SOMMOS connecta

Cooperación empresarial y emprendimiento

www.sommos-connecta.com

FINANCIA: GENERALITAT VALENCIANA · IVACE+i INSTITUTO VALENCIANO DE COMPETITIVIDAD E INNOVACIÓN

ORGANIZA: CEEI Centro Europeo de Empresas e Innovación de Valencia · AVALNET

PONENCIA: "LA REALIDAD DE LOS RIESGOS A LOS QUE SE EXPONEN LAS EMPRESAS QUE IMPLEMENTAN IA"

Ricard Martínez

Cátedra de privacidad y Transformación Digital Microsoft-Universitat de Valencia

"Gobernanza de datos retos y riesgos para la implantación dela IA en las organizaciones"

Ricard Martínez Martínez

Director de la Cátedra de privacidad y Transformación Digital Microsoft-Universitat de Valencia

Càtedra Microsoft
Universitat de València
Privacitat &
Transformació Digital

IA FIABLE
retos técnicos, éticos, legales, culturales y socio-económicos

MINISTERIO DE CIENCIA E INNOVACIÓN
AGENCIA ESTATAL DE INVESTIGACIÓN

Ayuda RED2022-134315-T financiada por MCIN/AEI /10.13039/501100011033

Estrategia digital UE

1. Inteligencia artificial
2. Estrategia europea de datos
3. Estrategia industrial europea
4. Informática de alto rendimiento
5. Ley de Mercados Digitales
6. Ley de Servicios Digitales
7. Ciberseguridad
8. Capacidades digitales
9. Conectividad
10. Identidad Digital Europea

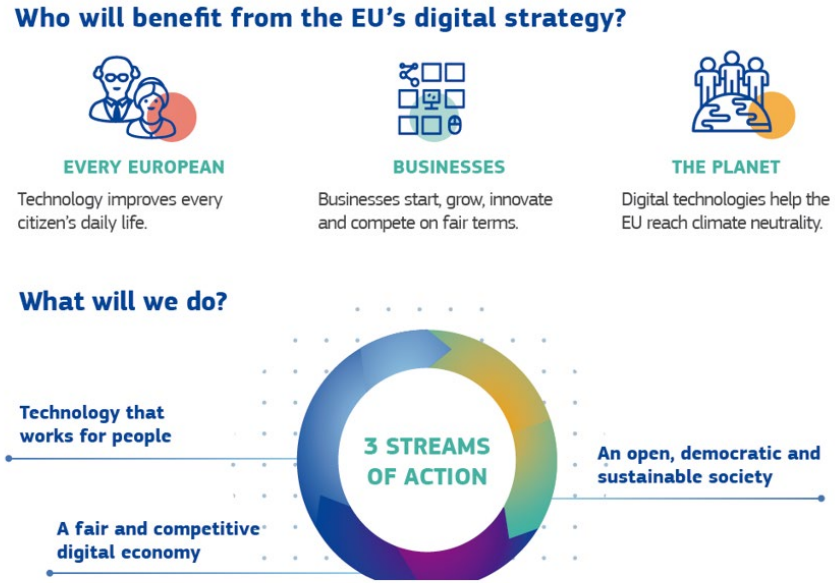


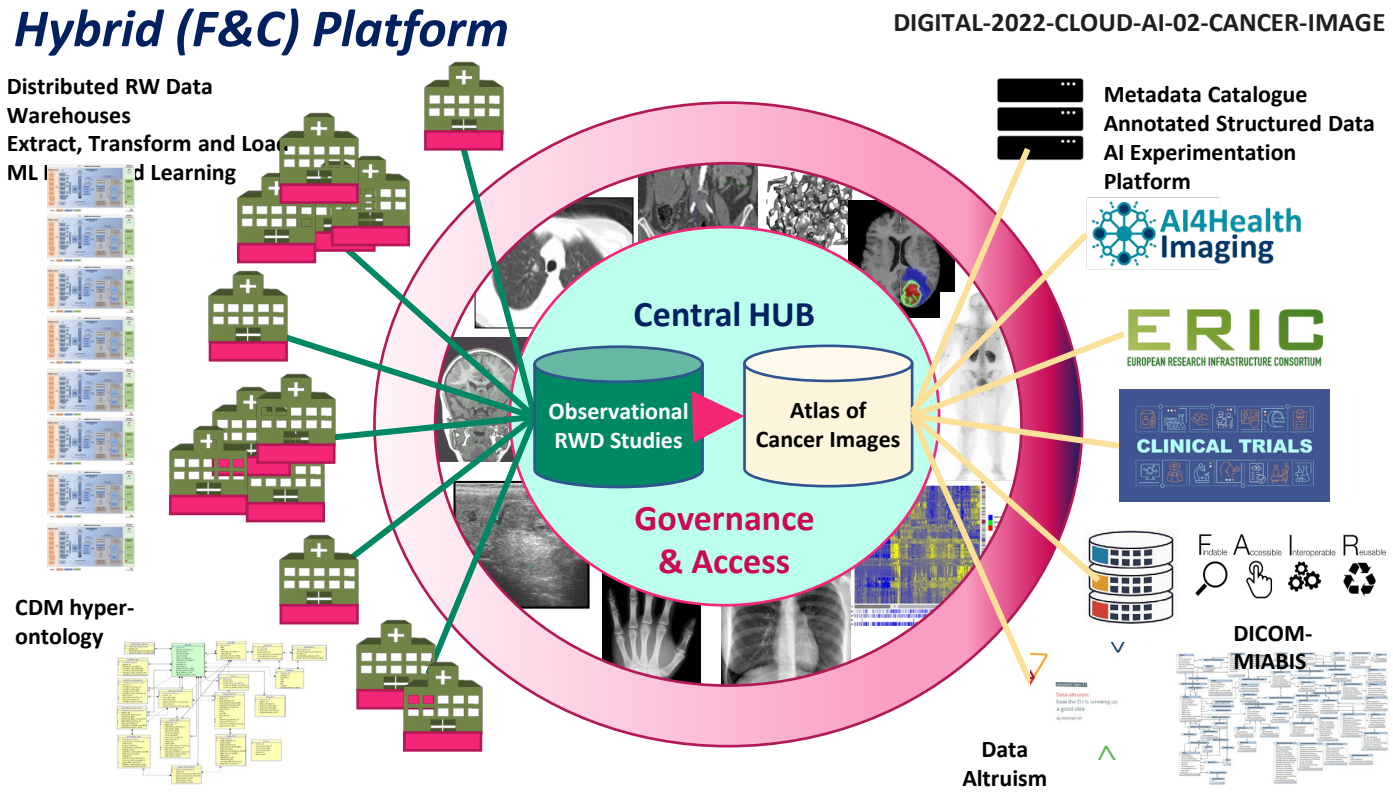
Figura 17. Shaping Europe's digital future. Fuente Comisión Europea[35]

