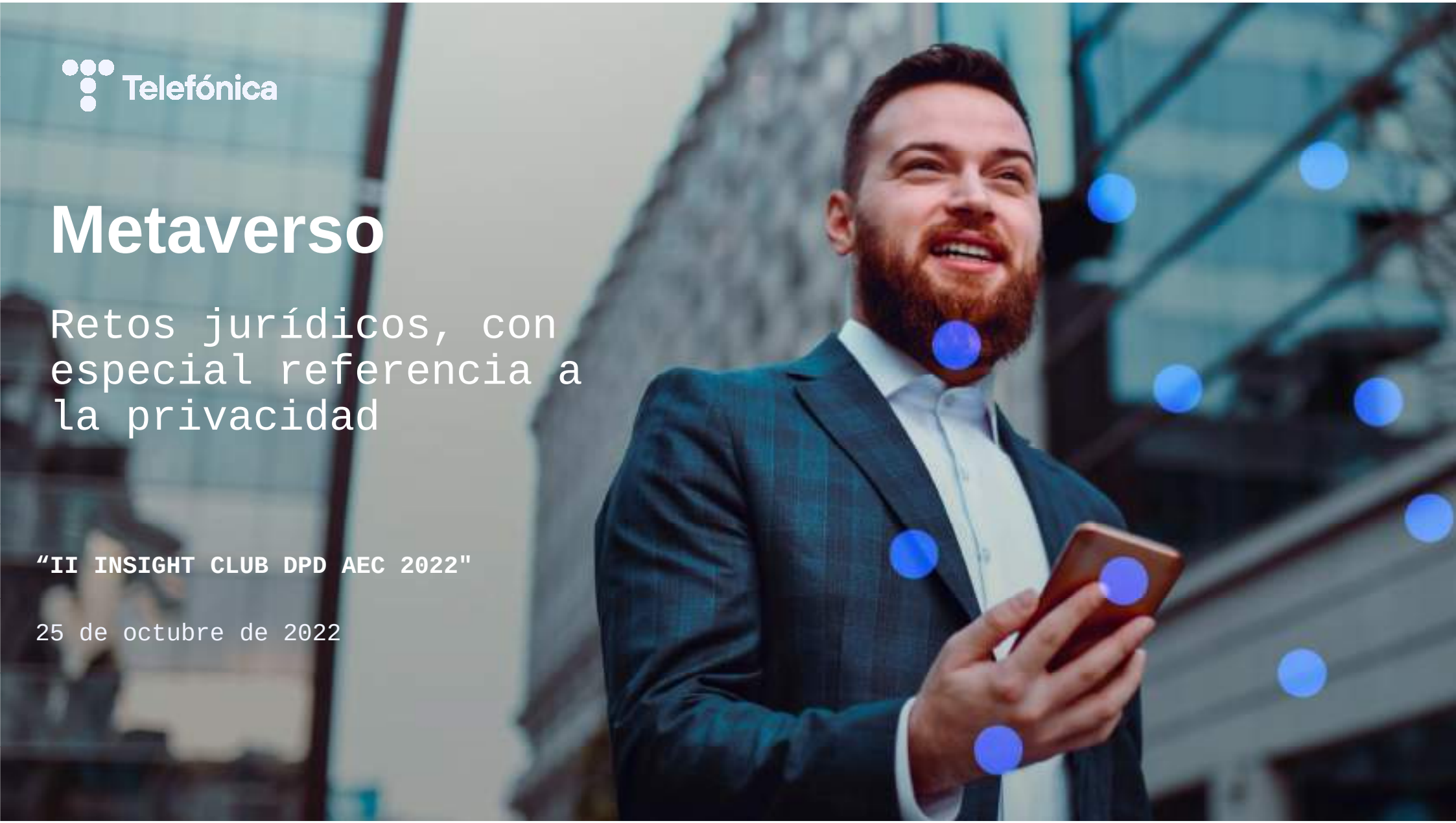
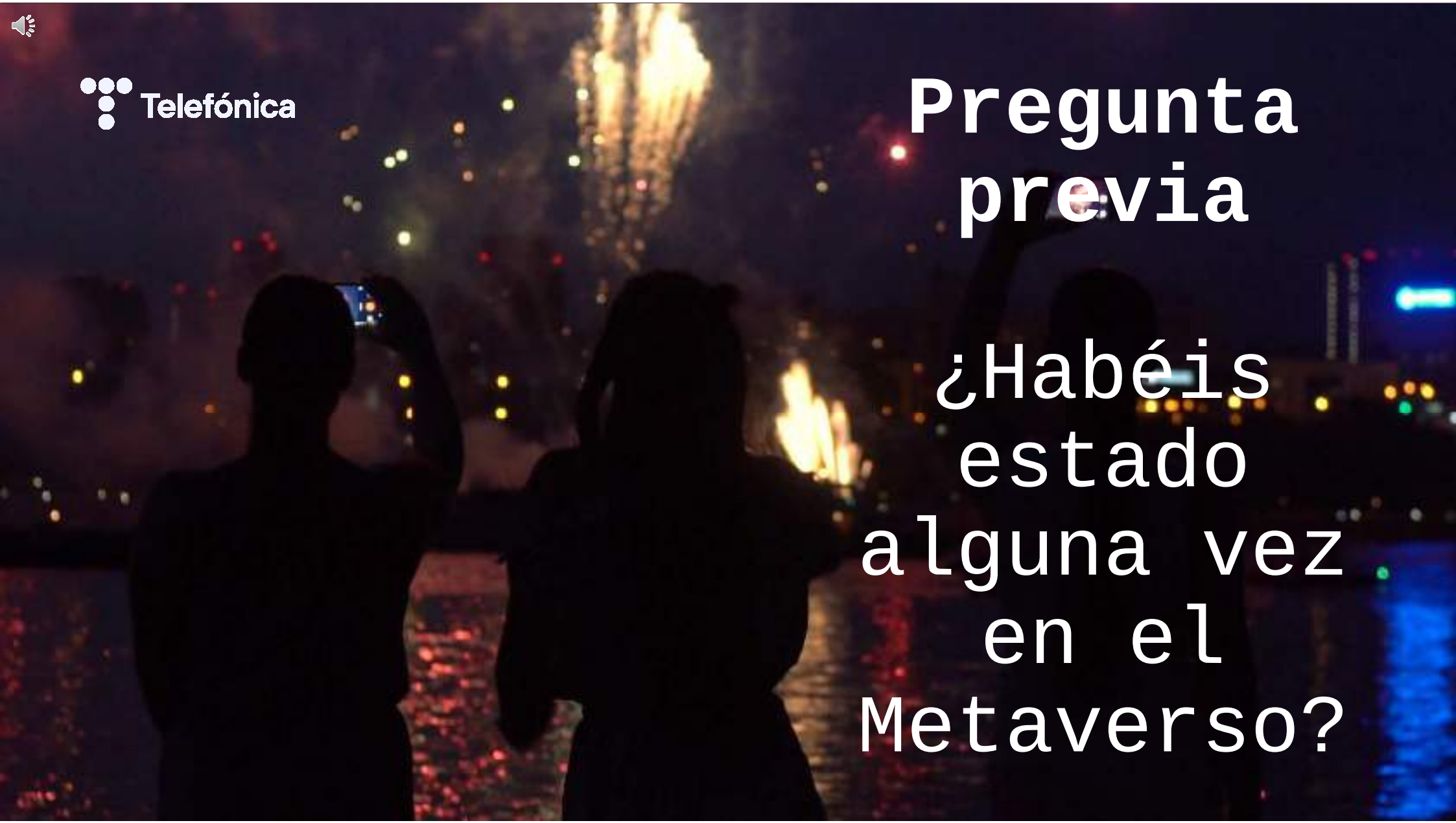


Metaverso

Retos jurídicos, con especial referencia a la privacidad

“II INSIGHT CLUB DPD AEC 2022"

25 de octubre de 2022


Telefónica
Pregunta previa
¿Habéis estado alguna vez en el Metaverso?

La tormenta perfecta

- Estamos viviendo una nueva era, no sólo ya con esta evolución de Internet que es el Metaverso, sino la revolución tecnológica más profunda de la historia de la humanidad con un impacto que se prevé cuatro veces mayor que el de la Revolución Industrial.
- Todo está ocurriendo a una velocidad asombrosa, con una pandemia que ha sido como una máquina del tiempo que ha acelerado aún más la digitalización. Y esto es irreversible.
- Nuestra vida digital se ha incrementado y hay una nueva generación Z (1994-2010) que pasa horas y horas consumiendo productos virtuales y son nativos digitales.
- Desaceleración de las RRSS y falta de innovación en dispositivos móviles.
- Desde una perspectiva tecnológica han confluido en un punto de madurez adecuado distintas tecnologías (dispositivos con mejores rendimientos, blockchain, criptomonedas, desarrollo de las gafas VR y AR, nuevos bienes digitales NFTs…).
- Mayor facilidad para el desarrollo - enfoque no code.
- Mayor conectividad que antes, y mayor vinculación con medios digitales, y acceso desde el móvil. Antes era PC sólo.

¿Qué es el Metaverso?

Concepto enormemente amplio que aún está en proceso de definición

… Como la web, pero en 3D”

… un amplio (y a menudo especulativo) cambio en la forma en que interactuamos con la tecnología”

…Mundos virtuales persistentes”

…Una propuesta de versión de Internet que incorpora entornos virtuales tridimensionales”

…Un mundo virtual tridimensional, en el que las personas pueden interactuar a través de un avatar especialmente en un juego de rol en línea”

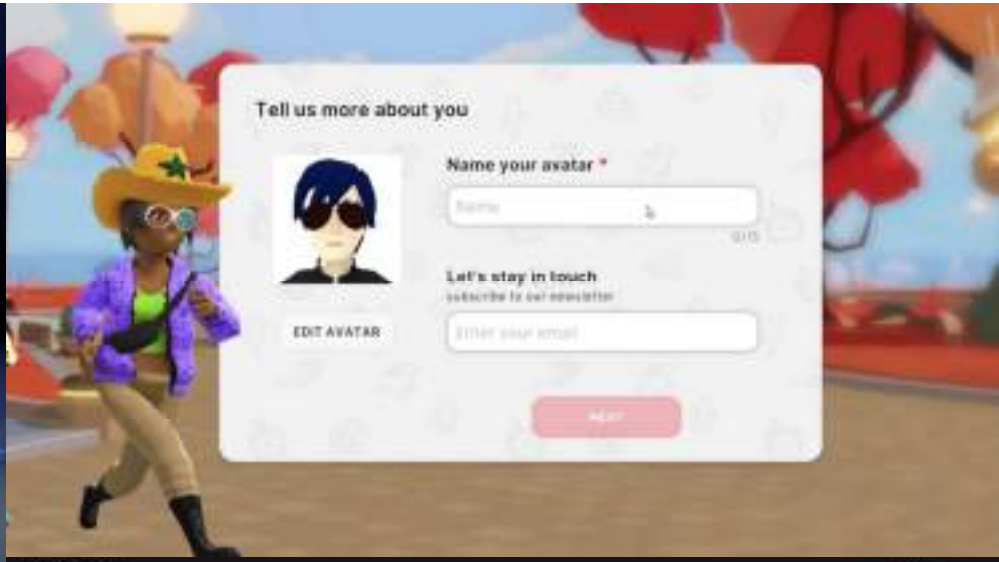
… el sucesor de Internet”

