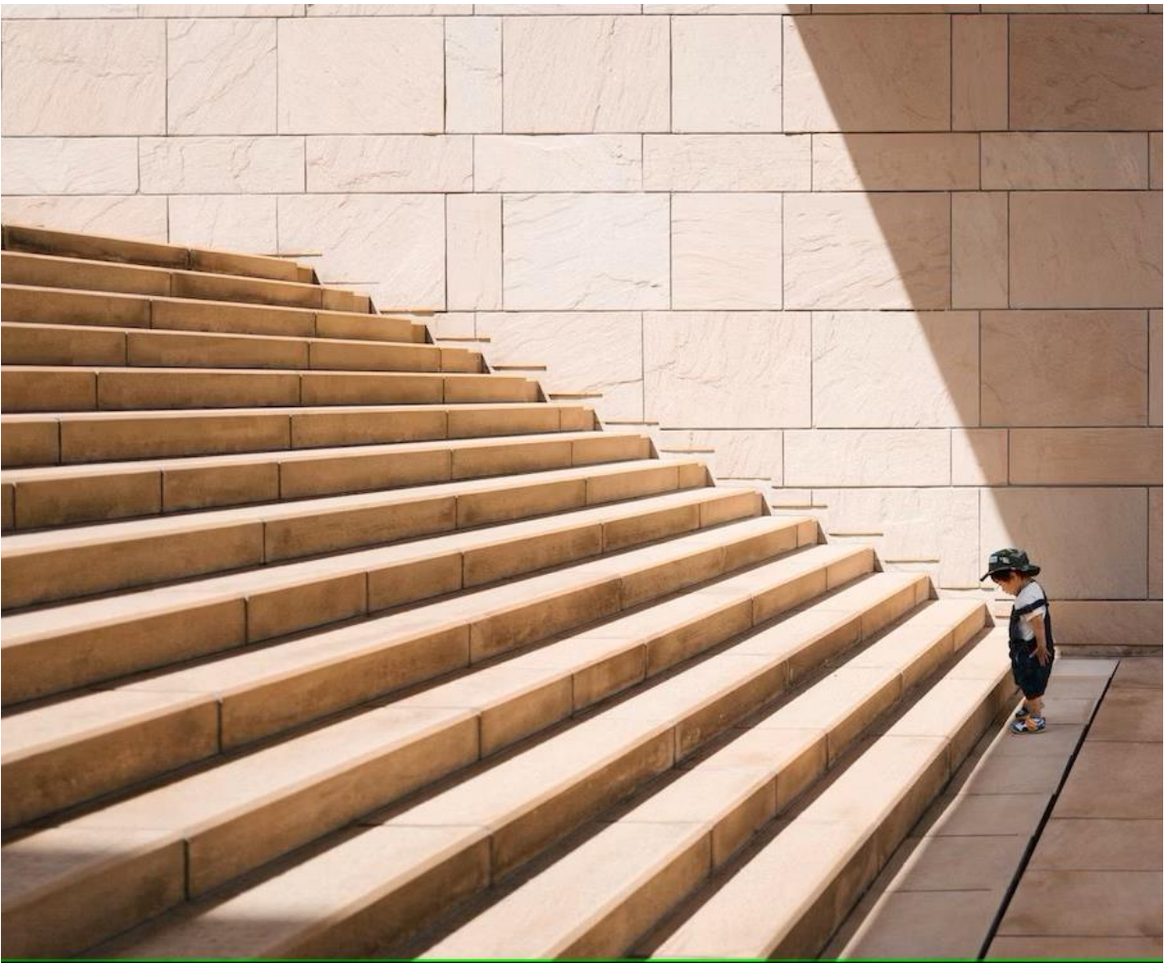
- Variedad
- Volumen
- Velocidad
- Veracidad + Valor

Beltrán, 2023



Beltrán, 2023

Retos diferentes en todas las capas



Seguridad y protección de datos

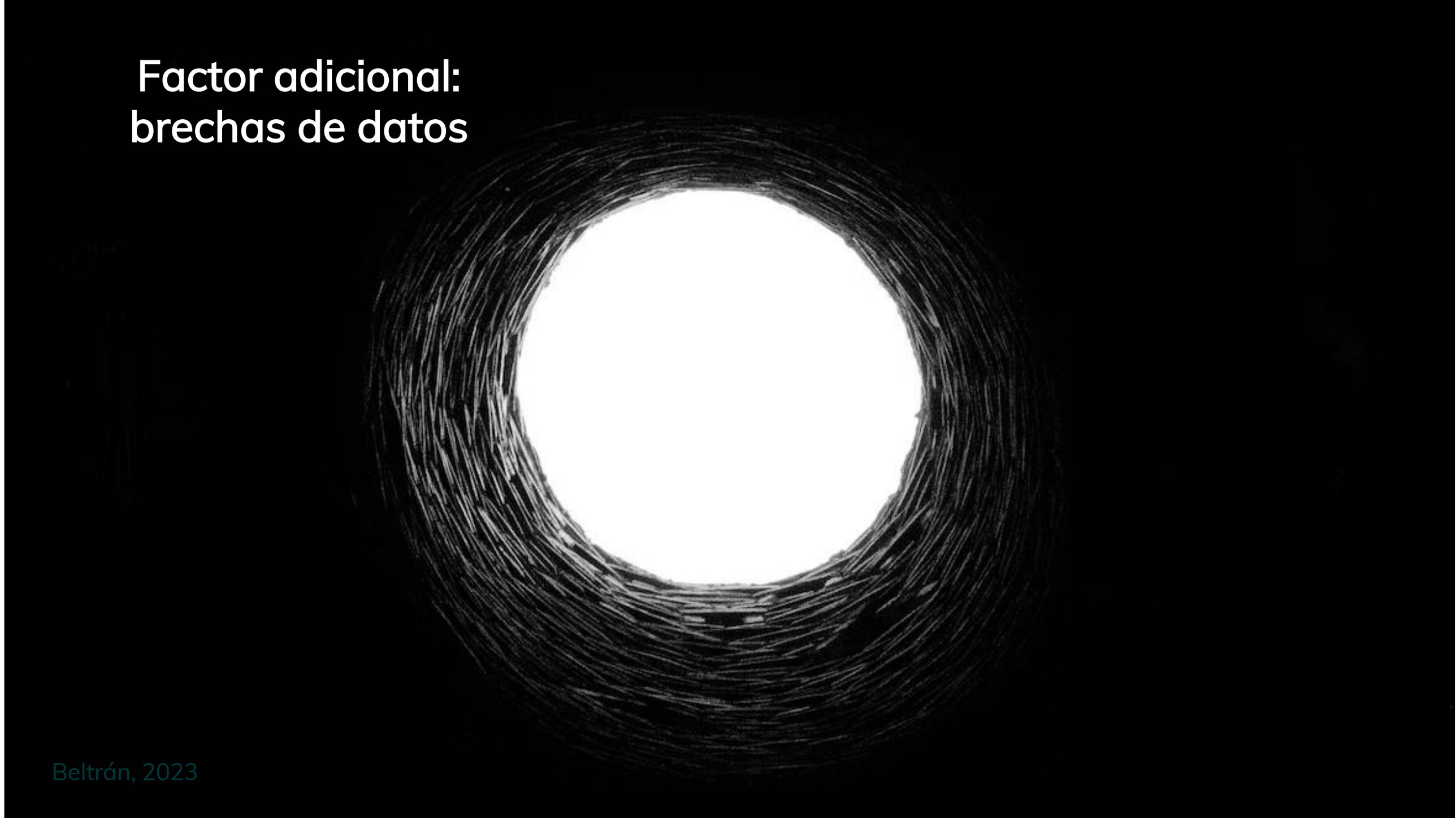
- Asegurar niveles suficientes de:
  - Confidencialidad.
  - Integridad.
  - Disponibilidad.