Figura 18. Estrategia Europea de Datos. Cifras previstas para 2025. Fuente Comisión Europea[36]

Complejidad en los sistemas de información

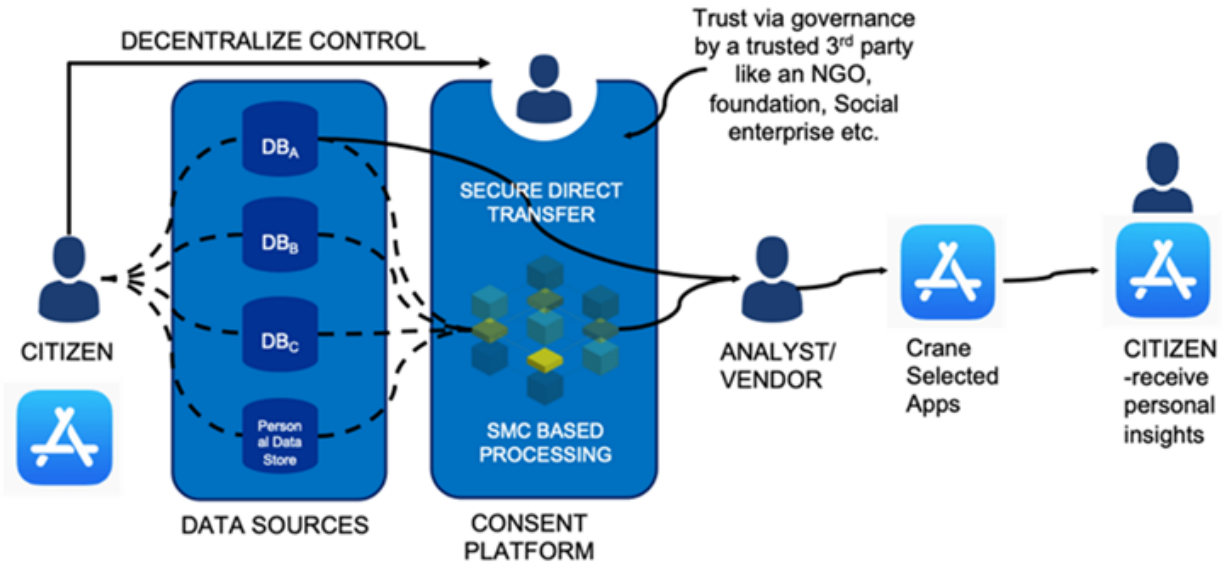
EUCAIM

Càtedra Microsoft Universitat de València Privacitat & Transformació Digital

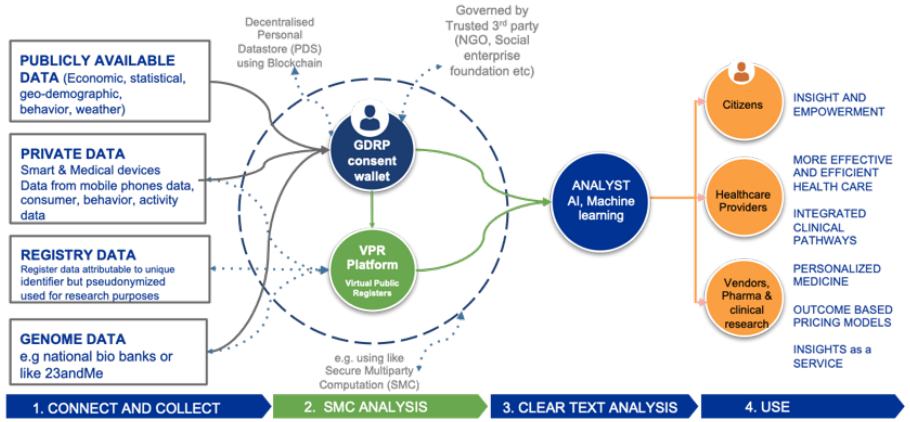


Empoderamiento de usuario

User consent wallet and insights

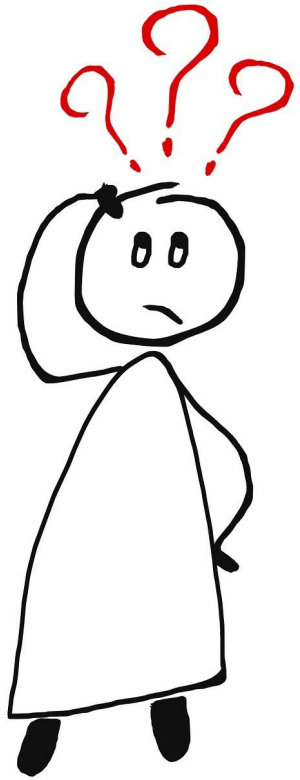


CRANE eco-system concept for a secure public-private virtual data lake platform



CRANE eco-system concept for a secure public-private virtual data lake platform

Cumplimiento normativo: el compliance como filosofía.



- Ética de los derechos
  - ✓ ¿Hay que romper cosas?
  - ✓ La dignidad y la autodeterminación individual.
  - ✓ Alterum non laedere.
- ¿En que nos ayudará la protección de datos?
  - ✓ Legitimación, veracidad, finalidad, proporcionalidad.
