Inteligencia Artificial desde la perspectiva de Protección de datos

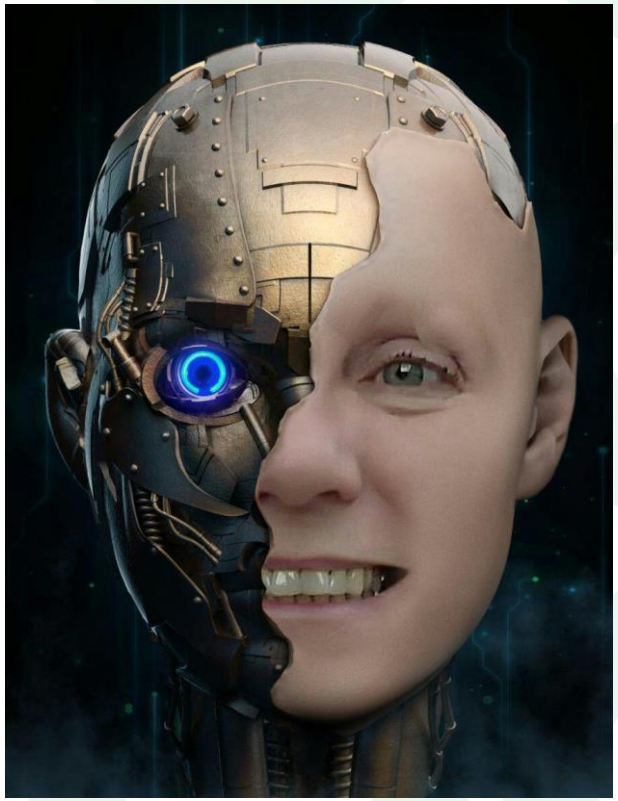
María Loza Corera, Lead Advisor Govertis

28 de Septiembre de 2020

GOVERTIS Advisory Services

ISACA Barcelona Chapter

Inteligencia Artificial



“programas informáticos (y posiblemente también equipos informáticos) **diseñados por seres humanos** que, dado un objetivo complejo, **actúan en la dimensión física o digital** mediante la percepción de su entorno mediante la adquisición de datos, la interpretación de los datos estructurados o no estructurados, el razonamiento sobre el conocimiento o el tratamiento de la información, fruto de estos datos y la decisión de las mejores acciones que se llevarán a cabo para alcanzar el **objetivo** fijado”.

Grupo expertos alto nivel IA.

MINSKY: “la ciencia de construir máquinas para que hagan cosas que, si las hicieran los humanos, requerirían inteligencia”.

Machine Learning- Deep Learning

IA débil o estrecha (weak)

se concreta o especializa en una determinada tarea.

Ej: DeepBlue, Watson, AlphaGo Zero

IA fuerte (strong)

