Playbook

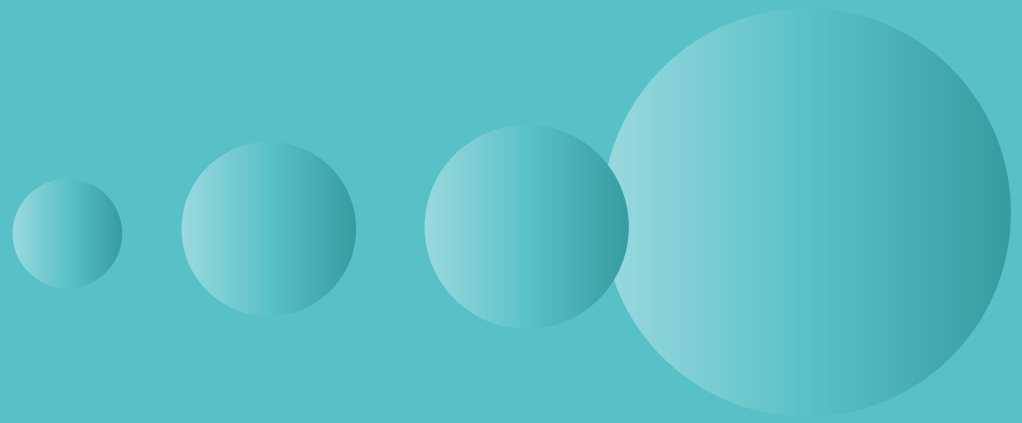
Innovación tecnológica

2025

Telefónica

Innovación tecnológica

La innovación forma parte de la identidad de Telefónica. Nuestra visión innovadora y espíritu emprendedor nos han permitido reinventarnos a lo largo de nuestra historia, ofrecer nuevas oportunidades a las personas y avanzar en la transformación digital, social y económica de los países en los que operamos.