Privacidad

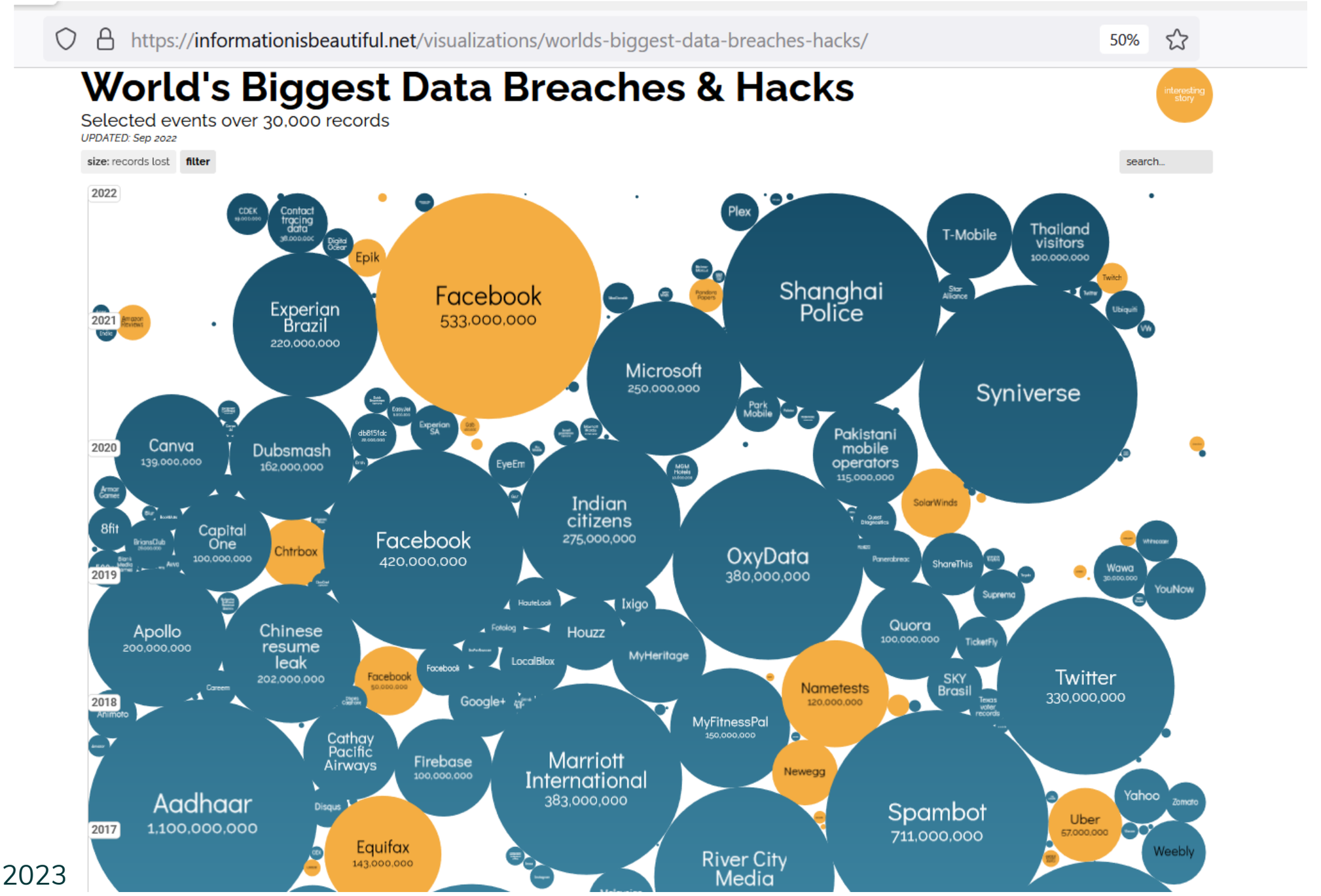
- Minimizar, separar, abstraer, esconder.
- Informar, controlar, obligar, demostrar.

