# ¿Árbol o flotador?

## Evolución del marco regulatorio y los medios de cumplimiento

Eusko Jaurlaritzaren Informatika Elkartea

Sociedad Informática del Gobierno Vasco

# Contenido del documento

Presentación

Marco regulatorio

Medidas para el cumplimiento

El futuro

# Agustín Moyano Díaz

Responsable de Seguridad Corporativa de EJIE

Ingeniero Informático

Director de Seguridad especializado en Infraestructuras Críticas y Estratégicas, habilitado por el Ministerio del Interior

Perito Judicial en Informática y Electrónica Forense.

Más de 20 años de experiencia en el sector tecnológico, centrado los últimos 15 en el mundo de la seguridad en sus múltiples vertientes (ciberseguridad, protección de servicios esenciales, compliance, sistemas de gestión, etc.)

# Somos EJIE

EJIE nace con el **propósito** de impulsar la digitalización del **Sector Público de Euskadi** y garantizar la continuidad de su infraestructura de **Tecnologías de la Información y Telecomunicaciones**.

Nuestra **misión** es ser el órgano gestor tecnológico del Gobierno Vasco que facilita la transformación digital de los servicios públicos mediante la gestión eficiente y sostenible de las tecnologías de la información y la comunicación, **garantizando la calidad, seguridad y continuidad de los servicios** que los soportan..

## Nuestra visión

Contribuir a lograr la completa digitalización del Sector Público de Euskadi para que ofrezca servicios sencillos, seguros, eficaces, inclusivos y accesibles a toda la ciudadanía

# Somos EJIE (volumetría 2024)

## Gestión IT

Nº de despliegues de aplicaciones en producción: **7.377**

Nº de procesos batch gestionados: **740.452**

Nº de Peticiones: **99.221**

* Nº de Incidencias: **416.720**

Nº de cambios: **13.015**

## Comunicaciones

* Nº de edificios conectados **2.100**

Nº de extensiones telefónicas **45.647**

Nº de switches: **6.381**

Nº de antenas wifi **16.149**

## Puesto de trabajo

* Nº de puestos **284.101**

Nº de impresoras **18.430**

Nº de usuarios gestionados **190.881**

Nº de dispositivos móviles **18.709**

## Hosting

Nº de instancias de bbdd gestionadas: **2.290**

Nº de servidores de aplicaciones: **8.314**

Nº de aplicaciones albergadas: **3.881**

## Infraestructuras

* Volumen total de almacenamiento: **52.528,33 TB**

* Volumen total de MV: **14.179**

Volumen total de servidores físicos: **759**

* **220,5M€**

# Marco Regulatorio

*“El espíritu humano debe prevalecer sobre la tecnología”*

Albert Einstein

# Marco Regulatorio

## Protección de datos personales

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos.

# Marco Regulatorio

## Propiedad intelectual

RD 1/96 de propiedad intelectual

## LSSI/CE

Ley 34/2002, LSSI

Real Decreto-ley 13/2012

## Transparencia

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

# Marco Regulatorio

## Protección de Infraestructuras Críticas

Ley 8/2011

RD 704/2011

ORDEN de 7 de junio de 2024, del Vicelehendakari Primero y Consejero de Seguridad, por la que se regula la elaboración de planes de continuidad en materia de ciberseguridad para ciertas actividades sujetas a la norma vasca de autoprotección

# Marco Regulatorio

## Protección de las redes y sistemas de información

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

# Marco Regulatorio

## Administración, identificación y firma electrónica

Reglamento 910/2014 (eIDAS) de la UE

Esquema Nacional de Seguridad (RD 311/2022)

Ley 39/2015 de procedimiento administrativo

Ley 40/2015 de régimen jurídico del sector público

Ley 9/2017 de Contratos del Sector Público

# Marco Regulatorio

## Ciberamenazas e incidentes

REGLAMENTO (UE) 2025/38 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 19 de diciembre de 2024 por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad) .

## Servicios de seguridad gestionados

REGLAMENTO (UE) 2025/37 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 19 de diciembre de 2024 por el que se modifica el Reglamento (UE) 2019/881 en lo que se refiere a los servicios de seguridad gestionados.

# Marco Regulatorio

## Inteligencia Artificial

**REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).**

A nivel estatal: anteproyecto de ley para un uso ético, inclusivo y beneficioso de la Inteligencia Artificial.

ISO/IEC 42001 es una norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar de forma continua un sistema de gestión de inteligencia artificial (SGIA) en las organizaciones.