  - ✓ Análisis de riesgos.
  - ✓ Evaluación de impacto relativa a la protección de datos
  - ✓ Protección de datos desde el diseño y por defecto.
  - ✓ Transparencia.
  - ✓ Garantía de los derechos.

Inserción del cumplimiento normativo en los modelos y procesos

- Responsabilidad proactiva y gestión de las organizaciones

- Accountability

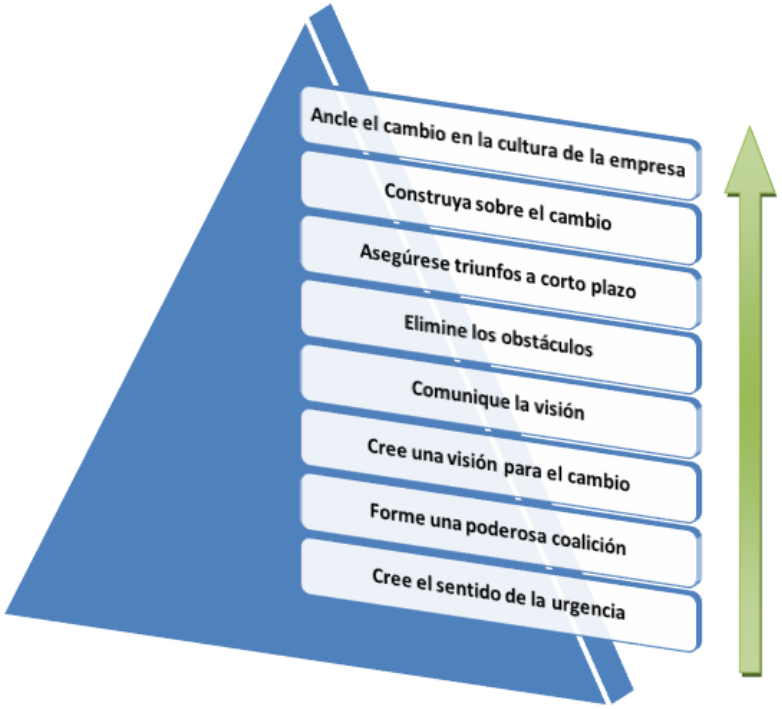
Càtedra Microsoft
Universitat de València
Privacitat & Transformació Digital

- Responsabilidad v. “responsabilidad por la diligencia en el cumplimiento”. (Caso BBVA).

> (74) Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

- Deber de diligencia en el diseño de las condiciones que garanticen el cumplimiento normativo cuya inobservancia genera responsabilidad.

- Gestionar el cambio



Estrategias de cumplimiento normativo desde el diseño.