realizando actividades como si de un humano se tratase

Super inteligencia artificial

que llegará a ser igual o mayor que la inteligencia humana

Singularidad. Vernor VINGE

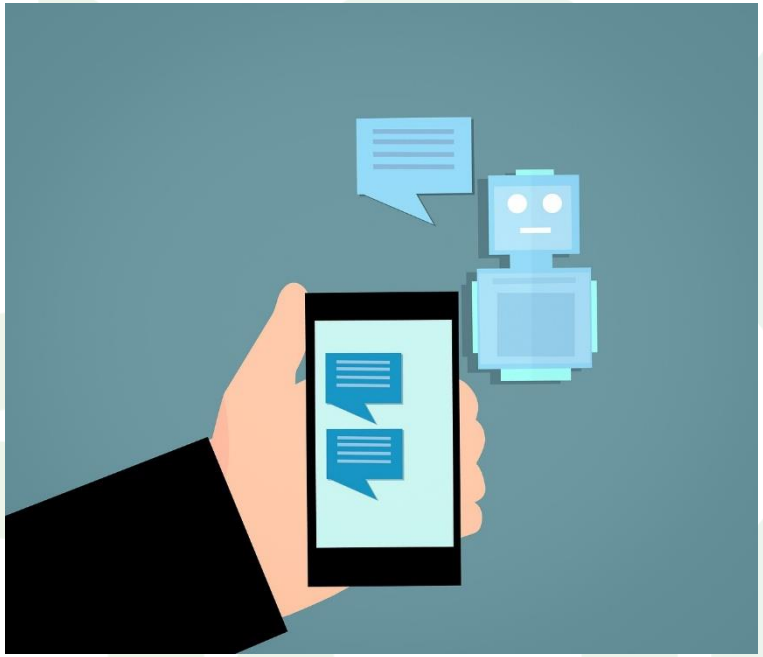


Imagen de mohamed Hassan en Pixabay

Encuadre jurídico

DERECHO FUNDAMENTAL (protección de datos y otros)

BIEN ECONÓMICO (Economía de los datos)

Problemáticas principales

DERECHOS FUNDAMENTALES (protección de datos y otros)

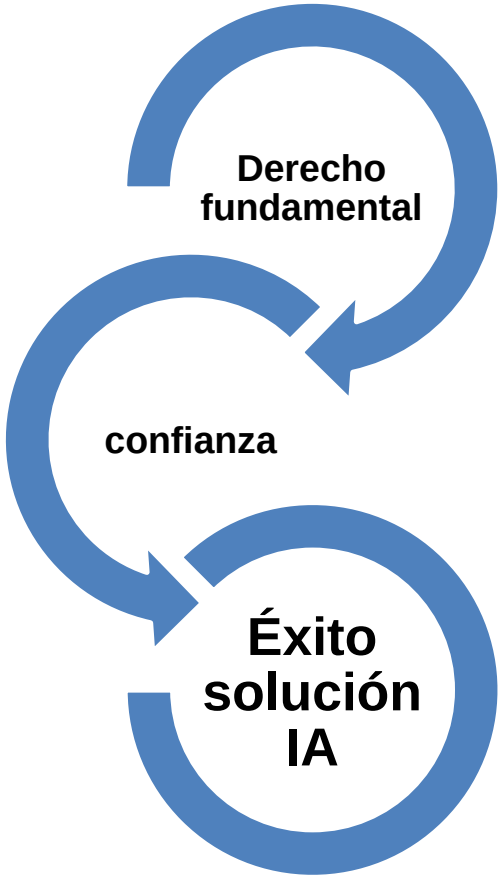
SEGURIDAD/ RESPONSABILIDAD (productos defectuosos..)

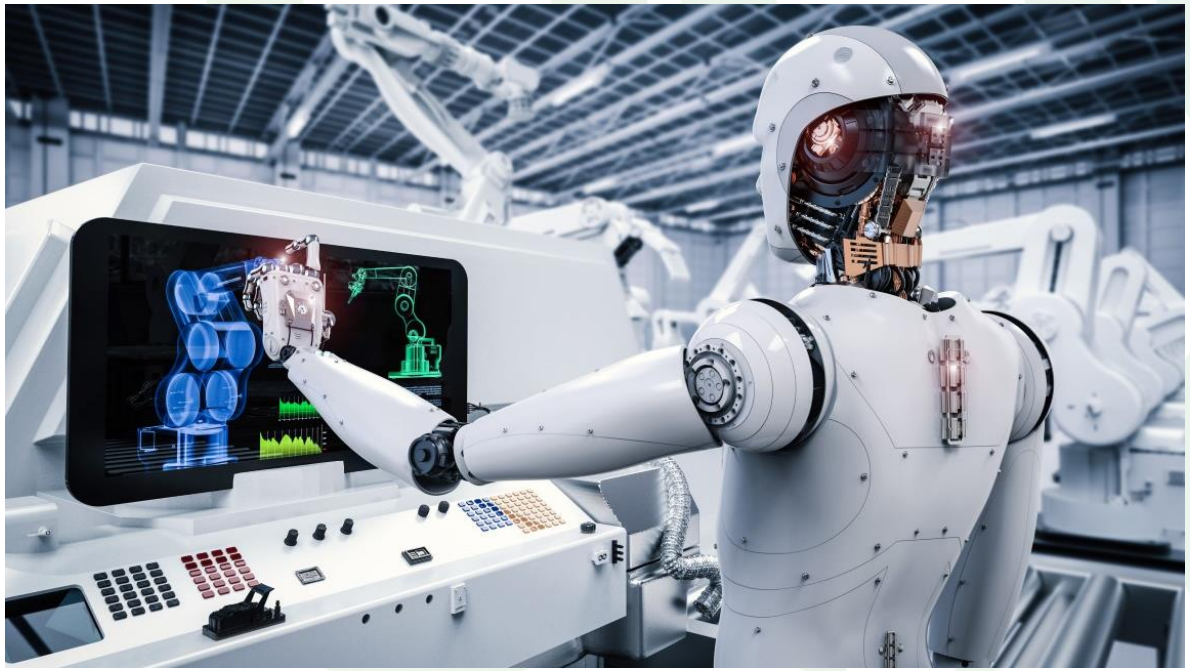
Parlamento Europeo *Civil liability regime for AI*