Beltrán, 2023

Factor adicional: brechas de datos

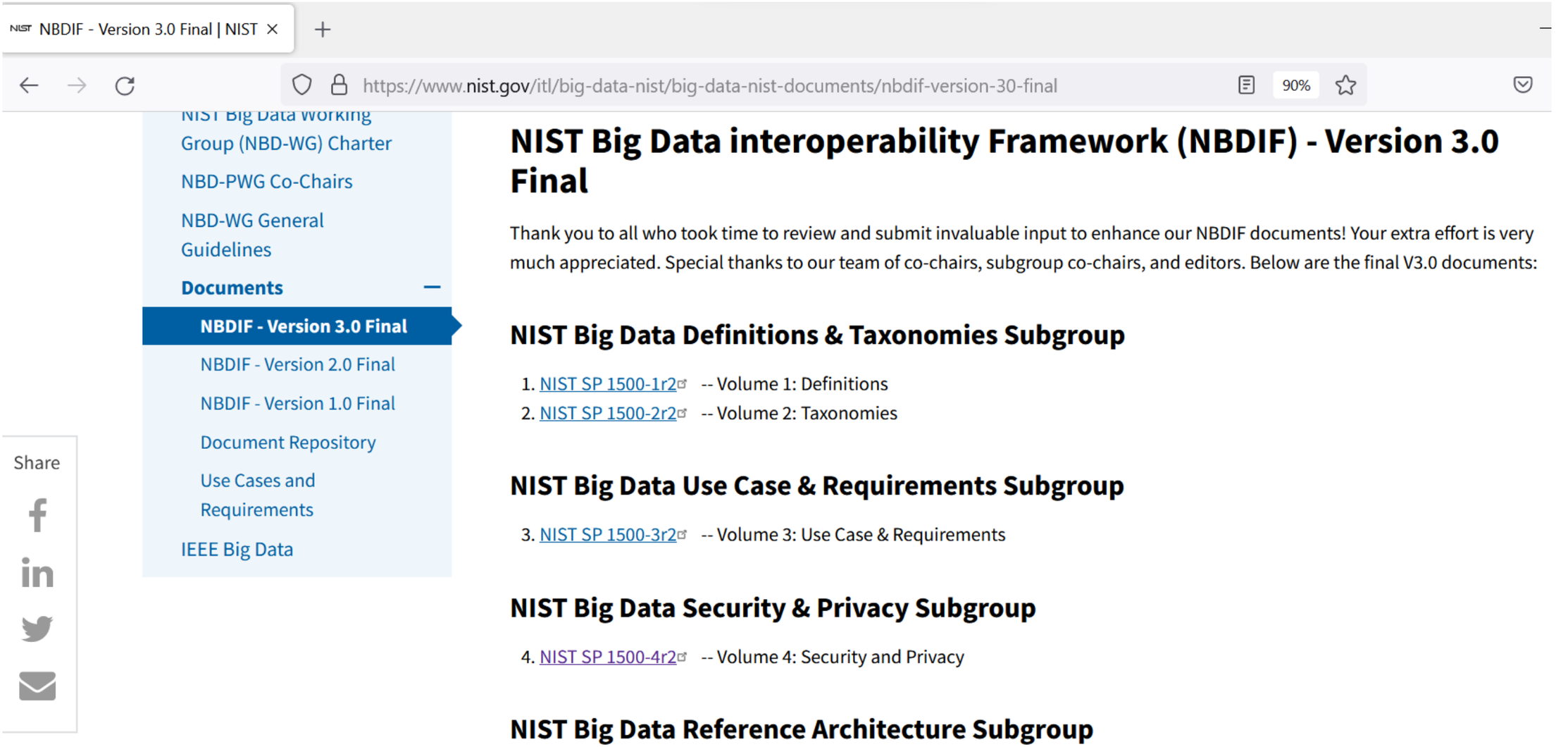


Beltrán, 2023



Beltrán, 2023

Beltrán, 2023



Beltrán, 2023

NIST Special Publication 1500-4r2

NIST Big Data Interoperability Framework: Volume 4, Security and Privacy

Version 3

NIST Big Data Public Working Group
Definitions and Taxonomies Subgroup
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-4r2

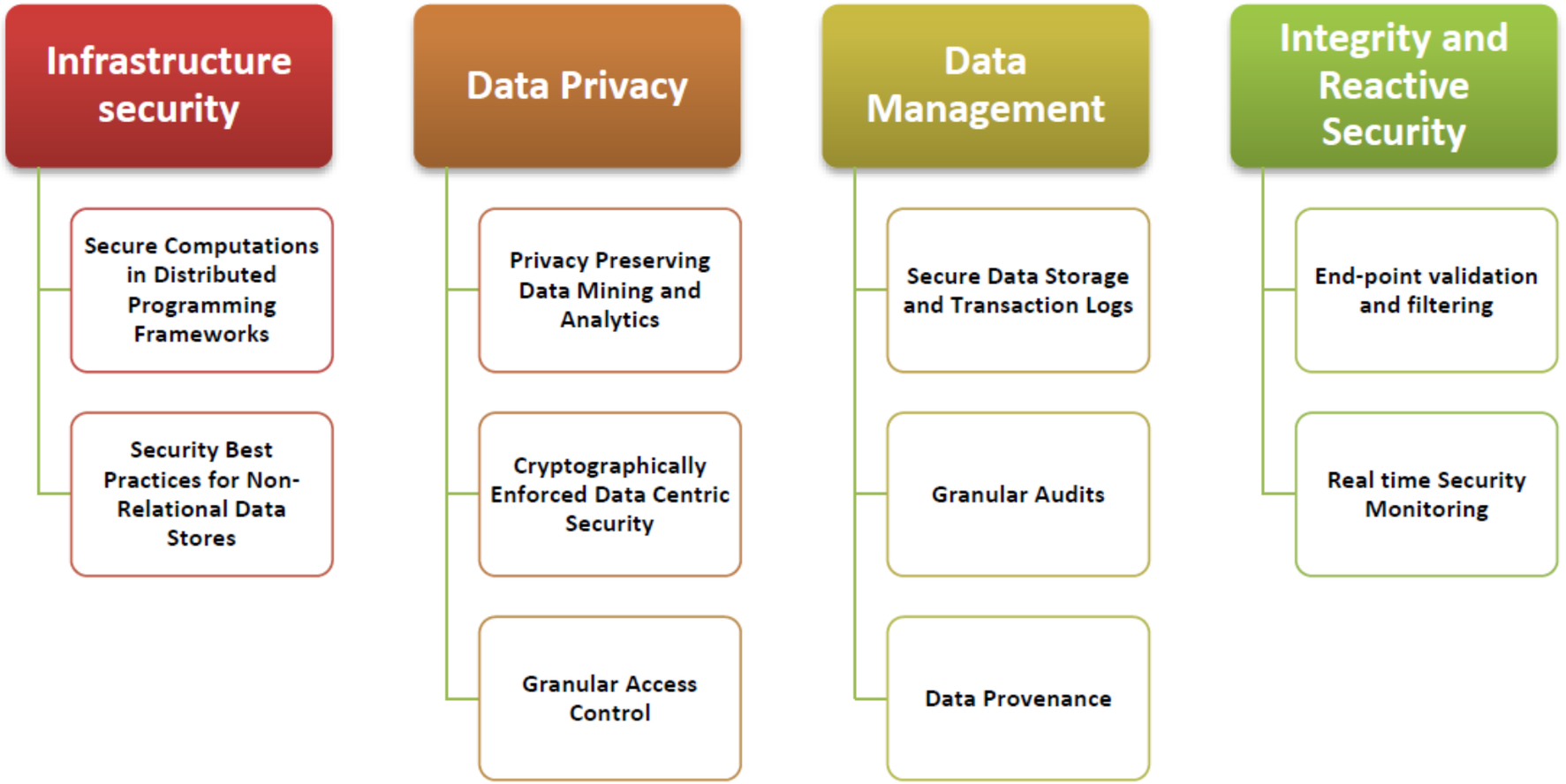
October 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