INTELIGENCIA ARTIFICIAL DESDE EL DISEÑO. RETOS Y ESTRATEGIAS PARA EL CUMPLIMIENTO NORMATIVO

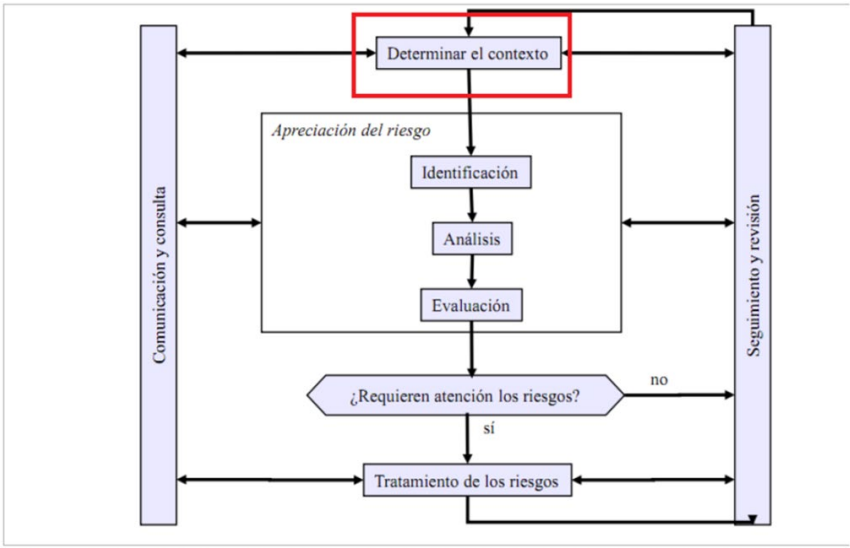
- Metodologías orientadas al riesgo

  - No existe el riesgo cero

Probabilidad					
	Máxima 4	4	8	12	16
	Significativa 3	3	6	9	12
	Limitada 2	2	4	6	8
	Despreciable 1	1	2	3	4
		Despreciable · 1	Limitada · 2	Significativa · 3	Máxima · 4

Bajo
Medio
Alto
Muy Alto

IMPACTO

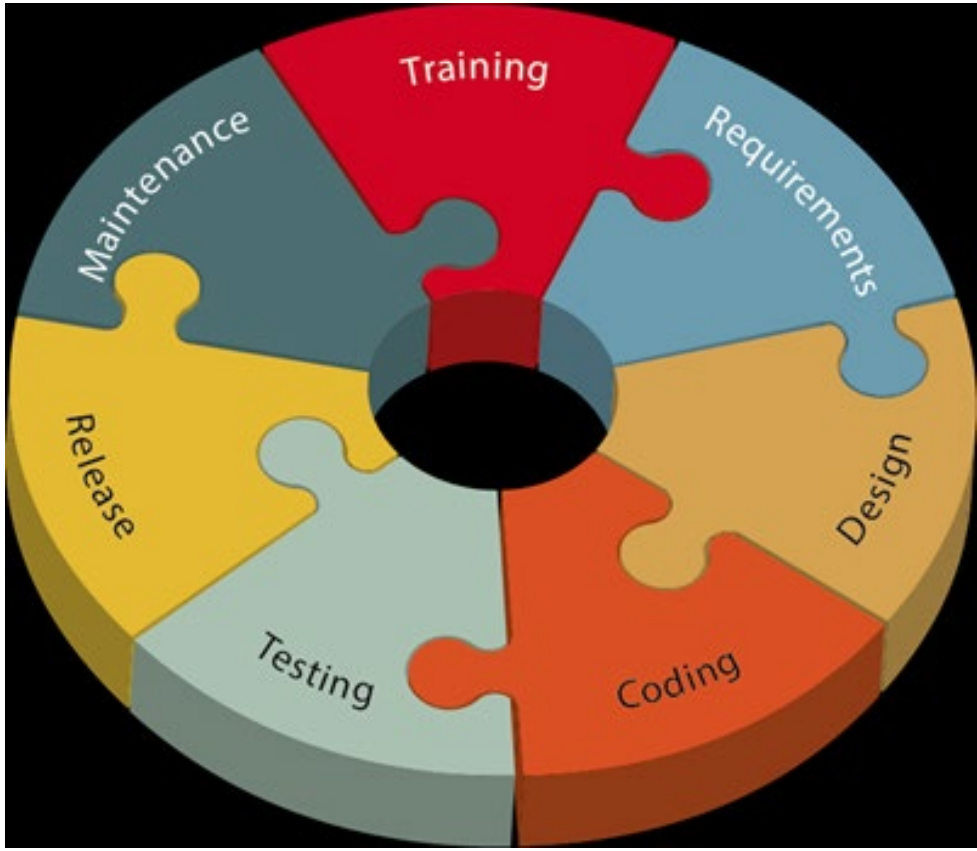


Norma UNE 71504:2008. Metodología de análisis y gestión de riesgos para los sistemas de información. AENOR.

- ¿Cómo debería funcionar?

Datatilsynet

The Norwegian Data Protection Authority has developed these guidelines to help organisations understand and comply with the requirement of data protection by design and by default in article 25 of the General Data Protection Regulation. We have cooperated with security professionals and software developers in public and private sector among others.



Artículo 4

Alfabetización en materia de IA

Los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas.