ISACA Barcelona Chapter

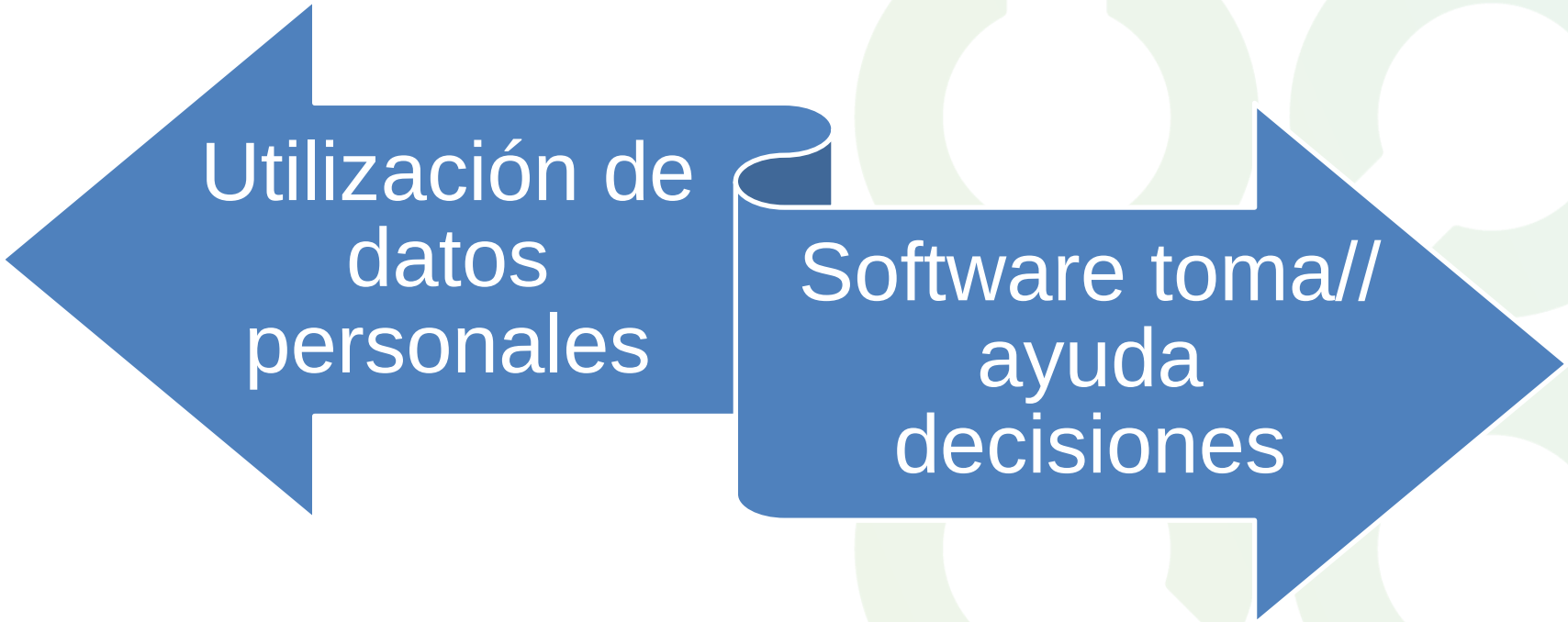
IA y Protección de datos

¿Por qué es importante la protección de datos en IA?