Beltrán, 2023

cloud security alliance®



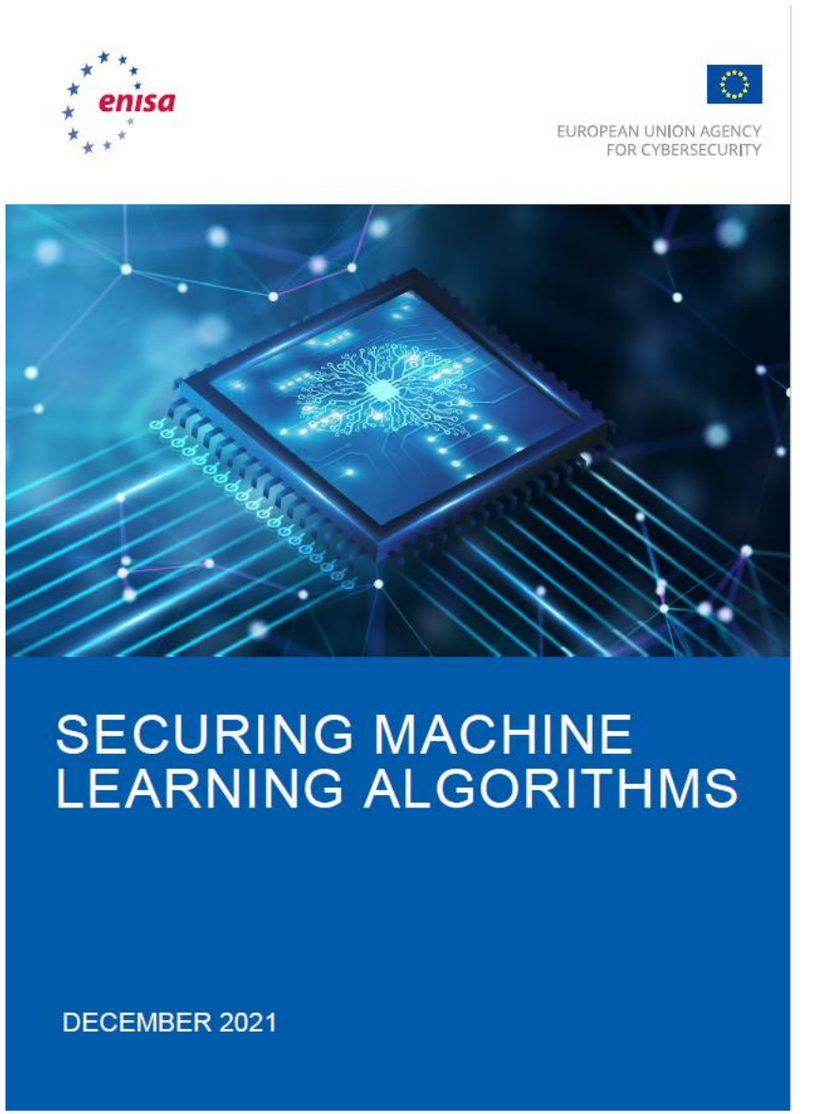
Beltrán, 2023

Beltrán, 2023

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

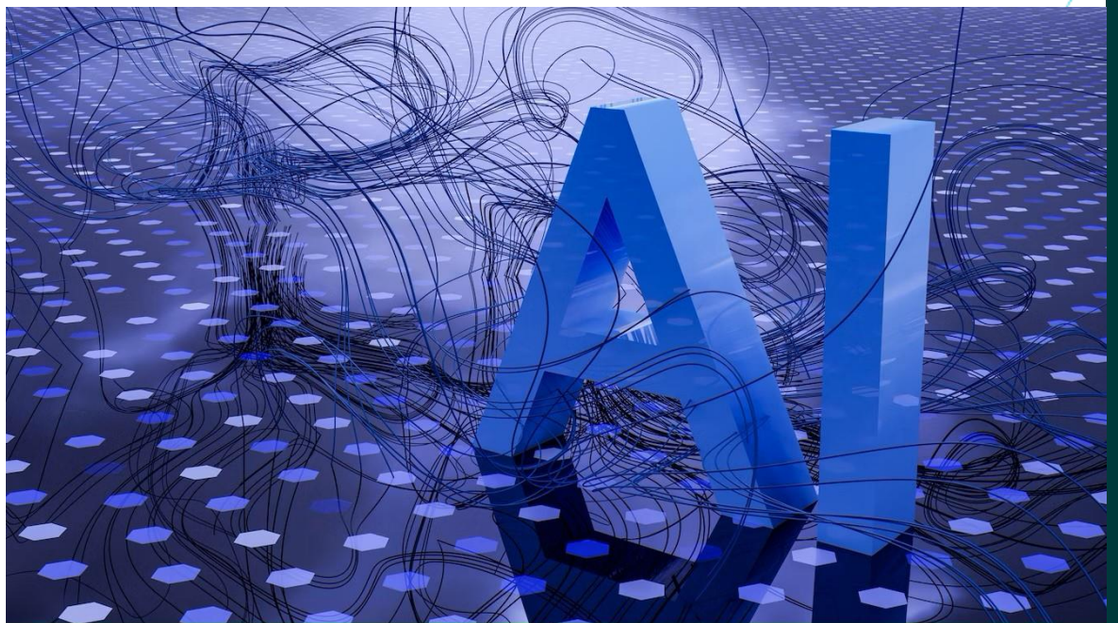
CHALLENGES/ MITIGATION MEASURES	ENCRYPTION	SECURITY TESTING AND CODE AUDITING	CERTIFICATION STANDARDS	RISK ASSESSEMENT	SOURCE FILTERING	ACCESS CONTROL AND AUTHENTICATION	MONITORING AND LOGGING
Source validation and Filtering	Yes	Yes		Yes	Yes	Yes	Yes
Secure computation	Yes	Yes	Yes		Yes	Yes	Yes
Access control and authentication	Yes	Yes	Yes			Yes	Yes
Secure Data Management	Yes	Yes				Yes	Yes
Infrastructure security		Yes	Yes		Yes	Yes	Yes
Supply chain security		Yes	Yes	Yes			
Application software security		Yes	Yes			Yes	
Trustworthiness of devices		Yes	Yes			Yes	
Interoperability of applications		Yes	Yes			Yes	
Secure Use of Cloud computing	Yes	Yes	Yes	Yes		Yes	Yes
Distributed Denial of Service Attacks		Yes			Yes		Yes