# Medidas para el cumplimiento

*“Todo parece imposible hasta que se hace”*

Nelson Mandela

# Medidas para el cumplimiento

## Reglamento IA

Reto: identificar todas las iniciativas relacionadas con IA

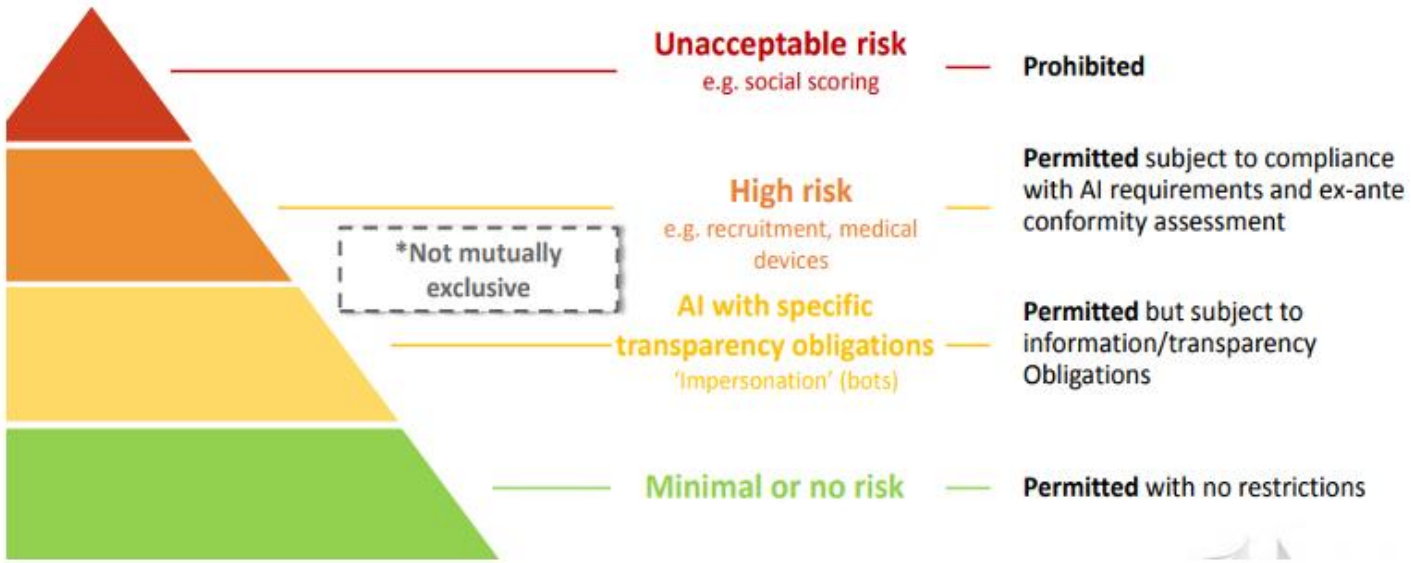
Reto: identificar el papel de la organización: ¿usuario? ¿distribuidor? ¿fabricante? ¿varios? ¿cambiante?

Reto: diferenciar IA de lo que no es IA…

Reto: asegurar nuestras obligaciones con nuestros clientes sin meternos en su terreno

# Medidas para el cumplimiento

## Clasificación de sistemas IA




**Prohibido**: Sistemas IA que desplieguen técnicas subliminales, social scoring, entre otros.

**Alto**: Sistemas de IA destinados a ser utilizados para la contratación o selección de personas físicas, destinados al reconocimiento de emociones, entre otros.

**Limitado**: Chatbots, deepfakes, entre otros.

**Bajo**: como los videojuegos con IA y los filtros de spam, entre otros.

# Medidas para el cumplimiento

## Principales roles del RIA

**Proveedor**: una persona física o autoridad pública que desarrolle (o para la que se desarrolle) un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado, o ponga en servicio el sistema de IA, con su propio nombre o marca

**Responsable del despliegue**: una persona física o jurídica o autoridad pública que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional

# Medidas para el cumplimiento

## Roles y obligaciones del RIA

| Proveedor | Responsable del despliegue | Importador | Distribuidor | Fabricante | Representante autorizado |
|---|---|---|---|---|---|
| Cumplimiento de los requisitos | Medidas para asegurar que el sistema se utiliza conforme a instrucciones | Asegurarse de que se hizo evaluación de conformidad, documentación, marcado CE | Verificación marcado CE | Se convierten en proveedores si ponen un sistema bajo su nombre | Podrán hacer lo que les asigne el proveedor |
| Mostrar dirección de contacto | Nombrar supervisor humano | | Avisar a proveedor si hay no conformidad | | Verificar declaración de conformidad |
| Sistema de gestión de calidad | Asegurar datos de entrada relevantes | Asignación de representante | Cooperar/informar | | Mantener contacto del proveedor |
| Mantener la documentación | Monitorizar la operación del sistema. Alertar | Notificación de deficiencias: falta de cumplimiento, falsificaciones, etc. | | | Cooperar/informar |
| Realizar/redactar evaluación de conformidad | Mantener los logs. Notificación para post-RBI | | | | |
| Marcado CE | Informar a trabajadores | Mantener certificado | | | |
| Registro del sistema | FRIA | Cooperar/informar | | | |

# Medidas para el cumplimiento

## Iniciativas IA

Extracción de datos de formularios y validación

Asistente virtual soporte Nivel 1

Análisis y estudio de directrices estratégicas

Análisis de documentación de candidatos

Tramitación automatizada de sanciones

Generación automática de catalogación de publicaciones

Análisis de la calidad del dato aportado

# El futuro

*“Me interesa el futuro porque es el sitio donde voy a pasar el resto de mi vida”*

Woody Allen

# El futuro

Securizar los datos que alimentan y que genera la IA

Gestión de identidades de máquinas y sistemas

Optimización de las tecnologías de Ciberseguridad

Tolerancia al fallo

- Premisa: TODOS hemos tenido (o vamos a tener) incidentes graves
- Ha muerto el "*zero tolerance for failure*"
- El heroísmo y la ocultación son enemigos de la resiliencia

**… y, ahora, hay que elegir…**

# ¿Árbol o flotador?

# Eskerrik asko zuen arretagatik
# Gracias por vuestra atención

Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Mediterráneo, 14 · 01010 Vitoria-Gasteiz · 01080 Vitoria-Gasteiz · Tel. 945 01 73 00* · Fax. 945 01 73 01 · www.ejie.eus