¿Cuándo aplica la normativa de protección de datos?



GOVERTIS Advisory Services

ISACA Barcelona Chapter

Ciclo de vida de un Sistema IA y tratamientos de datos personales

(AEPD *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, Febrero 2020).*

ISACA Barcelona Chapter

Principios de Protección de datos (art 5 RGPD)

- Licitud, lealtad y transparencia
- Limitación de la Finalidad
- Minimización de datos
- Exactitud
- Limitación del plazo de conservación
- Integridad y confidencialidad

ISACA
Barcelona Chapter

Evaluación de Impacto en Protección de Datos (EIPD)

¿Cuándo?

“el tratamiento entrañe un **alto riesgo** para los **derechos y libertades** de las personas físicas”

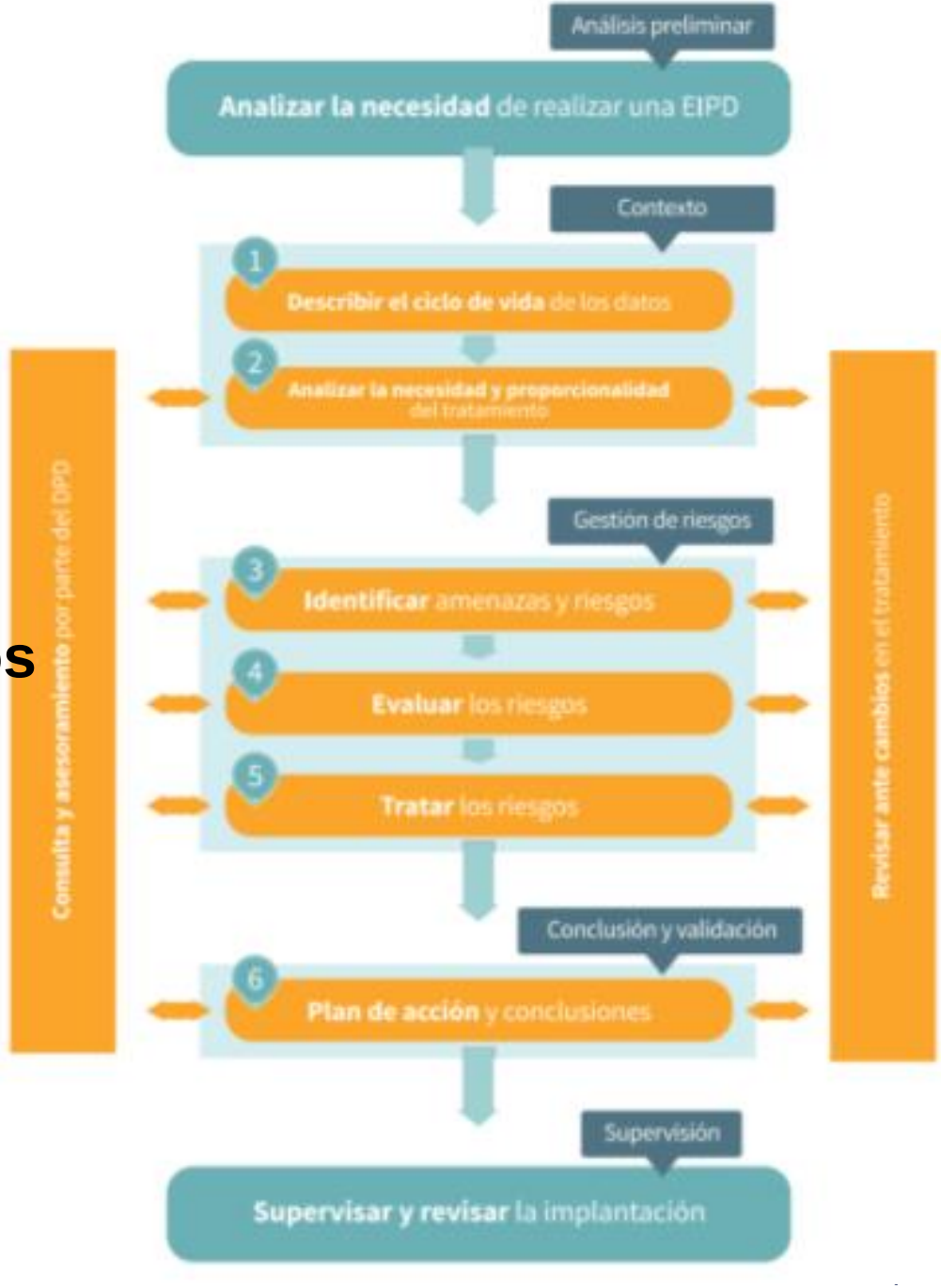
evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la **elaboración de perfiles**, y sobre cuya base se tomen **decisiones** que produzcan **efectos jurídicos** para las personas físicas o **que les afecten significativamente** de modo similar **Art 35.3 a)**