Beltrán, 2023

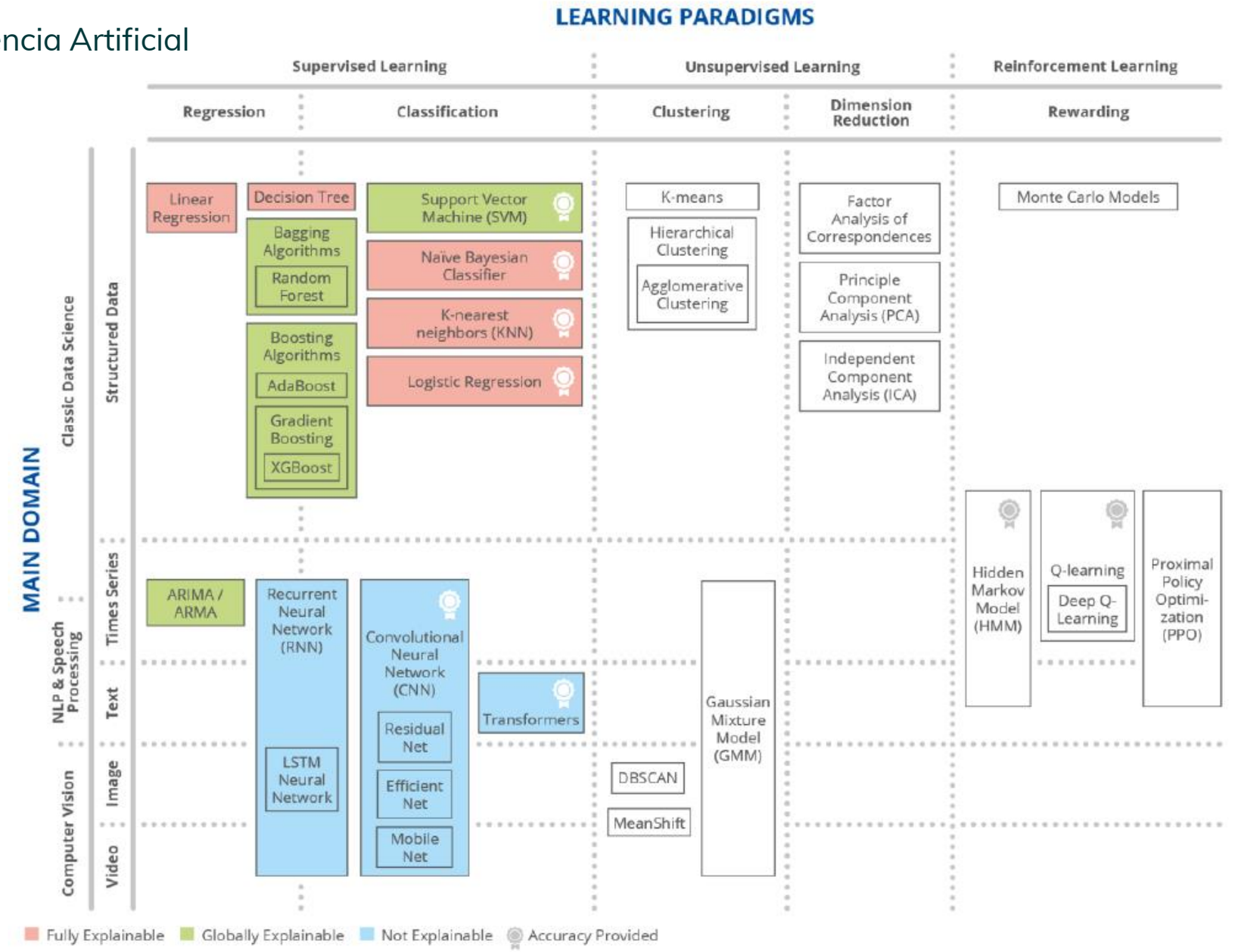


Beltrán, 2023

Big Data y Ciencia de datos -> Aprendizaje Automático -> Inteligencia Artificial



- Simulación de los mecanismos de aprendizaje de los organismos biológicos
- Una capa o multicapa (hasta el Deep Learning)
- Necesidad masiva de datos para el entrenamiento de los modelos
- Falta de transparencia, cajas negras, no explicables



Fuente: “SECURING MACHINE LEARNING ALGORITHMS”, ENISA, December 2021

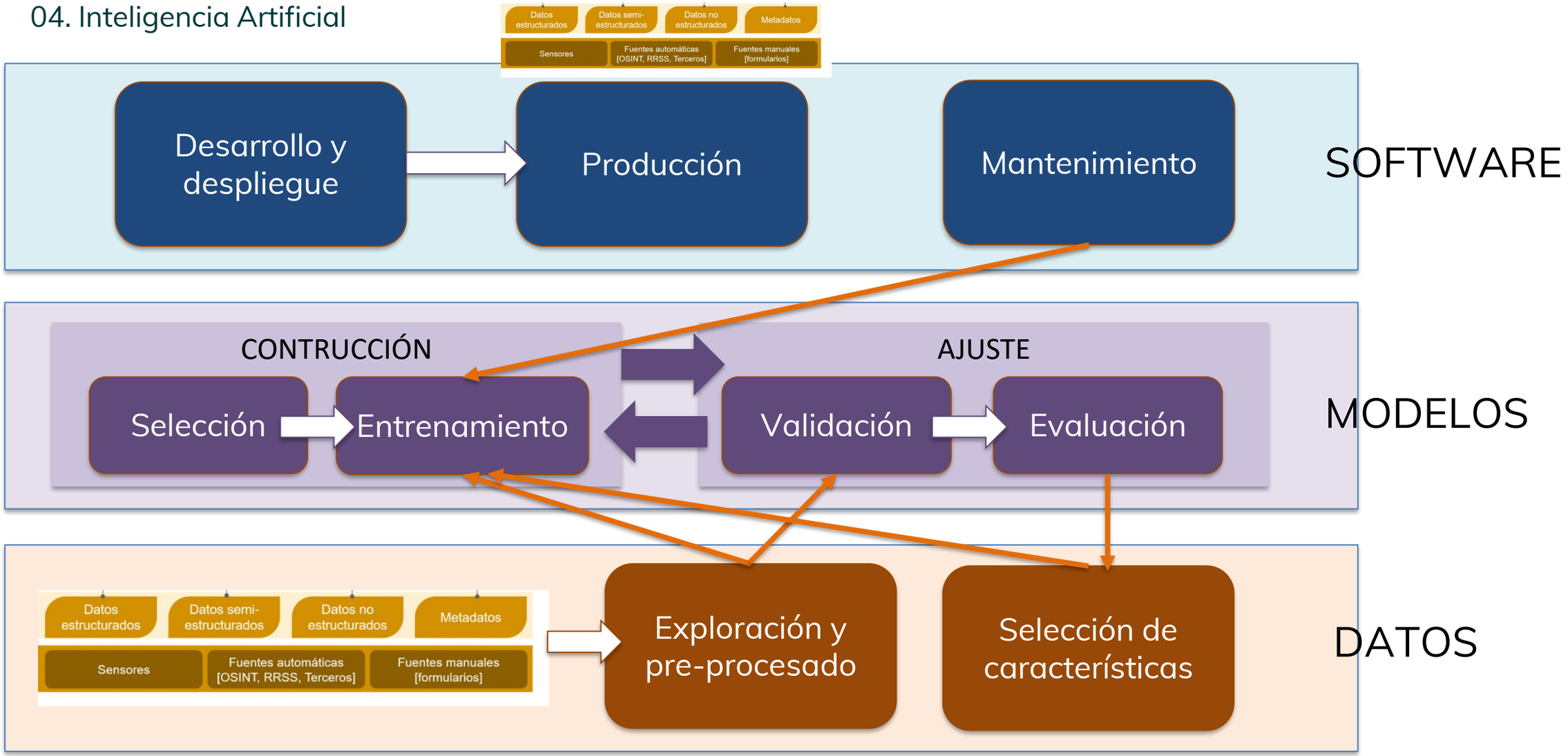
	AI taxonomy	
	AI domain	**AI subdomain**
Core	**Reasoning**	Knowledge representation
		Automated reasoning
		Common sense reasoning
	Planning	Planning and Scheduling
		Searching
		Optimisation
	Learning	Machine learning
	Communication	Natural language processing
	Perception	Computer vision
		Audio processing
Transversal	**Integration and Interaction**	Multi-agent systems
		Robotics and Automation
		Connected and Automated vehicles
	Services	AI Services
	Ethics and Philosophy	AI Ethics
		Philosophy of AI