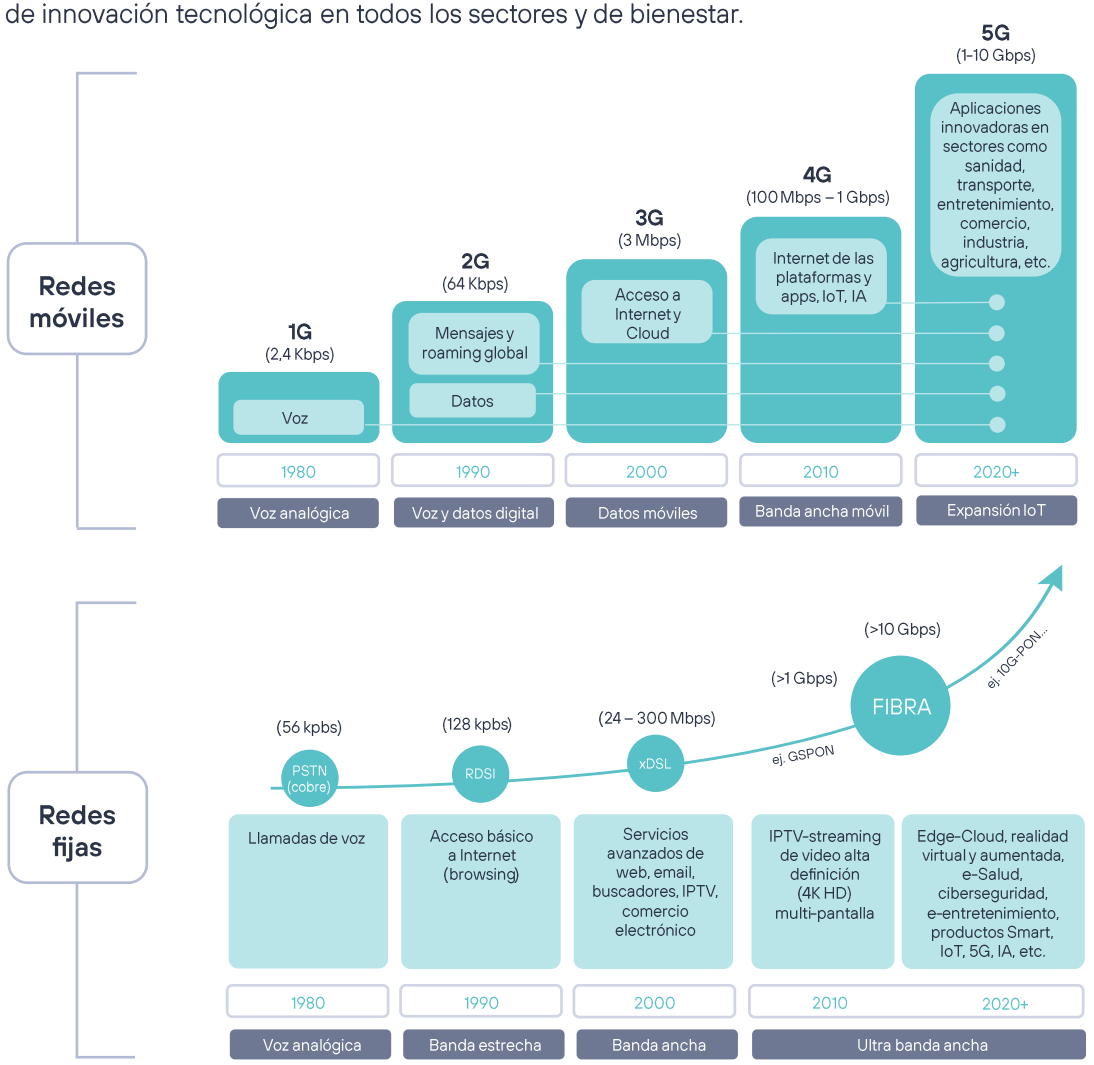
07

Conectividad:
El poder transformador de las telecomunicaciones y su impacto en la innovación

Telefónica

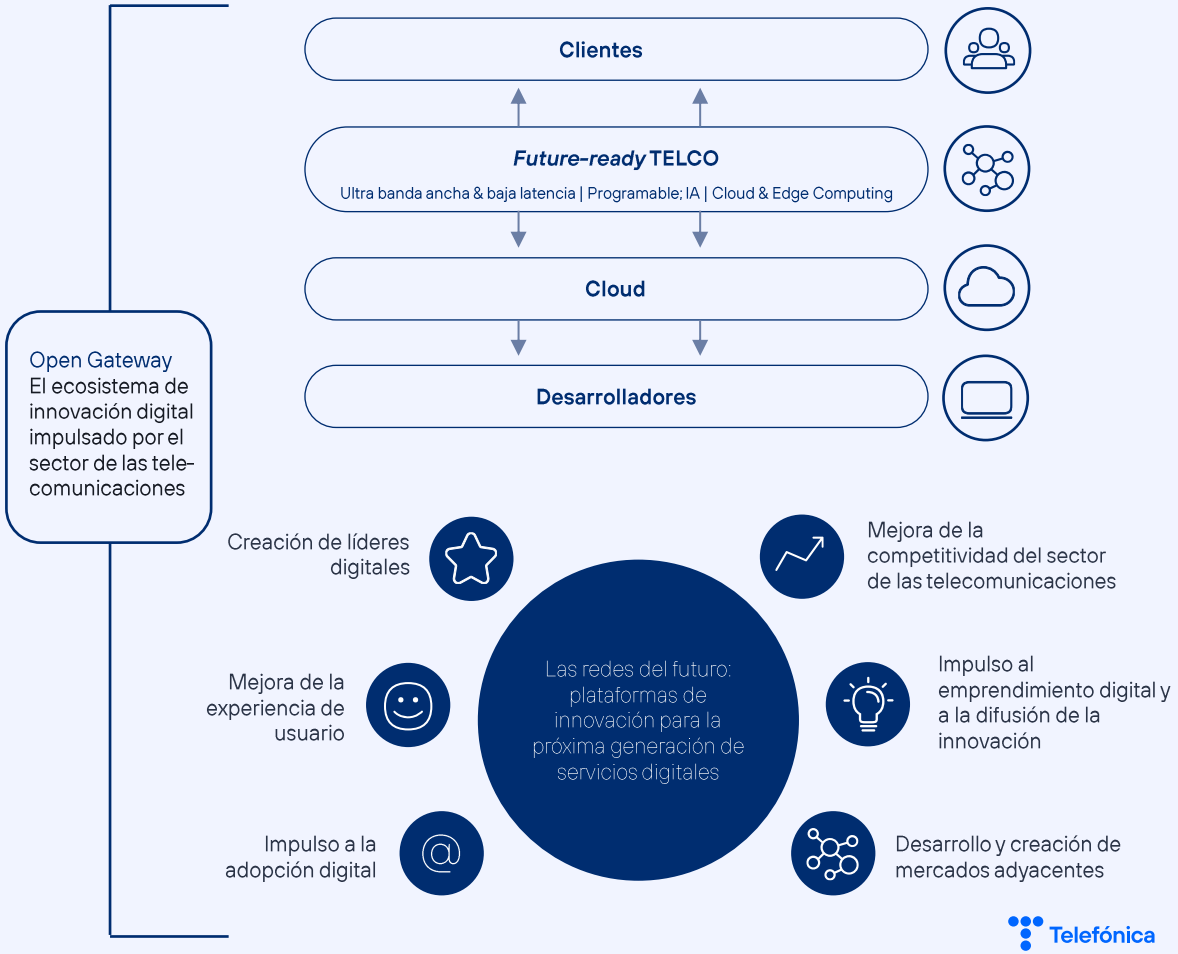
Impacto en innovación de la transformación de la conectividad