\+ Lista AEPD tratamientos sí necesitan EIPD

ISACA Barcelona Chapter

EIPD

- ✓ Evaluación **necesidad y proporcionalidad**
- ✓ Descripción operaciones de tratamiento
- ✓ Evaluación de los **riesgos** para los **derechos y libertades** de los interesados
- ✓ Medidas de seguridad: riesgo residual



AEPD Guía práctica para las EIPD

Auditoría protección de datos IA

AEPD: Es necesario realizar la auditoría para determinar la **adecuación** a las exigencias del **RGPD** y comprobar la **validez del tratamiento** basado en soluciones de IA.

- ✓ **Finalidades reales**
- ✓ Utilización de datos personales
- ✓ Elaboración de perfiles, decisiones automatizadas..
- ✓ Bases de legitimación
- ✓ Responsabilidades diferentes actores
- ✓ Deber de información y transparencia
- ✓ AARR, medidas de seguridad, EIPD, DPD
- ✓ Formación del RT (inferencias)
- ✓ Atención derechos ARSOPL
- ✓ Conservación: si supresión de oficio o anonimización

Estrategia digital Europea

Comunicación Una estrategia europea de datos, (COM) 2020 66 final

- situar los intereses de la persona en primer lugar
- volumen cada vez mayor de datos industriales no personales y de datos públicos en Europa
- modelo de referencia de una sociedad empoderada por los datos
- Estrategia para 2025

Libro Blanco IA - (COM) 2020 65 final

- formular **alternativas políticas** para facilitar un desarrollo de la IA seguro y fiable en Europa.

(COMUNICACIÓN estrategia sobre *Inteligencia artificial para Europa* [COM(**2018**) 237 final)

Libro Blanco IA

- **Comunicación** *Generar confianza en la IA centrada en el ser humano* COM(2019) 168
- **Directrices éticas** elaboradas por el **grupo de expertos de alto nivel sobre la IA**.
- **Marco regulador:** mantener, **modificar** o nueva legislación.

Enfoque basado en el riesgo:

aplicación de IA de riesgo elevado

Libro Blanco IA

Aplicación de IA de riesgo elevado:

1. que la aplicación de IA se emplee en un **SECTOR** es previsible que existan riesgos significativos

+

2. la aplicación de IA se **UTILICE**, además, **de manera que puedan surgir riesgos significativos**

Puntos clave:

- **datos** de entrenamiento;
- Conservación de **datos** y registros de **datos;**
- información que debe facilitarse;
- solidez y exactitud;
- supervisión humana;
- requisitos específicos en el caso de determinadas aplicaciones de IA, como las empleadas para la identificación biométrica remota**.**

control objetivo previo de la conformidad

Libro Blanco IA

Aplicaciones de IA que NO se consideran de riesgo elevado:

sistema de etiquetado voluntario (etiqueta de calidad)

Gobernanza:

estructura de gobernanza europea:
marco para la cooperación de las autoridades **nacionales** competentes

GOVERTIS Advisory Services

ISACA Barcelona Chapter

¡MUCHAS GRACIAS!

@Mlozac

GOVERTIS Advisory Services

ISACA Barcelona Chapter

ISACA®

Barcelona Chapter