- Fgormar ética y jurídicamente

Training

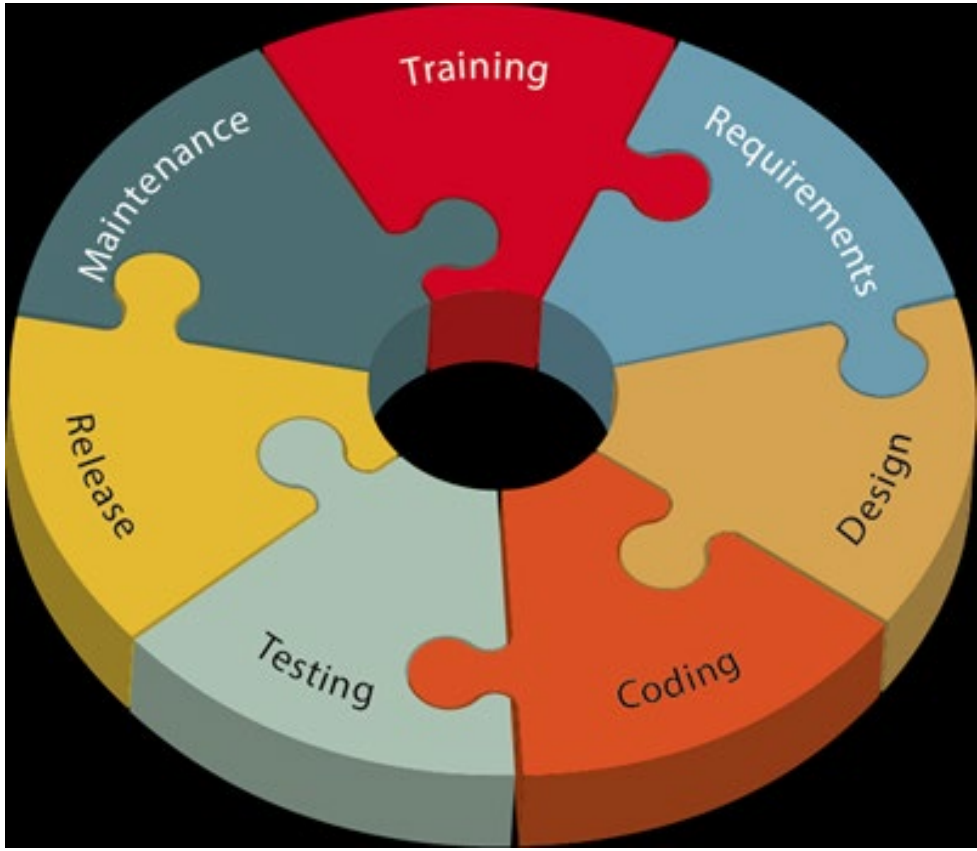
During this activity, the specific types of training that should be given are determined. To ensure that everyone in the organisation understands both the need for, and the risks associated with, data protection and security, the training needs to be structured.

- Formar no es el punto de llegada.
  - ✓ Empoderamiento previo de las personas implicadas.
  - ✓ Formar ética y jurídicamente al equipo.
    - ❖ Formación al órgano de gobierno.
    - ❖ Formación de cuadros directivos.
    - ❖ Formación al equipo IT.
    - ❖ Formación general.

- ¿Cómo debería funcionar?

Datatilsynet

The Norwegian Data Protection Authority has developed these guidelines to help organisations understand and comply with the requirement of data protection by design and by default in article 25 of the General Data Protection Regulation. We have cooperated with security professionals and software developers in public and private sector among others.



Desde RGPD

Datatilsynet

Software development with Data Protection by Design and by Default

The Norwegian Data Protection Authority has developed these guidelines to help organisations understand and comply with the requirement of data protection by design and by default in article 25 of the General Data Protection Regulation. We have cooperated with security professionals and software developers in public and private sector among others.

aepd agencia española protección datos

Guía de Privacidad desde el Diseño

Directrices 4/2019 relativas al artículo 25

Protección de datos desde el diseño y por defecto

Versión 2.0

Adoptadas el 20 de octubre de 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

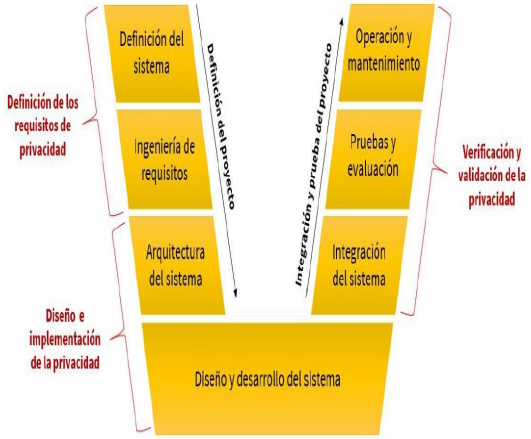


Figura 4 - Ingeniería de la privacidad [28]

Càtedra Microsoft
Universitat de València
Privacitat &
Transformació Digital

UNIÓN EUROPEA

EL PARLAMENTO EUROPEO — EL CONSEJO

Bruselas, 13 de junio de 2024
(OR. en)

2021/0106(COD)
LEX 2363

PE-CONS 24/1/24
REV 1

TELECOM 54
JAI 238
COPEN 69
CYBER 37
DATAPROTECT 76
EJUSTICE 11
COSI 16
IXIM 49
ENFOPOL 63
RELEX 180
MI 151
COMPET 154
CODEC 412

REGLAMENTO
DEL PARLAMENTO EUROPEO Y DEL CONSEJO
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)

Aproximación regulatoria de la Unión Europea

- Enfoque basado en la garantía del Estado de Derecho y los valores democráticos
  - ✓ Evaluación del impacto sobre los derechos fundamentales Evaluación del riesgo sistémico para la democracia y las sociedades europeas.
  - ✓ Principios éticos de AI: Evaluación de impacto ALTAI
  - ✓ Enfoques complementarios: DPIA en el GDPR
- Sanbox e investigación
- Enfoque orientado al producto:
  - ✓ Procesos de ingeniería basados en la ley
  - ✓ Normas para el diseño de sistemas de alto riesgo
  - ✓ Verificación de la conformidad
  - ✓ Certificación de la evaluación de la conformidad
- Normas para la IA generativa

- 1) «sistema de IA»: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;

¿Puedo?