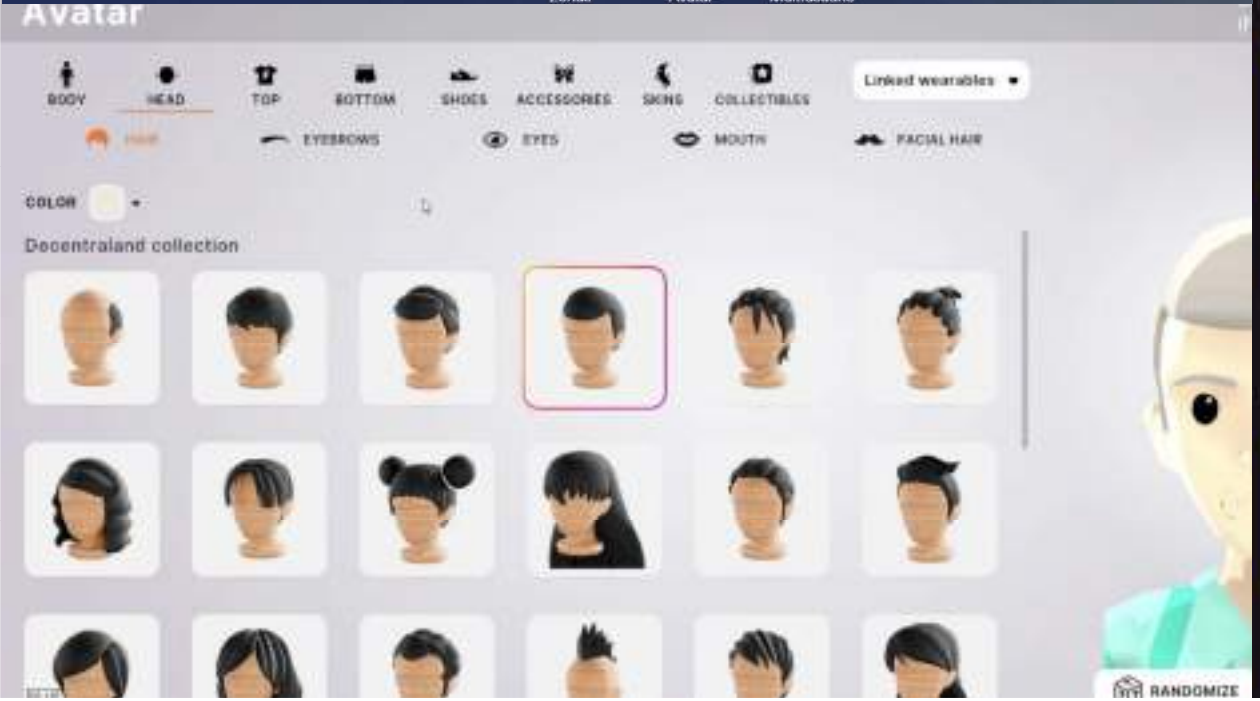
7 reglas del metaverso, que ayudan a definir lo que es (pero también lo que no es)

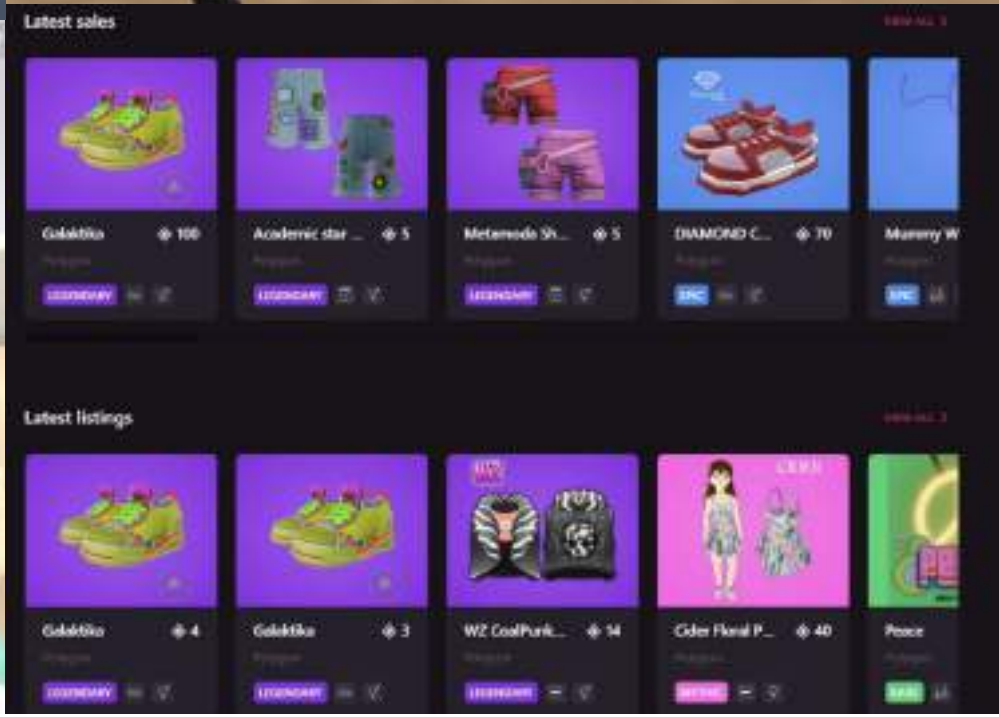
- Solo hay un metaverso
- El metaverso es abierto
- El metaverso es para todos
- Nadie controla el metaverso
- El metaverso es una red
- El metaverso es independiente del hardware
- El metaverso es Internet.

Tony Parisi 2021: The Seven Rules of the Metaverse. A framework for the coming immersive… by Tony Parisi | Metaverses | Medium)


Telefónica
Telefónica
Zonas
Avatar
Multiusuario


Tell us more about you
Name your avatar *
EDIT AVATAR
Let's stay in touch


Avatar
BODY
HEAD
TOP
BOTTOM
SHOES
ACCESSORIES
SKINS
COLLECTIBLES
Linked wearables
EYEBROWS
EYES
MOUTH
FACIAL HAIR
COLOR
Decentraland collection
RANDOMIZE


Latest sales
Latest listings

Metaverse
STANDARDS FORUM™

JOIN NEWS EVENTS MEMBERS CONTACT

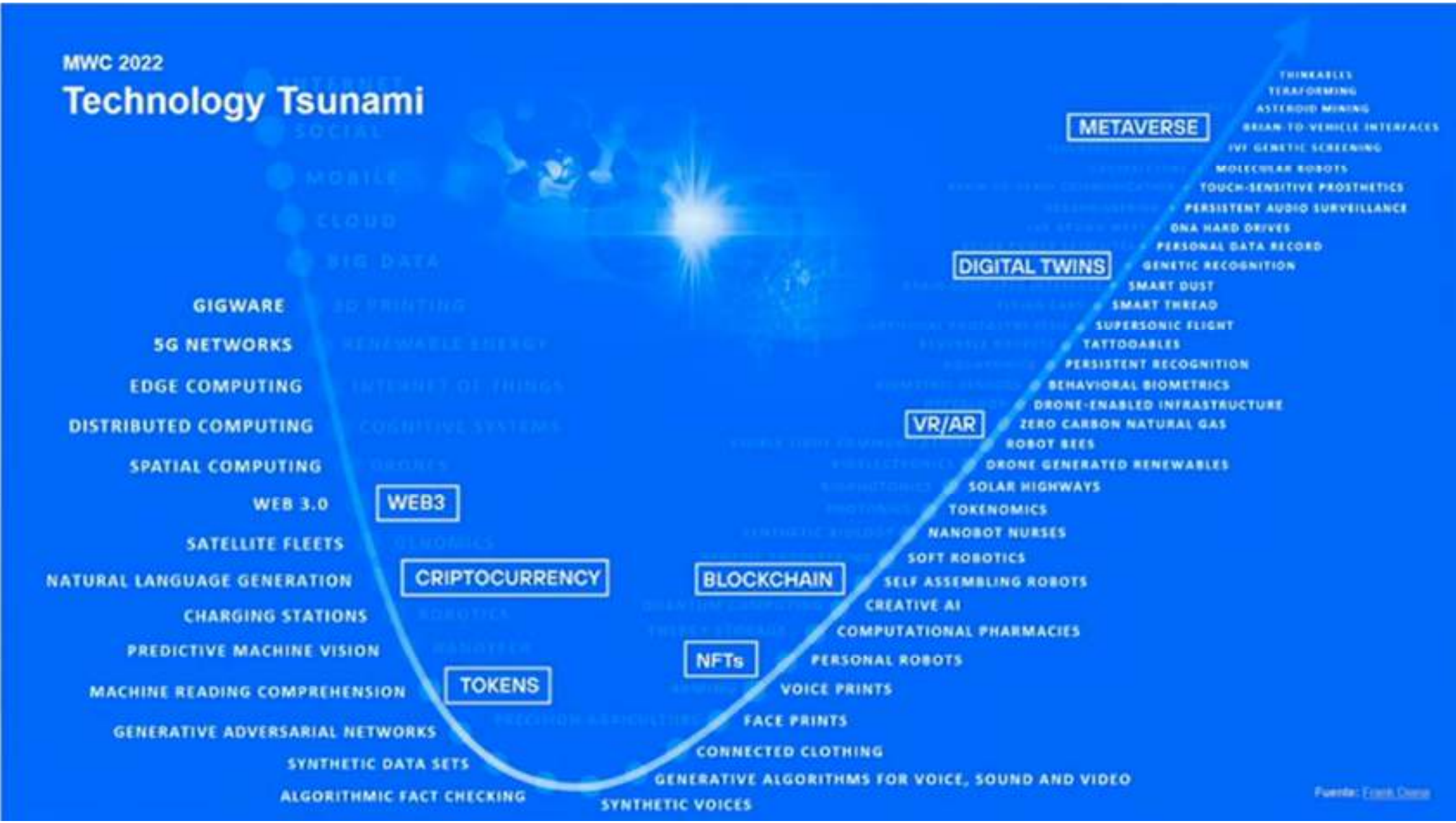
The Metaverse Standards Forum

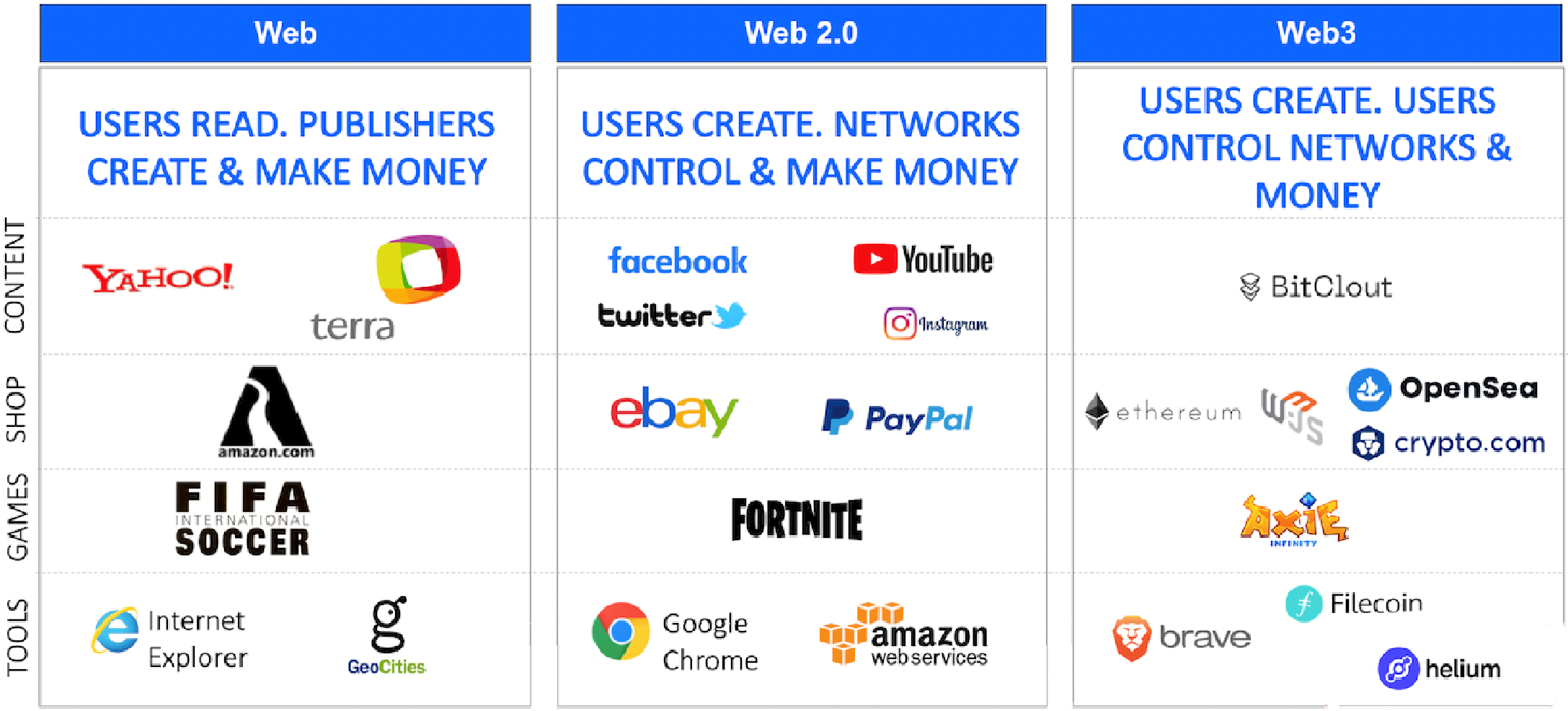
Where Leading Standards Organizations and Companies Cooperate to Foster Interoperability Standards for an Open Metaverse