Claramente, faltaría añadir una nueva fila para la **GENERACIÓN** de contenidos

Beltrán, 2023

Fuente: “AI WATCH: DEFINING ARTIFICIAL INTELLIGENCE 2.0”, European Comission, 2021

04. Inteligencia Artificial



Beltrán, 2023

Aparecen todas las amenazas ya mencionadas y otras nuevas

¿QUÉ ESTAMOS OBSERVANDO?

Apropiación de datos

Clearview AI y casos de *scraping* masivo

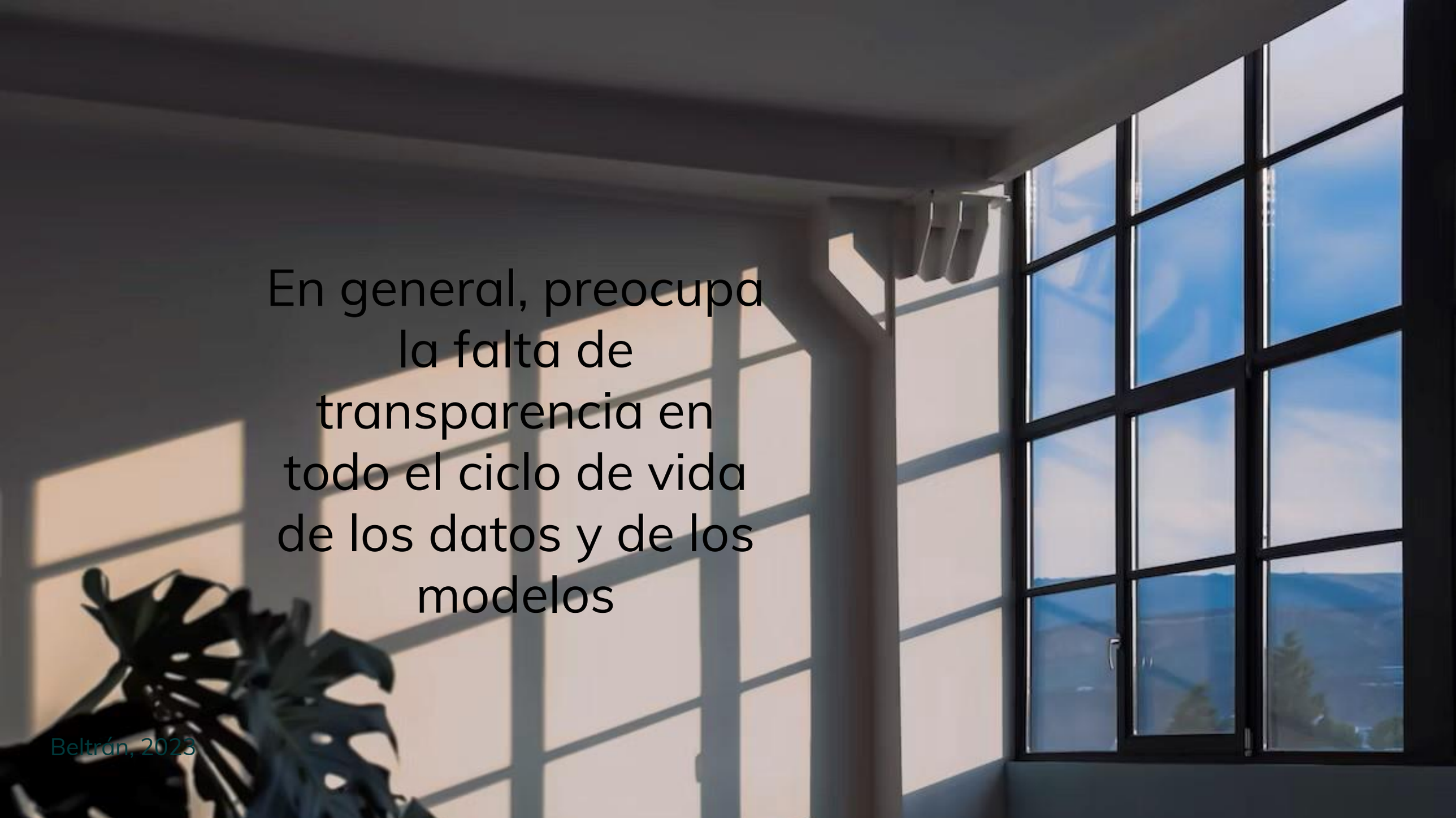
Manipulación masiva

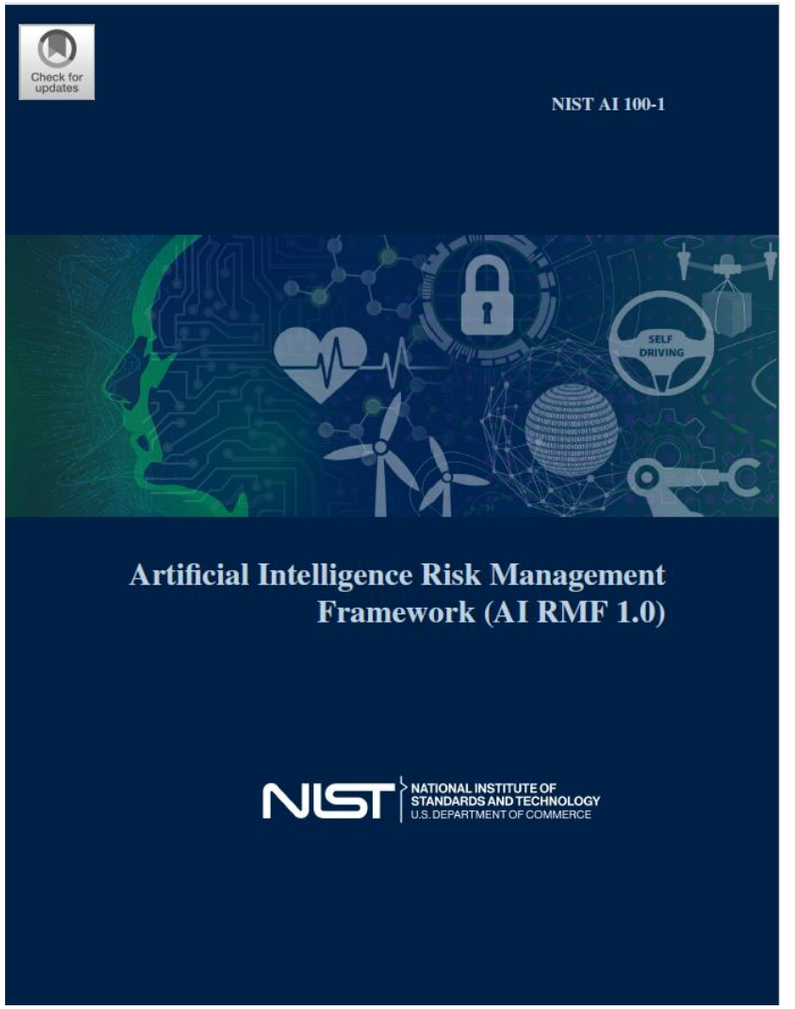
Procesos electorales, venta en momentos vulnerables (incluido perfilado de salud o genético)