Practicas prohibidas

- Técnicas de manipulación
- Personas o colectivos vulnerables

a) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;

b) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra;

- Profiling discriminatorio

c) la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para evaluar o clasificar a personas físicas o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:

i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente,

ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;

- Minority report
- No impide el uso con fines de investigación ex-post-facto

d) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva;

- Scrapping de imágenes

e) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;

- Biometría discriminatoria

g) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho;

- Sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

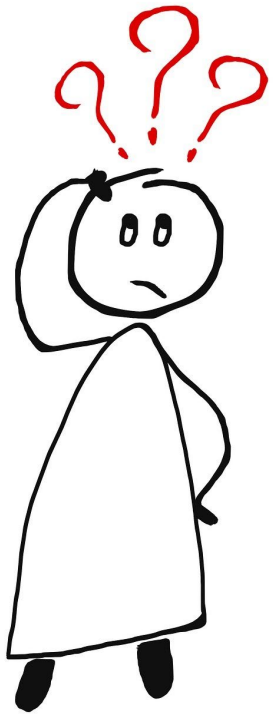
✓ i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,

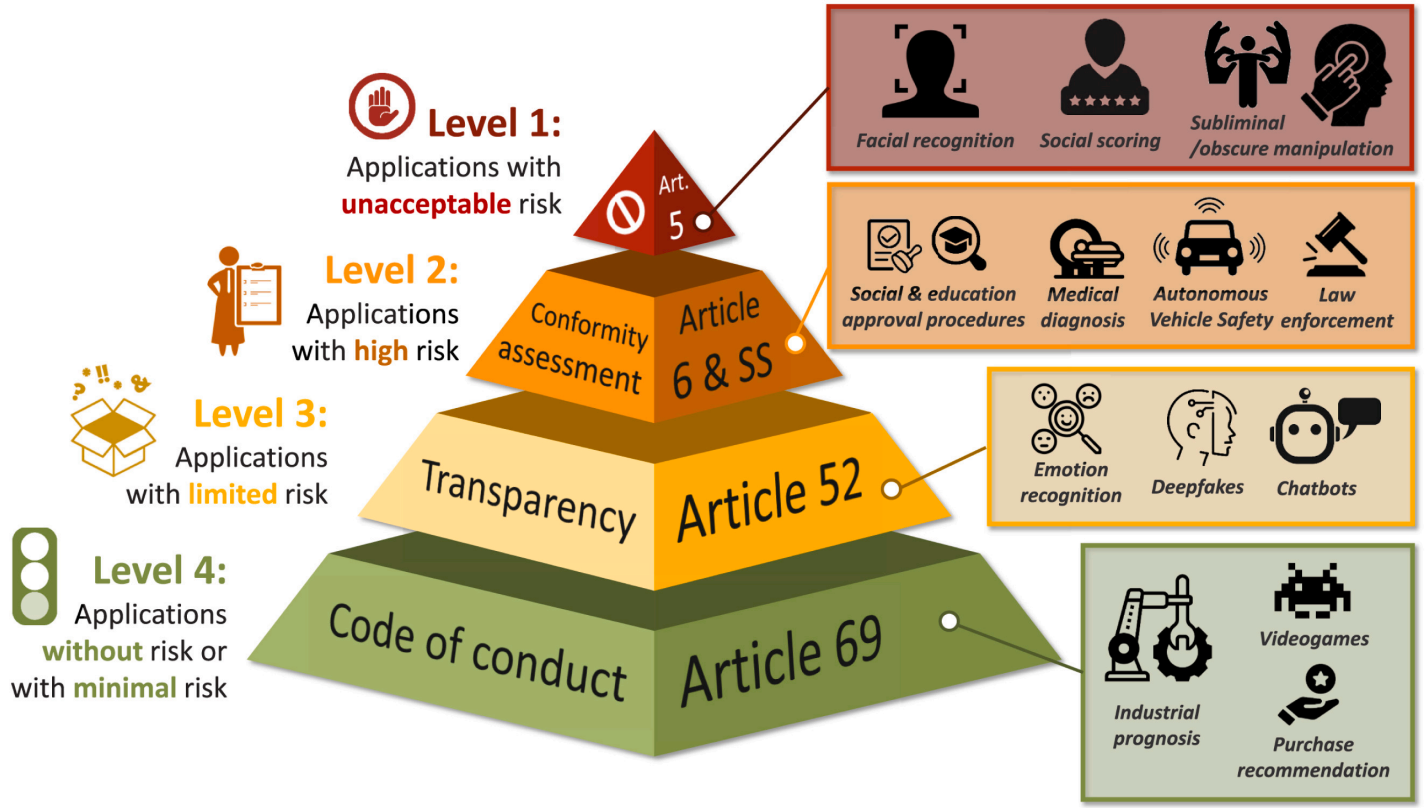
✓ ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista,

✓ iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

- ✓ Garantías adicionales
  - ❖ Aplica artículo 9 RGPD para tratamiento de datos biométricos con fines distintos de la garantía del cumplimiento del Derecho.
  - ❖ Juicio de proporcionalidad
  - ❖ Regulación específica por el derecho nacional
  - ❖ Concesión de autorización administrativa o judicial previa para uso de estos sistemas en tiempo real: excepción de urgencia
  - ❖ Notificación a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos
  - ❖ Informes anuales de la Comisión

¿Y si no esta prohibido?