Telefónica

Stack metaverso


El Backend del Metaverso
WEB3


MWC 2022
Technology Tsunami
GIGWARE
5G NETWORKS
EDGE COMPUTING
DISTRIBUTED COMPUTING
SPATIAL COMPUTING
WEB 3.0
SATELLITE FLEETS
NATURAL LANGUAGE GENERATION
CHARGING STATIONS
PREDICTIVE MACHINE VISION
MACHINE READING COMPREHENSION
GENERATIVE ADVERSARIAL NETWORKS
SYNTHETIC DATA SETS
ALGORITHMIC FACT CHECKING
WEB3
CRIPTOCURRENCY
TOKENS
BLOCKCHAIN
NFTs
SYNTHETIC VOICES
GENERATIVE ALGORITHMS FOR VOICE, SOUND AND VIDEO
CONNECTED CLOTHING
FACE PRINTS
VOICE PRINTS
PERSONAL ROBOTS
COMPUTATIONAL PHARMACIES
CREATIVE AI
SELF ASSEMBLING ROBOTS
SOFT ROBOTICS
NANOBOT NURSES
TOKENOMICS
SOLAR HIGHWAYS
DRONE GENERATED RENEWABLES
ROBOT BEES
ZERO CARBON NATURAL GAS
VR/AR
DRONE-ENABLED INFRASTRUCTURE
BEHAVIORAL BIOMETRICS
PERSISTENT RECOGNITION
TATTOOABLES
SUPERSONIC FLIGHT
SMART THREAD
SMART DUST
GENETIC RECOGNITION
DIGITAL TWINS
PERSONAL DATA RECORD
DNA HARD DRIVES
PERSISTENT AUDIO SURVEILLANCE
TOUCH-SENSITIVE PROSTHETICS
MOLECULAR ROBOTS
IVF GENETIC SCREENING
BRAIN-TO-VEHICLE INTERFACES
ASTEROID MINING
TERAFORMING
THINKABLES
METAVERSE



Juntas, estas tres evoluciones conducen naturalmente al metaverso: una nueva Internet con una experiencia mejorada y la posibilidad de difuminar las fronteras de poder y económicas entre empresas y usuarios

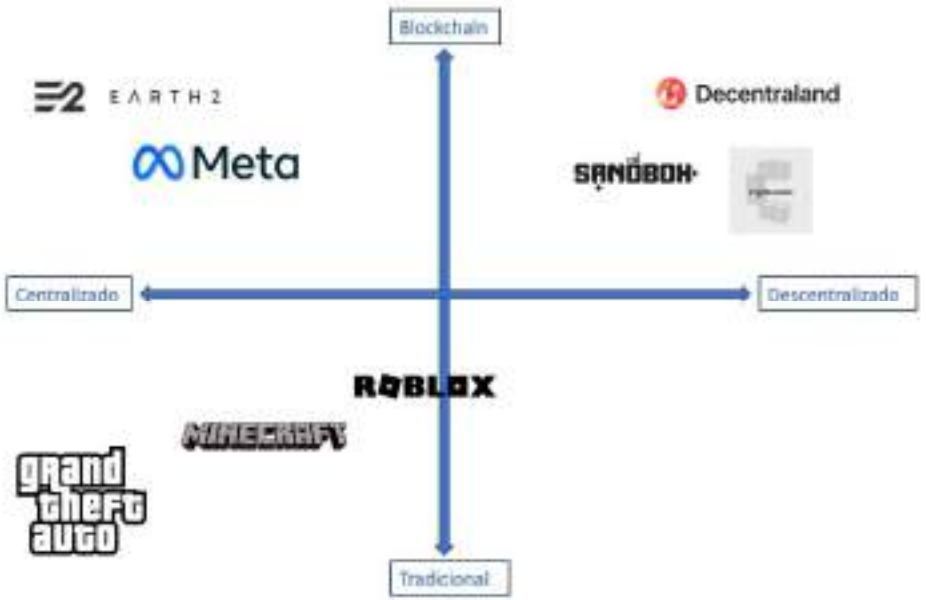
Telefónica

La identidad como elemento fundamental de Internet

- **Web 1.0:** Información no identifica a personas, salvos registros online (identidad falsa)
- **Web 2.0 (Identidad centralizada):** Personalidad social y el individuo se identifica de manera que la información y la publicidad empiezan a ser personalizadas y, en consecuencia, los tratamientos de información personal se convierten en su columna vertebral. Es la actual **economía de los datos.**
  - Pérdida de control y soberanía sobre los datos
  - Identidad centrada en el servidor de un tercero, que gestiona los datos de los usuarios en su propia infraestructura privada (RRSS, marketplace, etc)
  - Procesos de gestion de la identidad centralizados
  - Caos de contraseñas, problemas de seguridad, custodia y portabilidad de los datos
- **Web3 (Identidad descentralizada):** Gracias a tecnología Blockchain, la información ya no está centralizada en un solo operador (servidor) sino en los propios usuarios (cuyo equipo hace las veces de servidor) utilizando identificadores descentralizados (DID)
  - Información distribuida en diferentes nodos
  - Mayor capacidad de control sobre los datos y privacidad sobre

Clases de Metaverso

- **Metaverso blockchain**: El usuario se integra en un mundo virtual inmersivo con una económica virtual propia a través de micropagos con criptomonedas o NFT, lo que genera la posibilidad de conectar económica y comercialmente el mundo real con el virtual.
  - **Cerrados y Centralizados**: El control del mundo virtual está en una sola organización que tiene en su poder los datos de los usuarios y el control de su economía (Ej: Plataformas gaming, como Roblox, Fornite, Minecraft, o Horizon Worlds de Meta o Earth2)
  - **Abiertos y Descentralizados**: funcionan por medio de una organización autónoma descentralizada (DAO), su economía es autónoma y controlada por los usuarios (Ej: Decentraland, Sandbox)

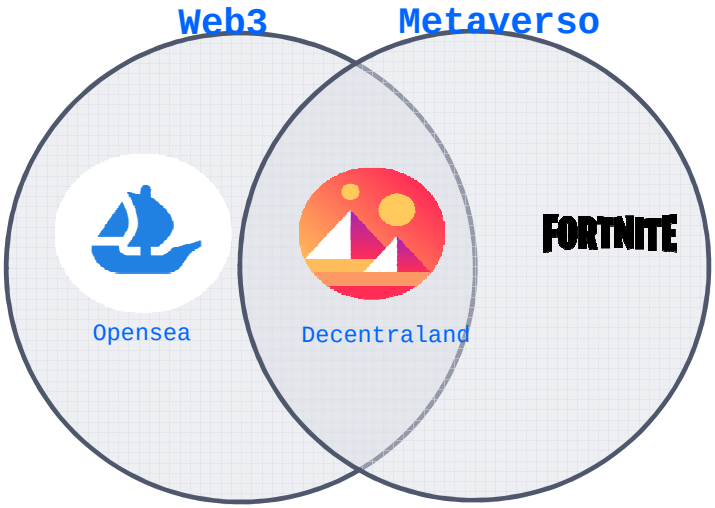


Es probable que ambas coexistan, pero las **redes descentralizadas** parecen tener **incentivos más atractivos para los creadores y emprendedores** y, además pueden servir para **resolver los problemas de privacidad** de los modelos centralizados, pero que al mismo tiempo generan **tensiones entre blockchain y la normativa de protección de datos**

Metaverso descentralizado: ¿Quién es el responsable?

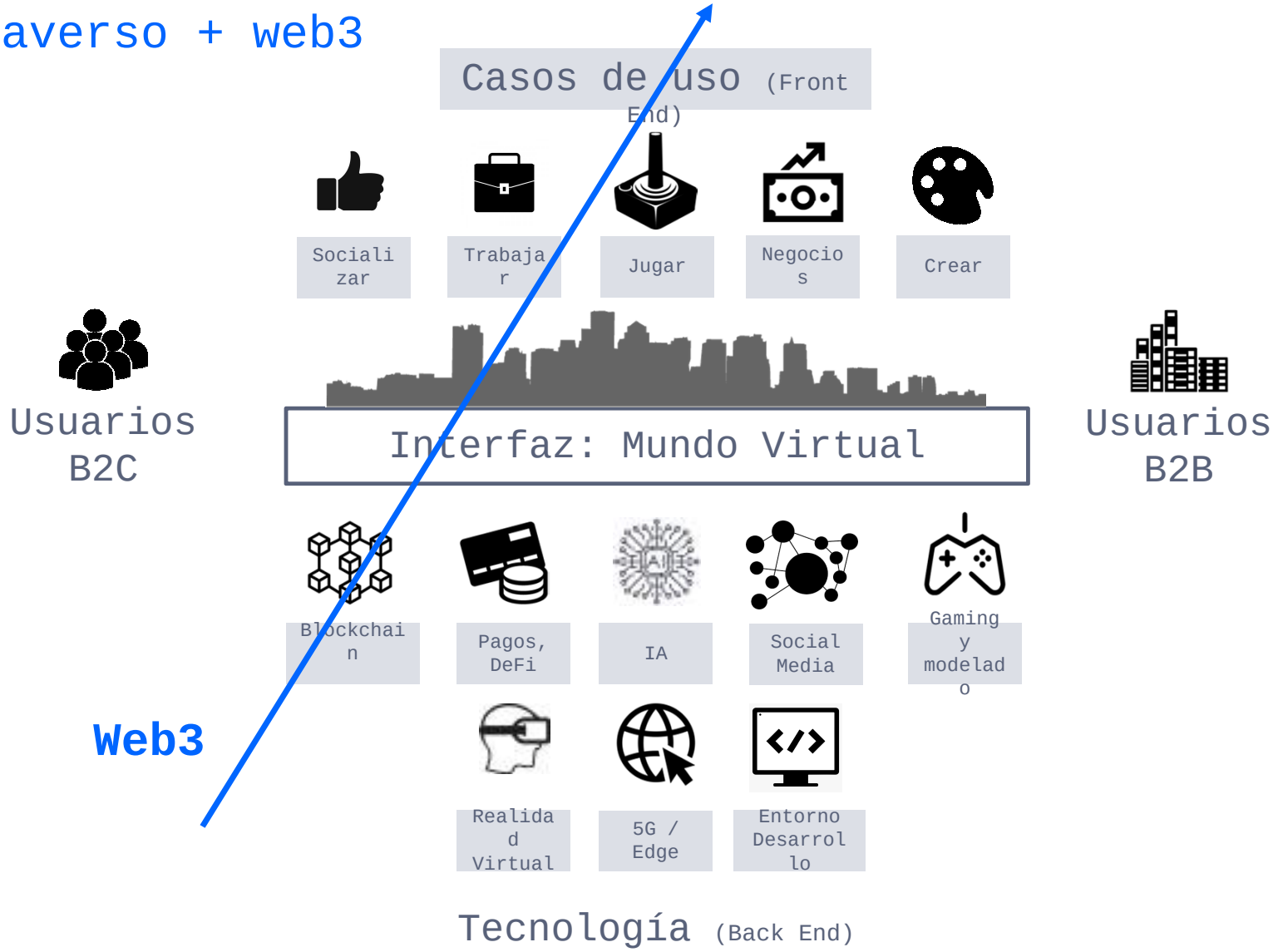
- En los **metaversos descentralizados** construidos en blockchain **no existe una autoridad a la que pueda exigirse el cumplimiento de determinadas normas, puesto que son plataformas descentralizadas gobernadas por DAOS** donde los TyC que rigen es el **protocolo diseñado en el código de programación con reglas ejecutadas automáticamente**.
- ¿posibilidad de desplazar al humano en el proceso de aplicación de la norma y del derecho, y sustituirlo por algoritmos que tomen las decisiones en un entorno virtual?
- ¿Esto significa que lo único que puede hacerse es poner límites a esos protocolos para que cumplan con las normativas?
- La **tecnología blockchain** nos trae varios **retos en materia de privacidad** por su **inmutabilidad** y por encontrase la **información distribuida en servidores** y **sin un intermediario claro que actúe como responsable del tratamiento** con capacidad para determinar las finalidades y medios del tratamiento.
- Blockchain se trata sólo de una tecnología, un programa, una aplicación, pero no es una empresa, ni una institución, ni una organización. **Blockchain no pertenece a nadie, ni nadie es responsable de blockchain**. Es algo que van formando de forma