Ataques al rendimiento de los modelos

Manipulación de los conjuntos de datos de entrenamiento o de los datos de entrada (*adversarial attacks*)

Generación de datos personales

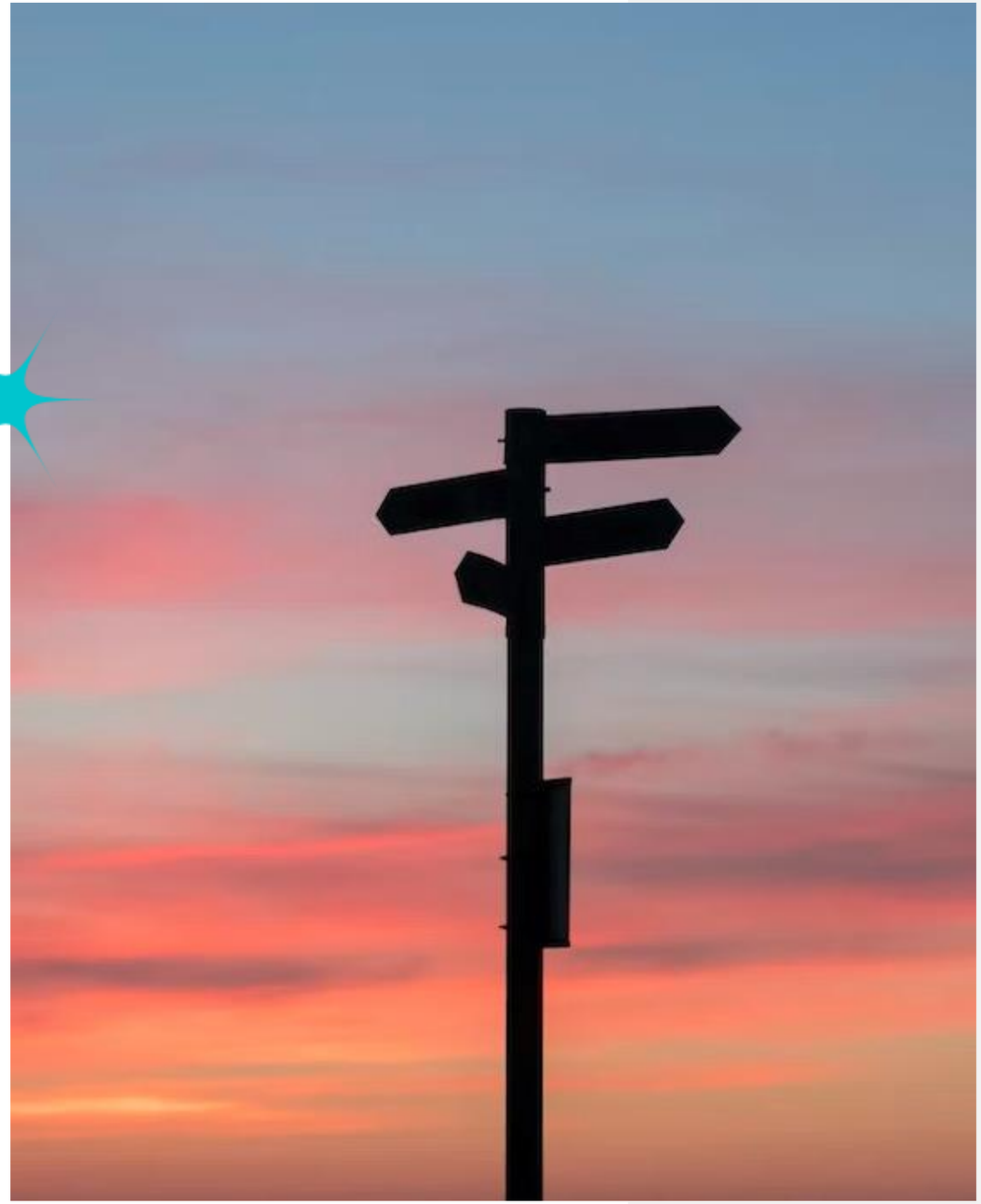

En general, preocupa la falta de transparencia en todo el ciclo de vida de los datos y de los modelos
Beltrán, 2023



Beltrán, 2023

Entornos muy complejos y cambiantes

1. Se debe trabajar el concepto de *Trustworthiness.*
2. Gestionando el riesgo, no sólo documentándolo.
3. El modelado de amenazas será cada vez más importante.



Beltrán, 2023

1 ¿Trustworthiness?

GESTIÓN CONJUNTA DE LOS RIESGOS

- Ya que todo está conectado…

Privacy	*Reliability*	*Resilience*	*Safety*	*Security*

Beltrán, 2023

2 Gestión del riesgo

GESTIÓN REAL, ANTICIPANDO LOS PROBLEMAS

- Las metodologías están evolucionando para dar respuesta a los nuevos retos.