- Fuente Natalia Díaz-Rodríguez, (et alii), Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation, Information Fusion, Volume 99, 023,https://doi.org/10.1016/j.inffus.2023.101896. (https://www.sciencedirect.com/science/article/pii/S1566253523002129)

Investigación

- (25) El presente Reglamento debe apoyar la innovación, respetar la libertad de ciencia y no socavar la actividad de investigación y desarrollo. Por consiguiente, es necesario excluir de su ámbito de aplicación los sistemas y modelos de IA desarrollados específicamente y puestos en servicio únicamente con fines de investigación y desarrollo científicos. Además, es necesario garantizar que el presente Reglamento no afecte de otro modo a la actividad de investigación y desarrollo científicos sobre sistemas o modelos de IA antes de su introducción en el mercado o su puesta en servicio. Por lo que se refiere a la actividad de investigación, prueba y desarrollo orientada a productos en relación con sistemas o modelos de IA, las disposiciones del presente Reglamento tampoco deben aplicarse antes de que dichos sistemas y modelos se pongan en servicio o se introduzcan en el mercado. Esa exclusión se entiende sin perjuicio de la obligación de cumplir el presente Reglamento cuando se introduzca en el mercado o se ponga en servicio como resultado de dicha actividad de investigación y desarrollo un sistema de IA que entre en el ámbito de aplicación del presente Reglamento, así como de la aplicación de disposiciones sobre espacios controlados de pruebas para la IA y pruebas en condiciones reales. Además, sin perjuicio de la exclusión de los sistemas de IA desarrollados específicamente y puestos en servicio únicamente con fines de investigación y desarrollo científicos, cualquier otro sistema de IA que pueda utilizarse para llevar a cabo cualquier actividad de investigación y desarrollo debe seguir estando sujeto a las disposiciones del presente Reglamento. En cualquier caso, toda actividad de investigación y desarrollo debe llevarse a cabo de conformidad con normas éticas y profesionales reconocidas para la investigación científica y con el Derecho aplicable de la Unión.

Alto riesgo

- Sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y
- que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I
- Listado de casos del Anexo III

Condiciones de desarrollo

- Artículo 9
- Sistema de gestión de riesgos

2. El sistema de gestión de riesgos ***se entenderá como*** un proceso iterativo continuo ***planificado y*** ejecutado durante todo el ciclo de vida de un sistema de IA de alto riesgo, que requerirá ***revisiones y*** actualizaciones sistemáticas periódicas. Constará de las siguientes etapas:

a) la determinación y el análisis de los riesgos conocidos y previsibles ***que el sistema de IA de alto riesgo pueda conllevar para la salud, la seguridad o los derechos fundamentales cuando el*** sistema de IA de alto riesgo ***se utilice de conformidad con su finalidad prevista;***

b) la estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible;

c) la evaluación de otros riesgos que podrían surgir, a partir del análisis de los datos recogidos con el sistema de vigilancia poscomercialización a que se refiere el artículo 72;

d) la adopción de medidas adecuadas ***y específicas*** de gestión de riesgos ***diseñadas para hacer frente a los riesgos detectados con arreglo a la letra a)***.

Artículo 10

Datos y gobernanza de datos

1. Los sistemas de IA de alto riesgo que utilizan técnicas que implican el entrenamiento de modelos de IA con datos se desarrollarán a partir de conjuntos de datos de entrenamiento, validación y prueba que cumplan los criterios de calidad a que se refieren los apartados 2 a 5 ***siempre que se utilicen dichos conjuntos de datos***.

2. Los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de gobernanza y gestión de datos ***adecuadas para la finalidad prevista del sistema de IA de alto riesgo***. Dichas prácticas se centrarán, en particular, en lo siguiente:

   a) las decisiones pertinentes relativas al diseño;

   b) los procesos de recogida de datos y el origen de los datos y, en el caso de los datos personales, la finalidad original de la recogida de datos;

c) las operaciones de tratamiento oportunas para la preparación de los datos, como la anotación, el etiquetado, la depuración, ***la actualización,*** el enriquecimiento y la agregación;

d) la formulación de supuestos [redacted], en particular en lo que respecta a la información que se supone que miden y representan los datos;

f) el examen atendiendo a posibles sesgos ***que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones***;

g) medidas adecuadas para detectar, prevenir y reducir posibles sesgos detectados con arreglo a la letra f);

h) la detección de lagunas o deficiencias ***pertinentes*** en los datos ***que impidan el cumplimiento del presente Reglamento***, y la forma de subsanarlas.

3. Los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, ***suficientemente*** representativos ***y, en la mayor medida posible***, carecerán de errores y estarán completos ***habida cuenta de su finalidad prevista***. Asimismo, tendrán las propiedades estadísticas adecuadas, por ejemplo, cuando proceda, en lo que respecta a las personas o los grupos de personas en relación con los ***cuales*** está previsto que se utilice el sistema de IA de alto riesgo. Los conjuntos de datos podrán reunir esas características para cada conjunto de datos individualmente o para una combinación de estos.