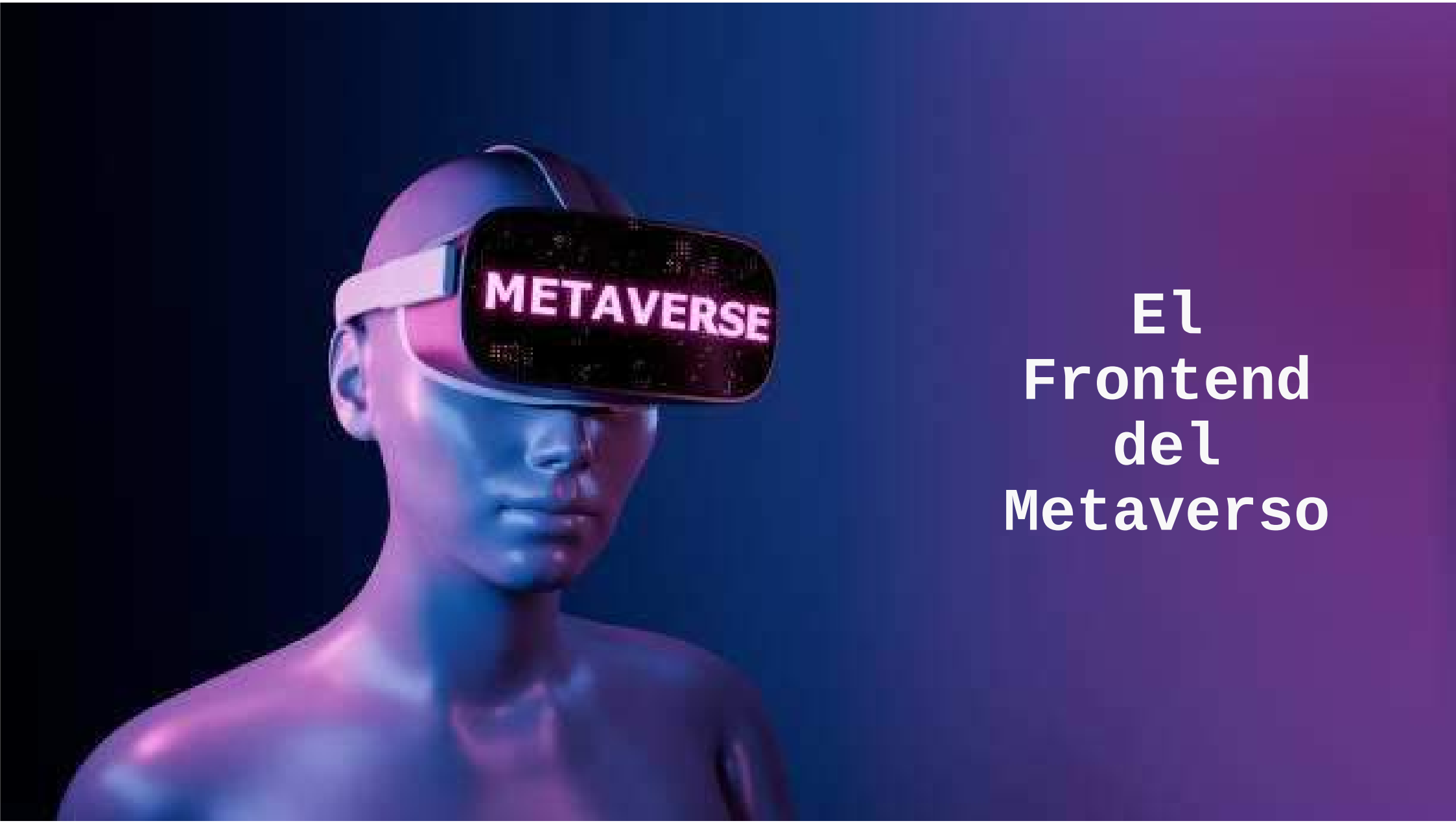
Resumen: Metaverso vs Web3



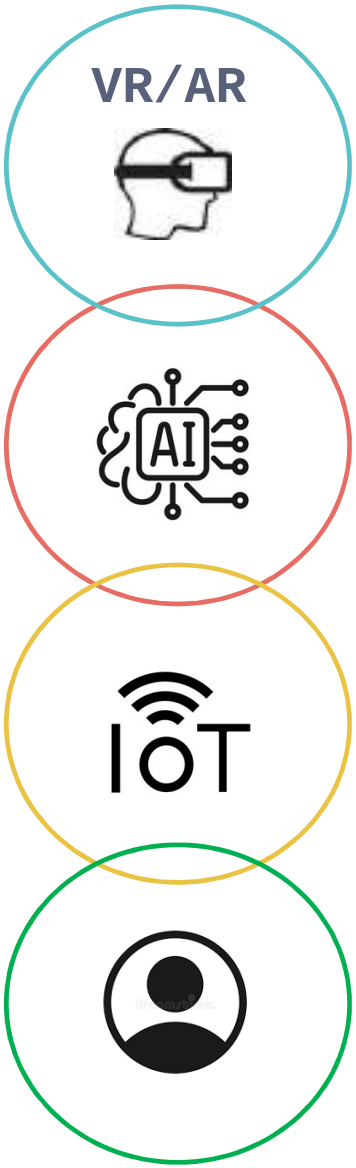
- No todo metaverso es Web3, y viceversa.
- Aunque el **Metaverso** actualmente está impulsado por algunos de los más importantes actores de la web 2.0 y hay muchas aplicaciones **web3** que no tienen su reflejo en un mundo virtual, **no son dos iniciativas aisladas**.
- Cada vez más se empiezan a ver plataformas distribuidas operando bajo el paradigma de la **web3**, que serán el **punto de acceso a un metaverso**.
- Además, a medida que proliferen los servicios y posibilidades a los que se acceda desde el **metaverso**, se irán incorporando la **posibilidad de interactuar con servicios web3.**
- ¿Será el **Metaverso Blockchain Descentralizado el metaverso más utilizado** en un futuro como suma de espacios interconectados por los que podremos desplazarnos, o será una plataforma dominada por una o varias empresas?
- El metaverso será el **sucesor de la Internet actual gracias a la Web3**, ya que supondrá un cambio de paradigma de Internet, por como se compone la identidad

Stack metaverso + web3





El Frontend del Metaverso



Telefónica


Telefónica
Retos de Privacidad del Metaverso

Protección de Datos y el Metaverso

¿Qué datos?

Avatares

Biometría

Interacción social y comportamiento

Telefónica

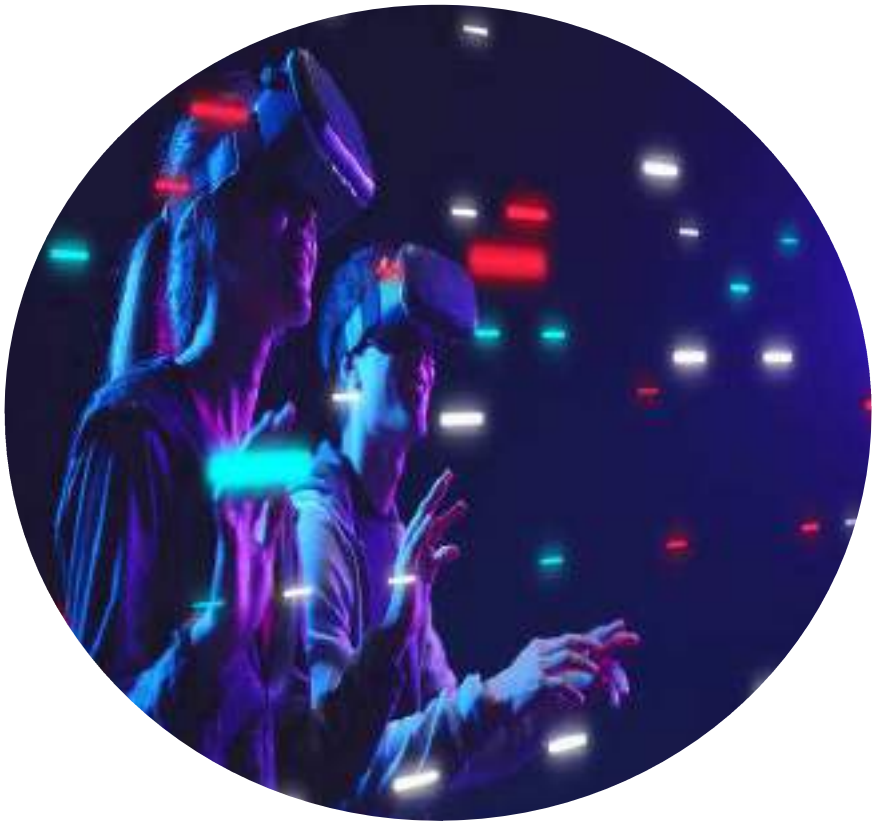
Protección de Datos y el Metaverso

¿Quién es el responsable?

La multitud de entidades presentes en el metaverso creará un entramado de relaciones que hará que no siempre sea fácil determinar los roles de responsables y encargados del tratamiento.