NIST PRIVACY FRAMEWORK

aepd agencia española protección datos

Gestión del riesgo y evaluación de impacto en tratamientos de datos personales

Junio 2021

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Quantitative Privacy Risk Analysis

Publisher: IEEE Cite This PDF

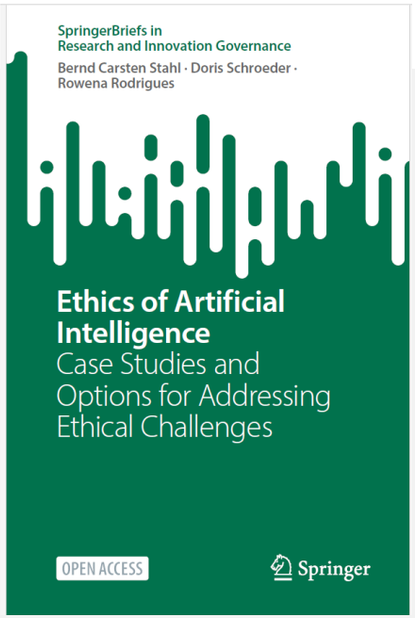
R. Jason Cronk ; Stuart S. Shapiro **All Authors**

Beltrán, 2023

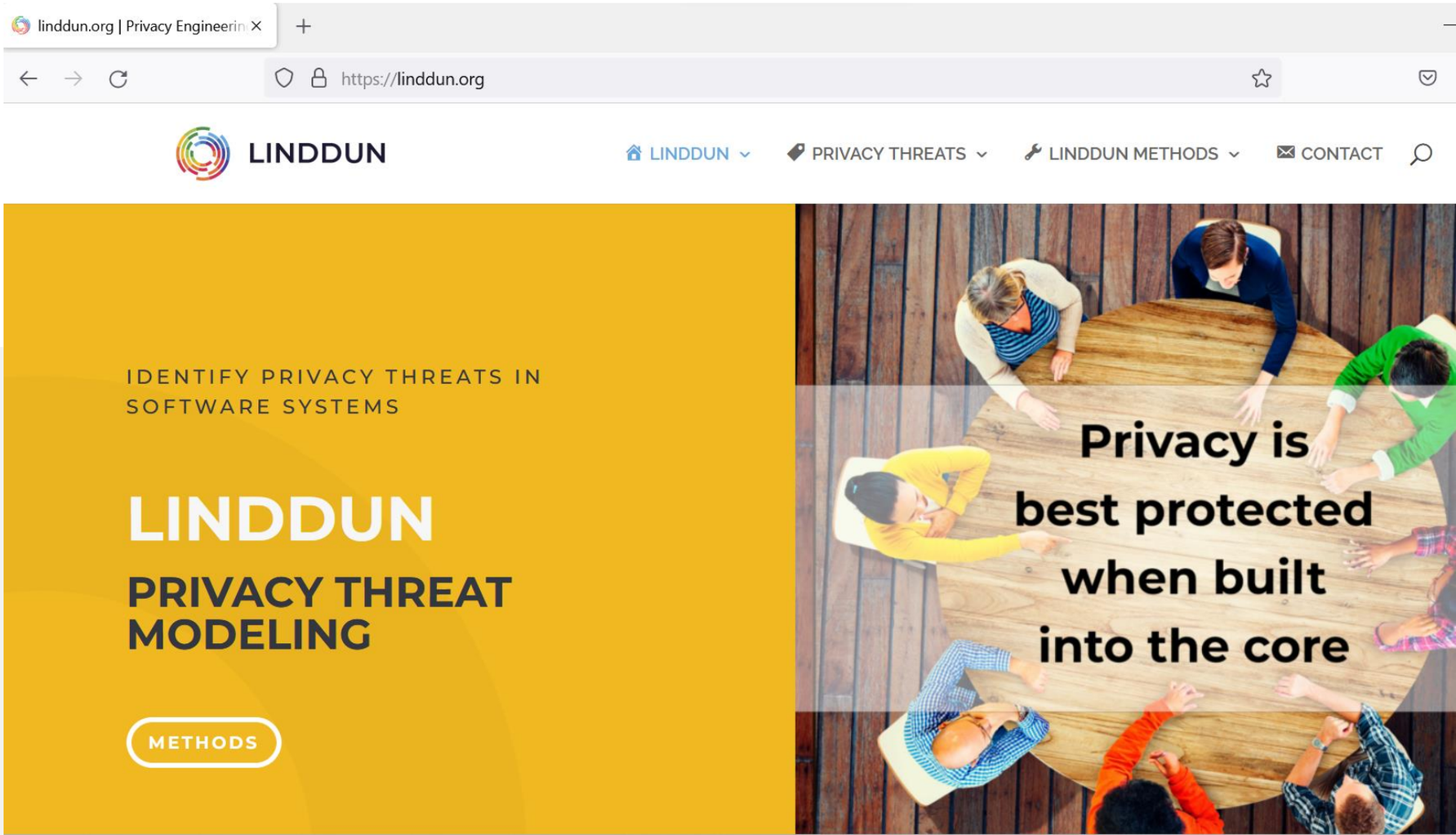
ISO/IEC 29134:2023(en) Information technology — Security techniques — Guidelines for privacy impact assessment

3 Modelado de amenazas

IMPRESCINDIBLE PARA COMPRENDER LOS ESCENARIOS DE RIESGO REALES

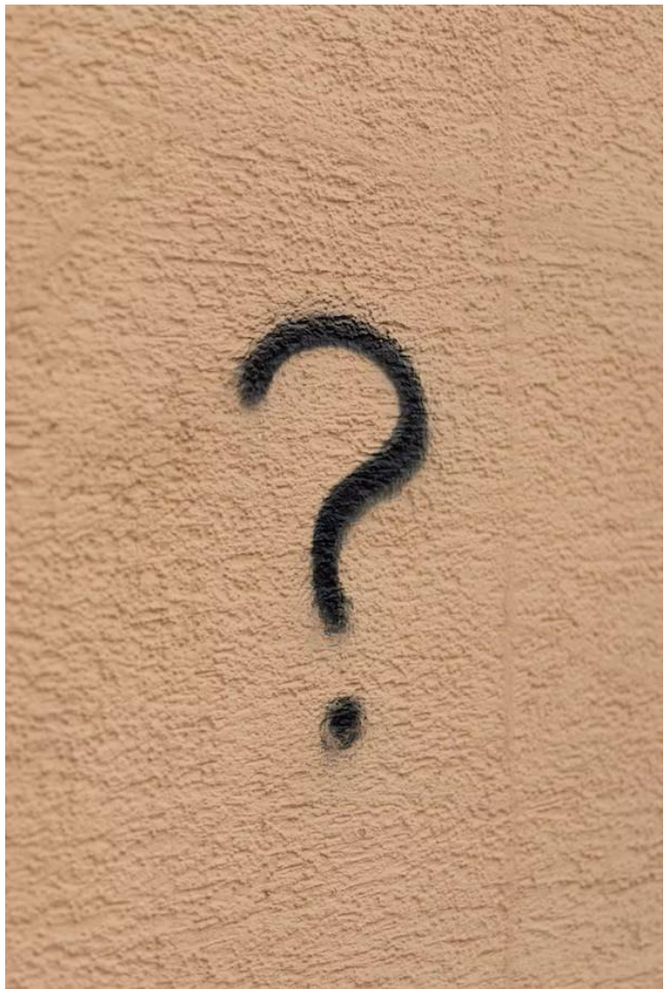


Beltrán, 2023



Beltrán, 2023

Gracias por su atención



- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/
- Plantilla
  - Visme