- Pueden tratarse categorías especiales de datos para la corrección de sesgos:

✓ a) que el tratamiento de otros datos, como los sintéticos o los anonimizados, no permita efectuar de forma efectiva la detección y corrección de sesgos;

✓ b) que las categorías especiales de datos personales estén sujetas a limitaciones técnicas relativas a la reutilización de los datos personales y a medidas punteras en materia de seguridad y protección de la intimidad, incluida la seudonimización;

✓ c) que las categorías especiales de datos personales estén sujetas a medidas para garantizar que los datos personales tratados estén asegurados, protegidos y sujetos a garantías adecuadas, incluidos controles estrictos y documentación del acceso, a fin de evitar el uso indebido y garantizar que solo las personas autorizadas tengan acceso a dichos datos personales con obligaciones de confidencialidad adecuadas;

✓ d) que las categorías especiales de datos personales no se transmitan ni transfieran a terceros y que estos no puedan acceder de ningún otro modo a ellos;

✓ e) que las categorías especiales de datos personales se eliminen una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, si esta fecha es anterior;

✓ f) que los registros de las actividades de tratamiento con arreglo a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680 incluyan las razones por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no podía alcanzarse mediante el tratamiento de otros datos.

Artículo 11

Documentación técnica

1. La documentación técnica de un sistema de IA de alto riesgo se elaborará antes de s introducción en el mercado o puesta en servicio, y se mantendrá actualizada.

Artículo 12

Conservación de registros

1. Los sistemas de IA de alto riesgo ***permitirán técnicamente*** el registro automático de eventos («archivos de registro») ***a lo largo de todo su ciclo de vida***.

Artículo 13

Transparencia y comunicación de información a los ***responsables del despliegue***

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los ***responsables del despliegue*** interpreten y usen correctamente su información de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el proveedor ***y el responsable del despliegue*** cumplan las obligaciones oportunas previstas en la sección 3.

Artículo 14

Vigilancia humana

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas.

Artículo 15

Precisión, solidez y ciberseguridad

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera uniforme en esos sentidos durante todo su ciclo de vida.

Evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo

Càtedra Microsoft
Universitat de València
Privacitat & Transformació Digital

- 1. Antes de desplegar uno de los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, con excepción de los sistemas de IA de alto riesgo destinados a ser utilizados en el ámbito enumerado en el anexo III, punto 2, los responsables del despliegue que sean organismos de Derecho público, o entidades privadas que prestan servicios públicos, y los responsable del despliegue de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, letras b) y c), llevarán a cabo una evaluación del impacto que la utilización de dichos sistemas puede tener en los derechos fundamentales

✓ Excepción:

- 2.Infraestructuras críticas: Sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas, del tráfico rodado o del suministro de agua, gas, calefacción o electricidad

Ministry of the Interior and
Kingdom Relations

March 2022

Impact Assessment
Fundamental rights and algorithms

Ética de la Inteligencia Artificial.

Càtedra Microsoft
Universitat de València
Privacitat &
Transformació Digital

- Información disponible en https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción

agencia española protección datos

Requisitos para Auditorías de Tratamientos que incluyan IA

Auditoría de tratamientos que incorporan IA

El presente documento recoge una serie de controles específicos para la auditoría de tratamientos de datos personales que hacen uso de componentes basados en inteligencia artificial. Se ha elaborado siguiendo las recomendaciones incluidas en la guía sobre "Requisitos para Auditorias de tratamientos que incluyan IA" publicada por la Agencia Española de Protección de Datos[1]. Los controles identificados están concebidos para realizar un análisis de la adecuación del tratamiento de datos desde la perspectiva del RGPD.

		Control	SI	NO
ID	**A. IDENTIFICACIÓN Y TRANSPARENCIA DEL COMPONENTE**			
1	Inventario del componente IA auditado	¿En la documentación del proyecto ¿se ha identificado el componente IA con un nombre o código, identificación de la versión y la fecha de creación?	☐	☐
		¿Puede garantizarse mediante firma digital la integridad del código o cualquier archivo adicional de control de versiones?	☐	☐
		Existe y está documentado un histórico de versiones de la evolución del componente IA utilizado, incluyendo los parámetros usados en el entrenamiento del componente y todo aquello que asegure la trazabilidad de la evolución/cambios en el componente.	☐	☐
	Identificación de responsabilidades	La documentación del proyecto incluye datos identificativos y de contacto de la/s persona/s o institución/instituciones responsables de las etapas del ciclo de vida del componente IA auditado y/o, corresponsables, representantes del responsable y de los encargados.	☐	☐
		Se ha concretado el reparto de responsabilidades en los contratos asociados a las etapas de tratamiento.	☐	☐
		¿El tratamiento de los datos personales auditado ha sido inscrito en el Registro de Actividades de Tratamiento de los responsables respectivos, y/o los encargados'?	☐	☐
		¿En caso de ser necesario, se ha designado un Delegado de Protección de Datos y se ha comunicado a la autoridad de control?	☐	☐
	Transparencia	¿Se ha implantado un mecanismo para informar y se ha documentado el origen de los datos?	☐	☐
		¿Las características de los datos usados para entrenar al componente IA están identificadas, documentadas y adecuadamente justificadas?	☐	☐

Requisitos para Auditorías de Tratamientos que incluyan IA

Cátedra Microsoft
Universitat de València
Privacitat &
Transformació Digital

Dr. Ricard Martínez Martínez
Director de la Cátedra de privacidad y Transformación Digital Microsoft-Universitat de Valencia
ricard.martinez@uv.es
Twitter: @ricardmm; @catedramuv1
Linkedin: https://www.linkedin.com/in/ricardmartinezmartinez/