Protección de Datos y el Metaverso

Publicidad, perfilado e intercambio de datos



- Aumento sustancial del potencial de la elaboración de perfiles y la publicidad personalizada en base a comportamientos, reacciones y respuestas emocionales (eye-tracking, etc)
- Menor capacidad de los usuarios para evitar la recogida de datos personales, la cual tendrá lugar muchas veces de forma involuntaria e inconsciente.
- Menores y diseño apropiado para su edad (¿verificación edad?)
- Intercambio y portabilidad de datos a gran escala: transferencias

Protección de Datos y el Metaverso
Información y Consentimiento

- Nuevas formas de interactuar legalmente con los usuarios.
- Dificultad para informar y, en su caso, obtener consentimientos válidos.
- Publicidad subliminal o contextual sin que los usuarios sean conscientes.

En definitiva..

- Estamos en los **albores de un nuevo Internet.**
- Necesidad de **incorporar la privacidad por defecto en la tecnología y el diseño del metaverso**, formando parte de ella de manera indisoluble.
- **Momento crítico para la privacidad en Internet**, como lo fue hace una década el nacimiento de las redes sociales, con muchas lecciones aprendidas.


Telefónica
Otros retos jurídicos del Metaverso
GHOST

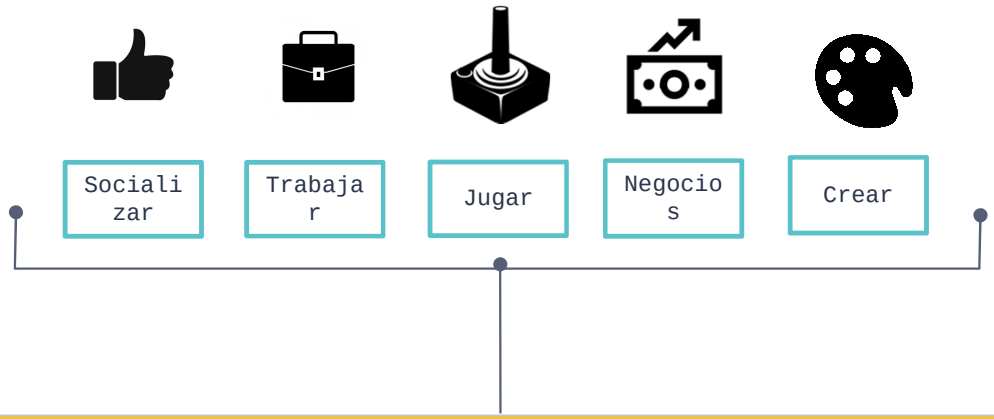
Reto jurídico 1: Regulación vertical de plataformas

Plataforma online	Gatekeeper	Servicio de intermediación online
Digital Services Act	Digital Markets Act	Reglamento P2B
Obligaciones: transparencia, incluir determinados contenidos, términos y condiciones, cooperación con autoridades, contacto y representante legal, moderación de contenidos, marcadores de confianza, resolución de conflictos extrajudicial, etc.	Obligaciones: interoperabilidad con terceros, portabilidad datos para Usuarios B2B, inversión publicitaria auditada, permitir a Usuarios B2B firmar contratos fuera de la plataforma con Usuarios B2C, no discriminación, no obligar el uso de software/apps	Obligaciones: transparencia e incluir determinados contenidos en términos y condiciones, imposibilidad de terminar la prestación del servicio sin causa justificada, sistema de quejas internas, no discriminación

Reto jurídico 2: Regulación horizontal de plataformas

Servicio de la sociedad de la información	Servicio o entorno digital	Tratamiento de datos	Propiedad Intelectual
Ley de Servicios de la Sociedad de la información	Ley General de Consumidores y Usuarios	GDPR, ePrivacy	IPRs, Marcas, Diseños, Secretos comerciales
Obligaciones: facilitar determinada información, deber de colaboración, información sobre seguridad, portabilidad de datos no personales, responsabilidad, etc.	Obligaciones: régimen conformidad en base a criterios objetivos y subjetivos, obligaciones de reembolso y suministro	Obligaciones: obligaciones generales de protección de datos	Protección derechos de autor: Creación de nuevas obras protegidas por derechos autor; usos no autorizados; control derechos morales y de explotación Protección de la marca: Ampliar la protección de las marcas; Vigilancia de marcas; Infracciones y C&D Secretos comerciales: actos de divulgación y explotación

Reto jurídico 3: Gobernanza de la plataforma



Una nueva experiencia de usuario legal	Ley aplicable y resolución de conflictos	Responsabilidad, Infracciones y Códigos de Conducta
El metaverso implicará nuevas formas de interactuar legalmente a través de un canal 3D (p.ej. Aceptar T&Cs, informar, capturar consentimientos, etc.)	Se requiere la determinación de una jurisdicción aplicable y un mecanismo de resolución de conflictos	Definir operativa de actuación ante infracciones de los T&Cs y de derechos de terceros, así como la fijación de un código de conducta para usuarios

Reto jurídico 4: aspectos jurídicos específicos de las tecnologías utilizadas (I)

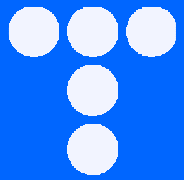
Web3

Tecnologías distribuidas	Pagos, DeFi, Crypto	Inteligencia artificial
• Retos GDPR y Blockchain • Retos Consumo y Blockchain • eIDAS y terceros de confianza (identidad descentralizada) • Capacidad probatoria • Tokenización (retos jurídicos NFTs) • Retos jurídicos Smart Contracts (elementos esenciales contratos)	• Regulación financiera (MiCa y LMV) • Publicidad de criptoactivos • Blanqueo de capitales (registro BdE) • Identificación de transacciones • Ley de medios de pago (para Fiat) • Criptoactivos como bienes muebles • Fiscalidad	• Reglamento IA • Retos IA y GDPR • Sesgos y discriminación no deseada de grupos vulnerables • Explicabilidad y algoritmos de caja negra (decisiones autónomas sin intervención humana) • Fake news

Reto jurídico 4: aspectos jurídicos específicos de las tecnologías utilizadas (I)




Gaming	Realidad virtual	5G / Edge	Entorno desarrollo
• Regulación de las “loot boxes” (Mecanismos Aleatorios de Recompensa (MAR) y normativa publicitaria • Regulación audiovisual • IPRs videojuegos	• Derecho de consumo y dispositivos (p.ej. Garantía) • Retos GDPR IoT RV (tratamiento datos sensibles) • Retos GDPR mundos virtuales • Ciberseguridad • IPRs modelos 3D	• Privacidad 5G (localización) • Regulación telco (priorización y neutralidad de red)	• Exportación de tecnología • Protección de activos intangibles


Telefónica

Organiza:

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Partners Estratégicos:

GOVERTIS
Part of Telefónica Tech

Telefónica Tech

"Hay privacidad más allá de la privacidad: intersecciones con otros marcos normativos"

Lorenzo Cotino Hueso www.cotino.es

Catedrático de Derecho Constitucional, Universidad de Valencia

https://www.linkedin.com/in/cotino/

@ cotino

Partners Estratégicos:

GOVERTIS Part of Telefónica Tech

Telefónica Tech

Lorenzo Cotino Hueso, U. Valencia

www.Odiseia.org www.derechotics.com

Observatorio UV

Observatorio de Transformación Digital del Sector Público. Contribuciones

10/05/21

Listado de contribuciones al Ciclo Observatorio

16/04/21

Patrocinio y colaboraciones

14/04/21

Entusiasmo robótico y externalización... por Enrique Benítez y Alejandro Teré

14/04/21

Bizum en el sector público, pensando en... por Eider Sarria Gutiérrez

11/03/21

Procedimiento de actuación contra... por Juan Francisco Sánchez Barrilao

11/03/21

Interoperabilidad = Transparencia + Protección... por Rubén Martínez Gutiérrez

II Insight Exclusivo Club DPD 2022

El DPD

Partners Estratégicos:

GOVERTIS Part of Telefónica Tech

Telefónica Tech

II Insight Exclusivo Club DPD 2022

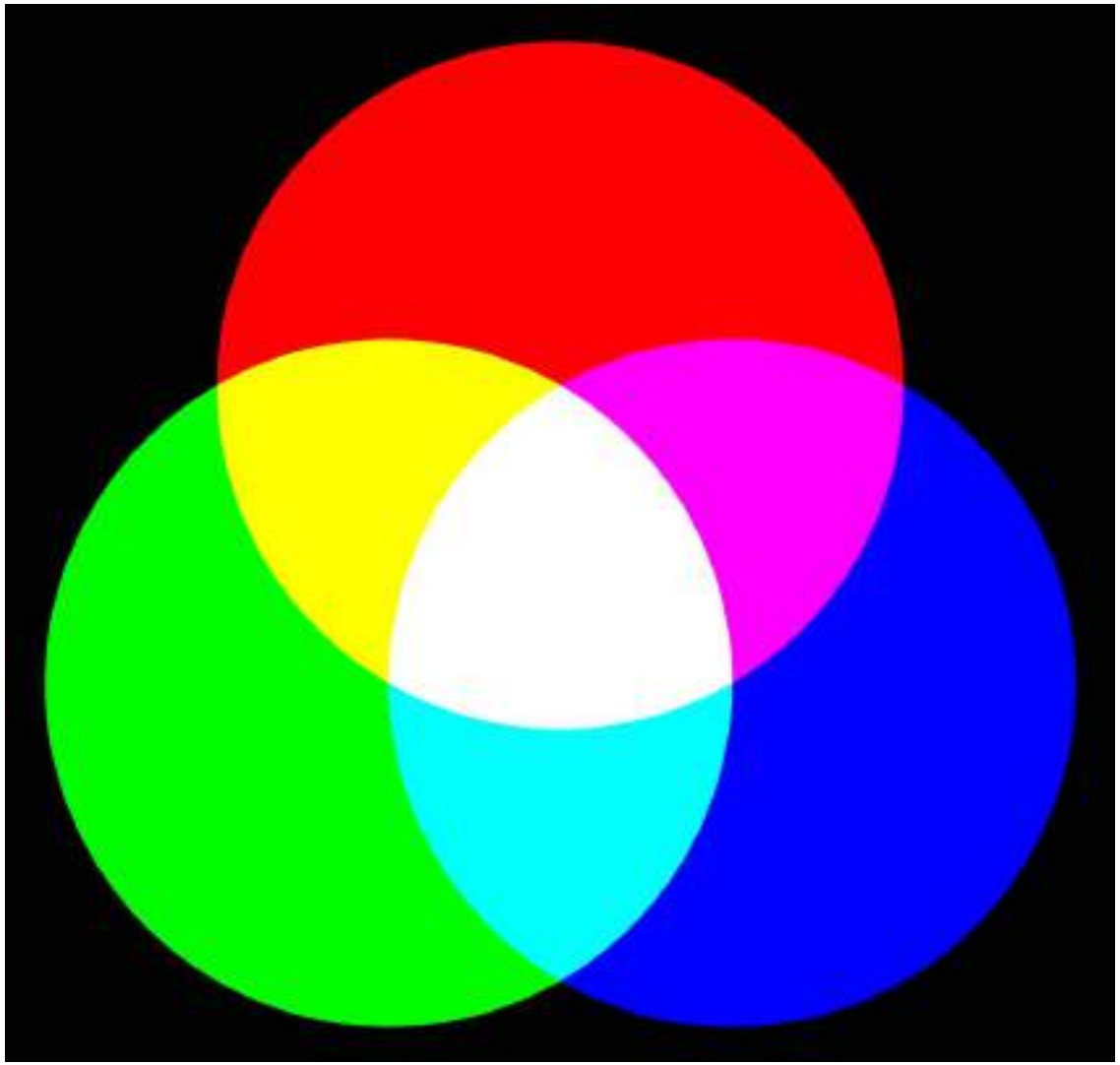
El DPD

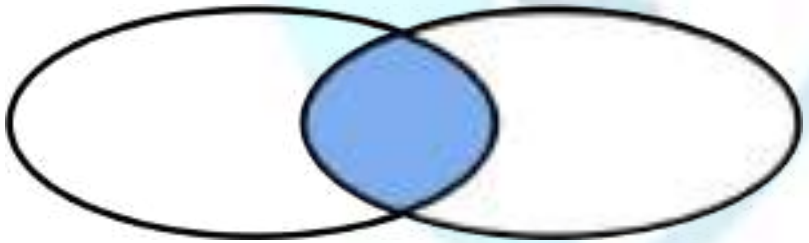
Partners Estratégicos:

GOVERTIS Part of Telefónica Tech

Telefónica Tech

Muchas áreas afines a la protección de datos y la privacidad





Evaluación del riesgo y Nuevo modelo de cumplimiento normativo, responsabilidad proactiva y demostrada, impacto social, diseño, defecto, DPOs…

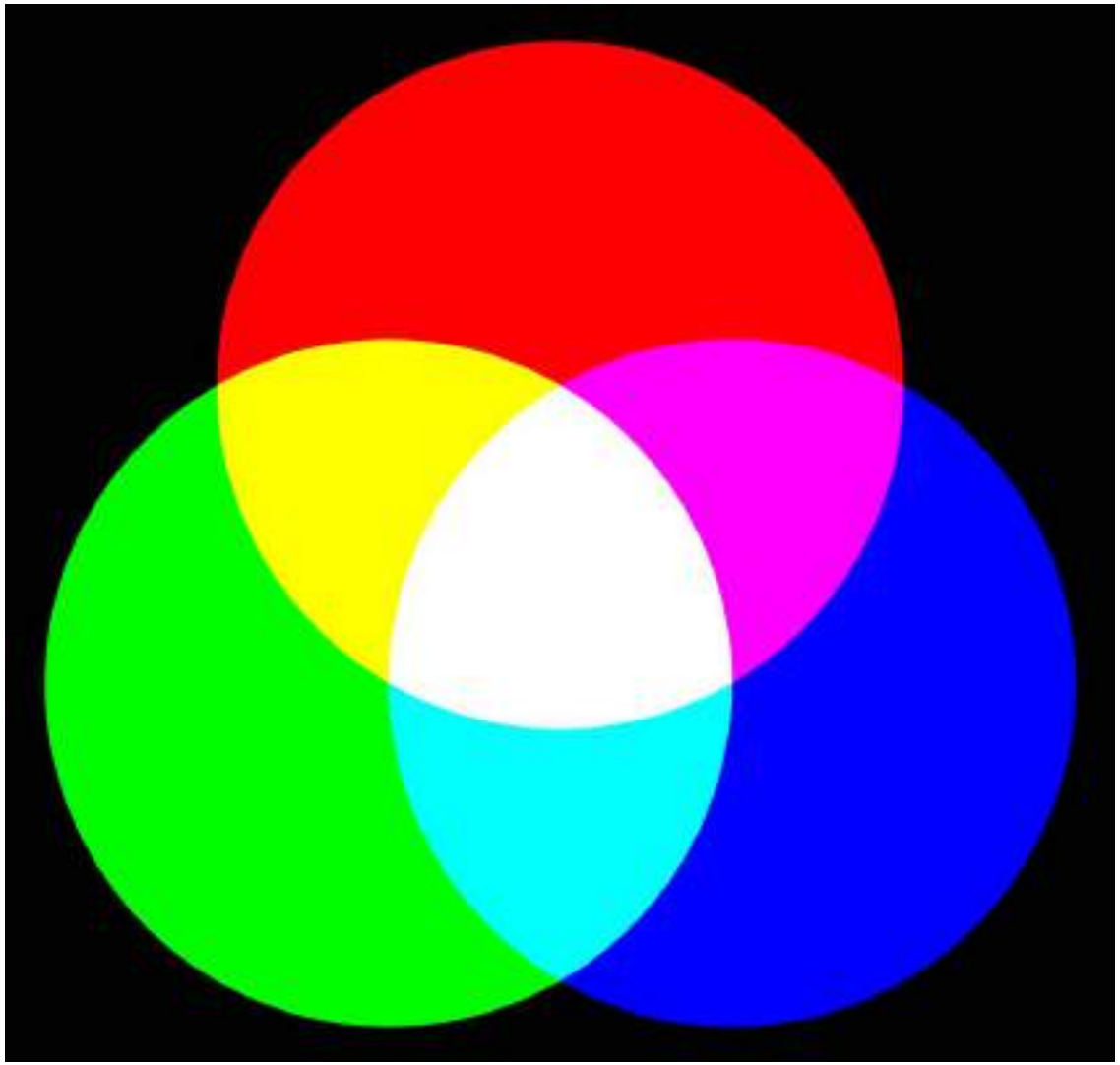
Más vale prevenir que curar…

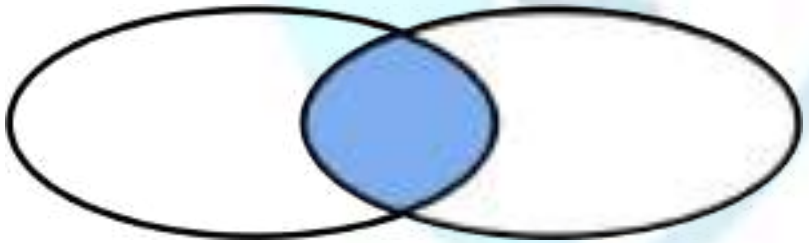
- **Principios:**
- Licitud del tratamiento
- Lealtad y transparencia
- Limitación de la finalidad
- Minimización de datos
- Exactitud
- proactividad

Partners Estratégicos

GOVERTIS
Part of Telefónica Tech

Muchas áreas afines a la protección de datos y la privacidad





RD 311/2022 Nuevo ENS

"incompatibilidad" de DPO y responsable de seguridad, ambos en "comité de seguridad"

"Nuevos" responsables de información, de servicio y de sistema (diferente de), responsable de seguridad.

Partners Estratégicos:

GOVERTIS Part of Telefónica Tech

Telefónica Tech

Transparencia y DPD

¿Administración 4.0?

¿Administración 4.0?

	España			UE
	DESI 2018	DESI 2019	DESI 2020	DESI 2020
	valor	valor	valor	valor
5a1 Usuarios de la administración electrónica % de usuarios de internet que necesitan presentar formularios	**67 %** 2017	**76 %** 2018	**82 %** 2019	**67 %** 2019
5a2 Formularios pre-cumplimentados Puntuación (0 a 100)	**72** 2017	**74** 2018	**80** 2019	**59** 2019
5a3 Compleción de servicios en línea Puntuación (0 a 100)	**95** 2017	**95** 2018	**96** 2019	**90** 2019
5a4 Servicios públicos digitales para empresas Puntuación (0 a 100) - incluidos nacionales y transfronterizos	**95** 2017	**93** 2018	**93** 2019	**88** 2019
5a5 Datos abiertos % de la puntuación máxima	**NP**	**NP**	**90 %** 2019	**66 %** 2019

Administración 4.0 Agenda 2025

Administración 4.0 ENIA

Administración 4.0 Plan Digitalización

Planes... DATA DRIVEN GOV

- Integración de todas las Administraciones en la Transformación Digital del Sector Público
- mejorar la **interoperabilidad** actualizar las infraestructuras tecnológicas con seguridad y el respeto al medio ambiente
- la **Inteligencia** Artificial en la articulación y ejecución de políticas públicas
- Estadísticas Inteligentes Fiables (*Trusted Smart Statistics*) .
- **puestos de trabajo de nueva generación**. *reskilling* de los empleados públicos
- **visión 360º**, acceso a los datos (***one-click data***), **asistentes virtuales** y desarrollo de aplicaciones móviles. **App factory**
- plataforma reutilizable de **servicios de lenguaje natural**?
- **tramitación automatizada** (Intelligent Automation as-a-Service)

ENIA

- mejorar la **transparencia y publicidad** de la actividad pública
- **sanidad servicios sociales, medio ambiente y energía, justicia, transporte y logística, educación, empleo y seguridad**
- utilizar la IA para determinar prioridades e idenficar ventajas y objetivos en el sector público
- **monitorizar la actividad de la Administración y personalizar servicios** aplicaciones adaptadas y personalizadas a sus necesidades
- mejorar las **políticas de empleo y de capacitación** de los trabajadores

¿"A España (la Administración) no la va a conocer ni la madre que la parió”?

Servicios 360, 24/7…

Partners Estratégicos:

Smart cities, contratación, datos y ciberseguridad

Partners Estratégicos:

GOVERTIS Part of Telefónica Tech

Telefónica Tech

Empleo público

Partners Estratégicos:

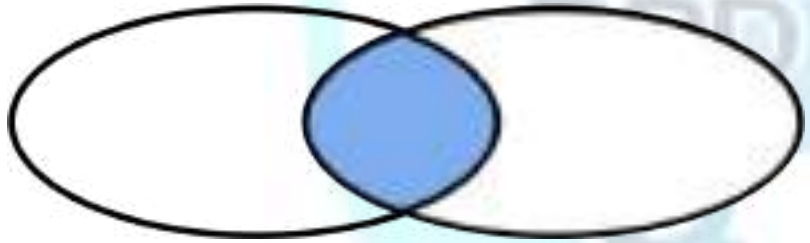
GOVERTIS Part of Telefónica Tech

Telefónica Tech

Partners Estratégic

GOVERTIS
Part of Telefónica Tech

Investigación y salud



Partners Estratégicos:

GOBERTIS Part of Telefónica Tech

Telefónica Tech

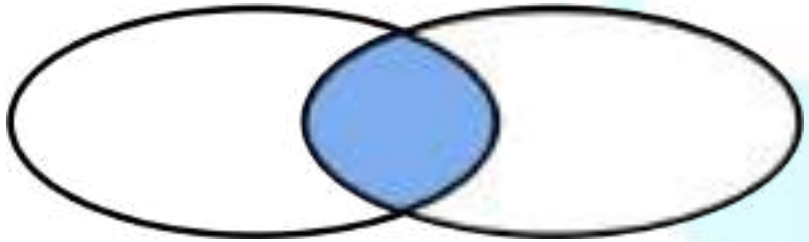
Guía para el cumplimiento normativo en la investigación y experimentación con Inteligencia Artificial y tecnologías conexas en Espacios de Datos e Innovación, centrada en privacidad y data governance

ITI INVESTIGATE TO INNOVATE

Lorenzo Cotino Hueso
Catedrático de Derecho Constitucional
Universitat de València

Edición y coordinación:
Óscar Valle Ballesteros.
Instituto Tecnológico de Informática.
Daniel Sáez Domingo.
Instituto Tecnológico de Informática.

Investigación y salud



OJO políticas,
Espacio europeo de datos de salud, gobernanza de datos, etc.

economía del dato jurídicos. Actuaciones propias, como GAIA-X

Directiva de reutilización, Ley de gobernanza de datos ., Ley datos, Ley datos salud

Gobernanza y calidad del dato

Gobernanza y calidad del dato

Decisiones automatizadas-INTELIGENCIA ARTIFICIAL

…privacidad y protección de datos

- **ESPECÍFICO art. 22 RGDP y error generalizado**
- decisiones automatizadas del artículo 22 RGPD, así como y los deberes de transparencia e información , (art. 13. 2º f y 14. 2º g).

IA “Made in Europe” ética en el diseño

Sistemas de evaluación de conformidad

Partners Estratégicos:

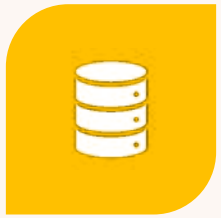
GOVERTIS Part of Telefónica Tech

Tech

ALTO RIESGO reglamento IA:

CUMPLIMIENTO DE LOS REQUISITOS

SISTEMA DE GESTIÓN DE RIESGOS



DATOS Y GOBERNANZA DE DATOS

DOCUMENTACIÓN TÉCNICA

REGISTRO DE DATOS

TRANSPARENCIA

SUPERVISIÓN HUMANA

PRECISIÓN, SOLIDEZ Y CIBERSEGURIDAD

Lorenzo Cotino Hueso, U. Valencia

www.Odiseia.org www.derechotics.com

CLUB
DPD
AEC

Organiza:

AEC

Partners Estratégicos:

GOBERTIS Part of Telefónica Tech

Telefónica Tech

"Taller práctico: Nuevo Esquema Nacional de Seguridad"

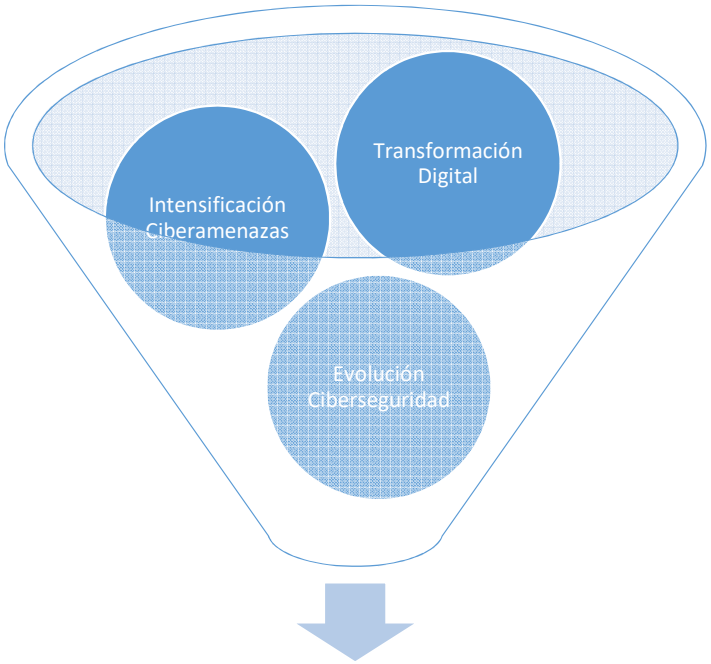
Lucía Arias Gil

Coordinadora Centro de Excelencia ENS Govertis

https://www.linkedin.com/in/luciarias/

@ l.arias@govertis.com

Motivación



Actualizar el ENS

Metodología de cumplimiento ENS

Partners Estratégicos:

GOVERTIS Part of Telefónica Tech

Telefónica Tech

DEFINIR ROLES Y ASIGNAR PERSONAS

- Art. 11. Diferenciación de responsabilidades

  En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el **responsable del sistema.**

- Art. 13. Organización e implantación del proceso de seguridad

  2.d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
  3. El responsable de la seguridad será distinto del responsable del sistema, **no debiendo existir dependencia jerárquica entre ambos**. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.

DEFINIR ROLES Y ASIGNAR PERSONAS

DEFINIR ROLES Y ASIGNAR PERSONAS

- Novedad!!
- Art. 13. Organización e implantación del proceso de seguridad

4. Una Instrucción Técnica de Seguridad regulará el **Esquema de Certificación de Responsables de la Seguridad**, que recogerá las condiciones y requisitos exigibles a esta figura.

5. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (**Punto o Persona de Contacto**) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

POLÍTICA DE SEGURIDAD

- Artículo 12. Política de seguridad y requisitos mínimos de seguridad

1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

a) Los objetivos o misión de la organización.

b) El marco regulatorio en el que se desarrollarán las actividades.

c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

f) Los riesgos que se derivan del tratamiento de los datos personales.

VALORAR Y CATEGORIZAR EL SISTEMA DE INFORMACIÓN

- Artículo 40. Categorías de seguridad
- Anexo I. Categorías de seguridad de los sistemas de información

VALORAR Y CATEGORIZAR EL SISTEMA DE INFORMACIÓN

Ejercicio práctico de categorización

SECUENCIA DE ACTUACIONES

IDENTIFICACIÓN DEL NIVEL DEL SERVICIO (BAJO, MEDIO o ALTO) PARA CADA DIMENSIÓN DE SEGURIDAD

Categoría BÁSICA → El nivel máximo es BAJO
Categoría MEDIA →El nivel máximo es MEDIO
Categoría ALTA → El nivel máximo es ALTO

VALORAR Y CATEGORIZAR EL SISTEMA DE INFORMACIÓN

Ejercicio práctico de categorización

Categorización del Servicio de Licitación Electrónica.

	[D]	[A]	[T]	[C]	[I]
Anuncio	BAJO	MEDIO	MEDIO	SIN VALORAR	MEDIO
Pliegos	BAJO	ALTO	MEDIO	SIN VALORAR	MEDIO
Ofertas	MEDIO	MEDIO	ALTO	ALTO	ALTO
Evaluación	ALTO	ALTO	MEDIO	ALTO	ALTO
Adjudicación	SIN VALORAR	MEDIO	ALTO	SIN VALORAR	MEDIO
Contratación	BAJO	MEDIO	MEDIO	BAJO	BAJO

¿¿Categoría del Servicio de Licitación Electrónica??

VALORAR Y CATEGORIZAR EL SISTEMA DE INFORMACIÓN

Ejercicio práctico de categorización

Categorización del Servicio de Licitación Electrónica.

	[D]	[A]	[T]	[C]	[I]
Anuncio	BAJO	MEDIO	MEDIO	SIN VALORAR	MEDIO
Pliegos	BAJO	ALTO	MEDIO	SIN VALORAR	MEDIO
Ofertas	MEDIO	MEDIO	ALTO	ALTO	ALTO
Evaluación	ALTO	ALTO	MEDIO	ALTO	ALTO
Adjudicación	SIN VALORAR	MEDIO	ALTO	SIN VALORAR	MEDIO
Contratación	BAJO	MEDIO	MEDIO	BAJO	BAJO

Categoría del Servicio de Licitación Electrónica: ALTA

REALIZAR ANÁLISIS DE RIESGOS

- Artículo 7. Gestión de la seguridad basada en riesgos

1. El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

2. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

REALIZAR ANÁLISIS DE RIESGOS

REALIZAR ANÁLISIS DE RIESGOS

PREPARAR Y APROBAR LA DECLARACIÓN DE APLICABILIDAD

- Artículo 28. Cumplimiento de los requisitos mínimos

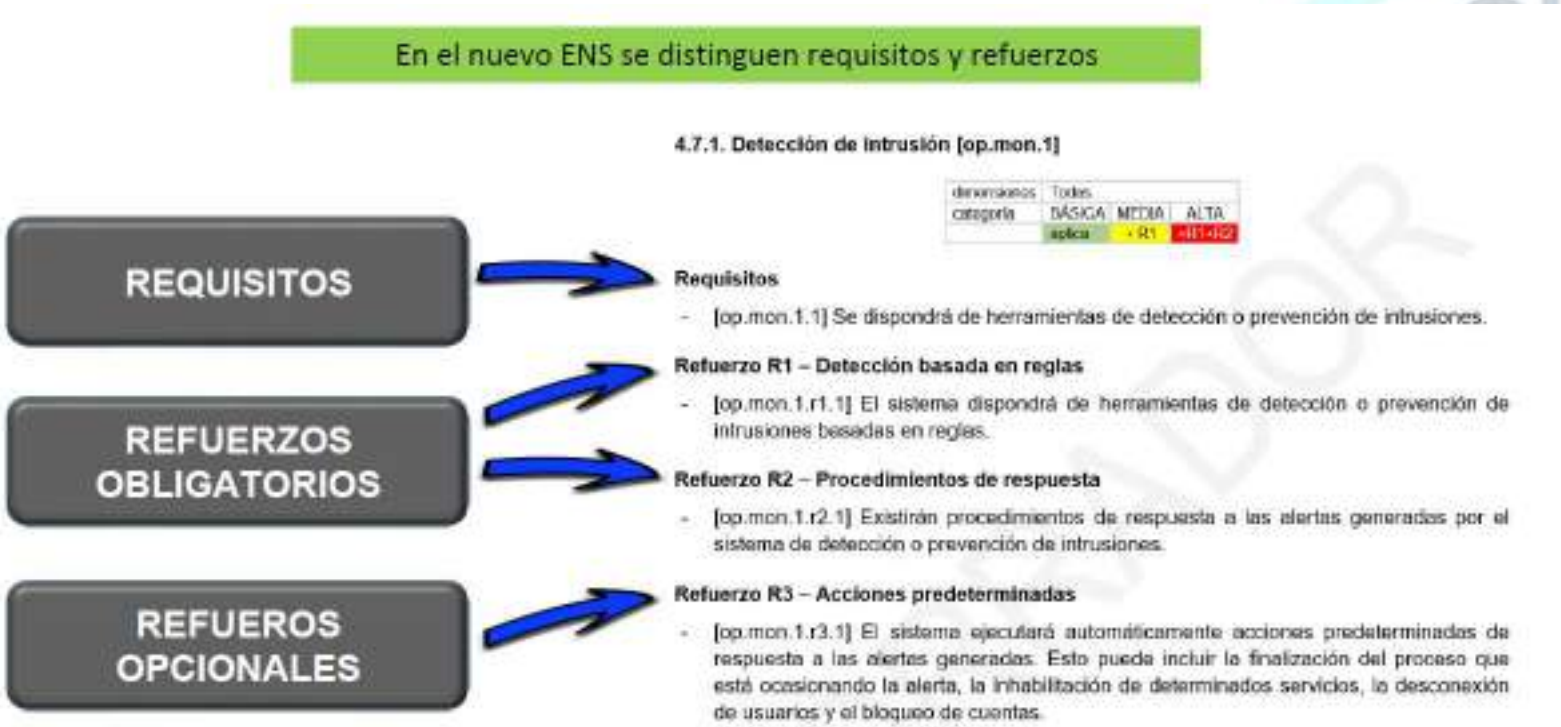
- 1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:
  a) Los activos que constituyen los sistemas de información concernidos.
  b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
  c) Las decisiones que se adopten para gestionar los riesgos identificados.
- 2. Las medidas a las que se refiere el apartado 1 tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados. La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado **Declaración de Aplicabilidad**, firmado por el responsable de la seguridad.

PREPARAR Y APROBAR LA DECLARACIÓN DE APLICABILIDAD

En el nuevo ENS se distinguen requisitos y refuerzos

REQUISITOS	Son obligatorios para **todas las categorías** en a las que la medida sea de aplicación.
REFUERZOS OBLIGATORIOS	Son obligatorios para **determinada(s) categoría**.
REFUEROS OPCIONALES	Son de aplicación discrecional al sistema de información.

PREPARAR Y APROBAR LA DECLARACIÓN DE APLICABILIDAD



PREPARAR Y APROBAR LA DECLARACIÓN DE APLICABILIDAD

REFUERZOS OPCIONALES Y REFUERZOS OBLIGATORIOS PARA UNA CATEGORIA SUPERIOR

GESTIÓN DE RIESGOS
(Apreciación + Tratamiento)

REQUISITOS Y REFUERZOS OBLIGATORIOS PARA LA CATEGORÍA

VALORACIÓN y CATEGORIZACIÓN

DECLARACIÓN DE APLICABILIDAD (SOA)

Doble vía de acceso para aplicar medidas que se reflejarán en la Declaración de Aplicabilidad.

Principales cambios Anexo II

Partners Estratégicos:

GOBERTIS Part of Telefónica Tech

Telefónica Tech

Principales cambios Anexo II

- Aparecen los refuerzos:
  - Para indicar una mayor exigencia se emplean los refuerzos de seguridad (R) que se suman (+) a los requisitos base de la medida pero que no siempre son incrementales entre sí.
  - Para indicar que se puede elegir entre un refuerzo u otro, se indica entre corchetes [Rm o Rn].

mp.com	Protección de las comunicaciones				
mp.com.1	Perímetro seguro	Todas	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separación de flujos de información en la red	Todas	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4

Implantar, operar y monitorizar el sistema

El nuevo ENS – gestión de la capacidad [op.pl.4]

4.1.4. Dimensionamiento / gestión de la capacidad [op.pl.4]

dimensiones	D		
nivel	bajo	medio	alto
	aplica	+ R1	+ R1

Requisitos

Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos:

- [op.pl.4.1] Necesidades de procesamiento.
- [op.pl.4.2] Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
- [op.pl.4.3] Necesidades de comunicación.
- [op.pl.4.4] Necesidades de personal: cantidad y cualificación profesional.
- [op.pl.4.5] Necesidades de instalaciones y medios auxiliares.

Refuerzo R1 –Mejora continua de la gestión de la capacidad

- [op.pl.4.r1.1] Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.
- [op.pl.4.r1.2] Se emplearán herramientas y recursos para la monitorización de la capacidad.

Implantar, operar y monitorizar el sistema

El nuevo ENS – Mecanismos de autenticación [op.acc.5] y [op.acc.6]

RD 3/2010

- Op.acc.5 Mecanismos de autenticación.
- Op.acc.6 Acceso local
- Op.acc.7 Acceso remoto

Certificado Digital

Nuevo ENS

- Op.acc.5 Mecanismo de autenticación (usuarios externos)
- Op.acc.6 Mecanismo de autenticación (usuarios de la organización)

Implantar, operar y monitorizar el sistema

El nuevo ENS – Mecanismos autenticación usuarios externos [op.acc.5]

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5

Refuerzo R1 – Contraseñas

- [op.acc.5.r1.1] Se empleará una contraseña como mecanismo de autenticación.
- [op.acc.5.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2 – Contraseña + OTP

- [op.acc.5.r2.1] Se requerirá una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario.

Refuerzo R3 – Certificados

- [op.acc.5.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.
- [op.acc.5.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.
- [op.acc.5.r3.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

Refuerzo R4 – Certificados en dispositivo físico

- [op.acc.5.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.
- [op.acc.5.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.
- [op.acc.5.r4.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

Refuerzo R5 – Registro

- [op.acc.5.r5.1] Se registrarán los accesos con éxito y los fallidos.
- [op.acc.5.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Nivel BAJO
op.acc.5 + [R1 o R2 o R3 o R4]

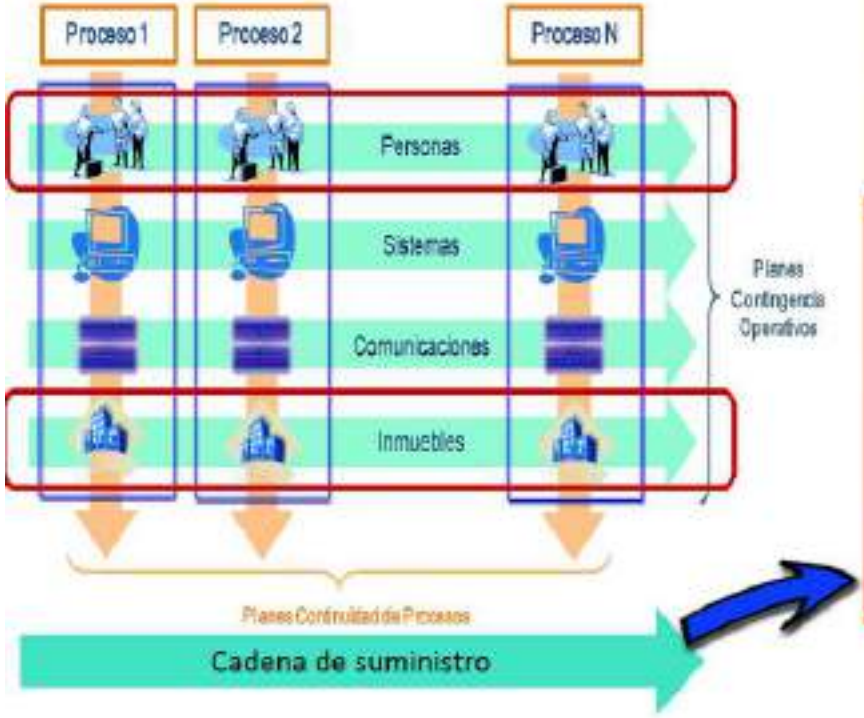
Nivel MEDIO
op.acc.5 + [R2 o R3 o R4] + R5

Nivel ALTO
op.acc.5 + [R2 o R3 o R4] + R5

Implantar, operar y monitorizar el sistema

El nuevo ENS – protección de la cadena de suministro [op.ext.3]

Escenarios de contingencia en el Plan de Continuidad (PCN/BCP):



ISO/TS 22318:2015
Business continuity management systems — Guidelines for supply chain continuity

Implantar, operar y monitorizar el sistema

El nuevo ENS – interconexión de sistemas [op.ext.4]

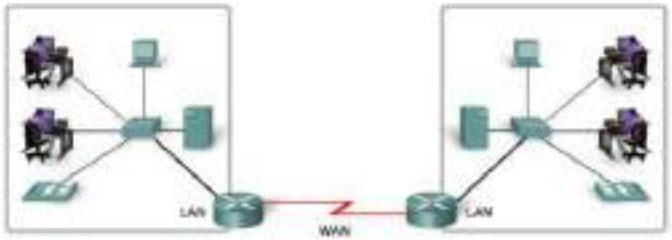
4.4.4. Interconexión de sistemas [op.ext.4]

Se denomina interconexión al establecimiento de enlaces con otros sistemas de información para el intercambio de información y servicios.

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	+ R1

Requisitos

- [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.
- [op.ext.4.2] Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.



Refuerzo R1 – Coordinación de actividades

[op.ext.4.r1.1] Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de seguridad locales se acompañarán de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

Implantar, operar y monitorizar el sistema

El nuevo ENS – protección de servicios en la nube [op.nub.1]

4.5. Servicios en la nube [op.nub]

4.5.1. Protección de servicios en la nube [op.nub.1]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1	

Requisitos

- [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a Service* SaaS), Plataforma como Servicio (*Platform as a Service* PaaS) e Infraestructura como Servicio (*Infrastructure as a Service* IaaS) definidas en las guías CCN-STIC que sean de aplicación.
- [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

  a) Auditoría de pruebas de penetración (*pentesting*).
  b) Transparencia.
  c) Cifrado y gestión de claves.
  d) Jurisdicción de los datos.

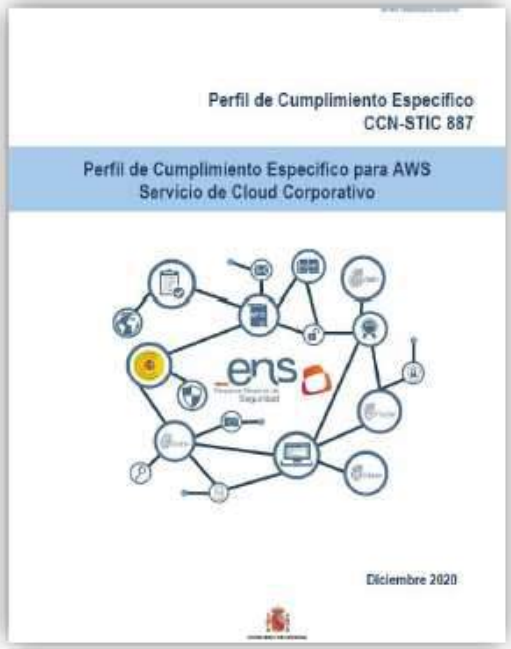
Refuerzo R1- Servicios certificados

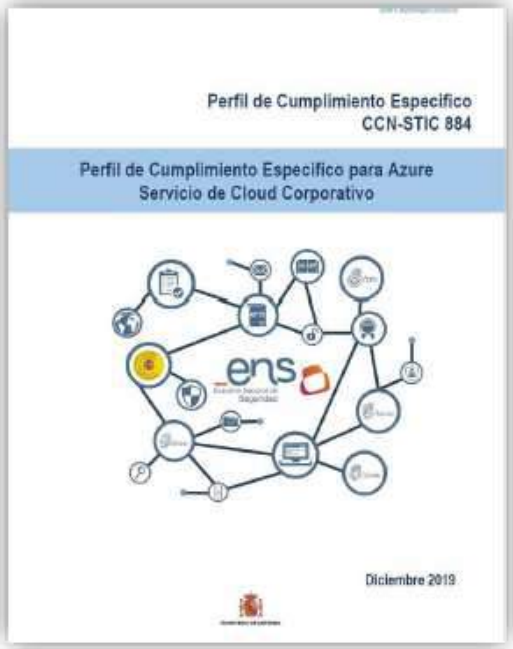
- [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.
- [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

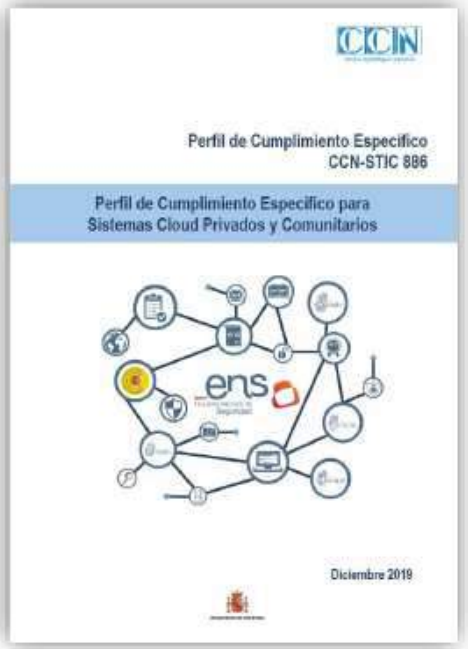
Refuerzo R2 – Guías de Configuración de Seguridad Específicas

[op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente Guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

Implantar, operar y monitorizar el sistema







Perfiles de cumplimiento

Implantar, operar y monitorizar el sistema

El nuevo ENS – vigilancia [op.mon.3]

4.7.3. Vigilancia [op.mon.3]

dimensiones:	Todas		
categoría	bajo	media	alta
	aplica	+ R1 R2	+ R3 R4 R5 R6 R7

Requisitos

[op.mon.3.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad.

Refuerzo R1 – Correlación de eventos

[op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

Refuerzo R2 – Análisis dinámico

[op.mon.3.r2.1] Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

Refuerzo R3 – Ciberamenazas avanzadas

- [op.mon.3.r3.1] Se dispondrá de sistemas para detección de amenazas avanzadas y comportamiento anómalos.
- [op.mon.3.r3.2] Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (*Advanced Persistent Threat* APT) mediante la detección de anomalías significativas en el tráfico de la red.

Refuerzo R4 – Observatorios digitales

[op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías, que pudieran representar indicadores de amenaza, en contenidos digitales.

Refuerzo R5– Minería de datos

Se aplicarán medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos.

- [op.mon.3.r5.1] Limitación de las consultas, monitorizando volumen y frecuencia.
- [op.mon.3.r5.2] Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.

Refuerzo R6 – Inspecciones de seguridad

Se realizarán las siguientes inspecciones periódicamente y tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas:

- [op.mon.3.r6.1] Verificación de configuración.
- [op.mon.3.r6.2] Análisis de vulnerabilidades.
- [op.mon.3.r6.3] Pruebas de penetración.

Refuerzo R7 – Interconexiones

[op.mon.3.r7.1] En las interconexiones que lo requieran, se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.


Gracias