El continuo flujo de inversión en el sector de las telecomunicaciones promueve la innovación tecnológica de sus redes, habilitando experiencias digitales avanzadas, y nuevas oportunidades de innovación tecnológica en todos los sectores y de bienestar.



Hacia una nueva era de innovación digital

Sin inversión, la innovación se estanca. Es necesario promover un entorno favorable a la inversión para adaptar las redes a la nueva era digital.



Telefónica

Evolucionar hacia un entorno que facilite la inversión para transformar la red e impulsar la innovación digital y una nueva generación de servicios digitales

1 Promover estructuras de mercados sostenibles

Reducir la fragmentación de los mercados de telecomunicaciones a nivel nacional para permitir a los operadores alcanzar la escala necesaria para fortalecer la capacidad de inversión y, por tanto, de innovación del sector.

2 Establecer un marco regulatorio que permita liberar recursos para agilizar el despliegue y la transformación de las redes

Reducir la carga administrativa y los costes asociados, incluidas las cargas fiscales, así como simplificar los trámites burocráticos al despliegue y la transformación.

3 Promover una política de espectro favorable a la inversión

Generar certidumbre sobre la renovación de las licencias e incrementar la oferta armonizada de espectro en bandas medias y bajas para redes terrestres celulares y asegurar su asignación en condiciones razonables, buscando la maximización del valor del espectro para los usuarios finales.

4 Evolucionar el marco regulatorio para impulsar la innovación y la igualdad de condiciones en el ecosistema digital

Abordar las asimetrías con marcos horizontales que cubran aspectos como competencia, derechos del consumidor, o fiscales, eliminando enfoques sectoriales.

Restablecer el equilibrio de la cadena de valor digital mediante el fomento de una relación justa entre los agentes.

Proporcionar directrices adicionales sobre la neutralidad de la red para habilitar casos de uso innovadores como los facilitados por 5G *network slicing* u Open Gateway.

5 Reconocer el papel clave de la conectividad para impulsar la transición verde

Fomentar la reorientación del flujo de inversiones hacia el despliegue de redes más eficientes, como son la fibra y el 5G.

¿Quieres saber más?
Lee nuestro posicionamiento
Accede a contenido relacionado

Contexto

Impulsar la competitividad de las sociedades depende directamente de la fortaleza y la modernización de las empresas presentes en un país o región, en particular de las empresas tecnológicas. El esfuerzo inversor de estas compañías es fundamental para fomentar la innovación, enriquecer el entramado social y fortalecer la competitividad de la estructura económica a través de avances tecnológicos sostenibles y accesibles para todas las personas y empresas.

En la era digital, el sector de las telecomunicaciones cobra especial relevancia. El desarrollo de una economía competitiva y una sociedad digital están intrínsicamente ligados a la disponibilidad de una conectividad efectiva facilitada por redes fijas y móviles de alta capacidad. Esta conectividad es clave por su contribución a la digitalización de todos los segmentos de la sociedad: las empresas, las administraciones públicas y las personas. Pero también es un pilar fundamental para el desarrollo de nuevas tecnologías y el impulso a la innovación digital, habilitando servicios y experiencias digitales cada vez más sofisticadas, que promueven la competitividad, la sostenibilidad y el bienestar.

El sector de las telecomunicaciones ha mantenido un proceso de innovación continua en sus sistemas, estrategias comerciales y, especialmente, en el desarrollo de las redes fijas y móviles. Como pionero en la evolución tecnológica, este sector desempeña un papel clave al ofrecer una conectividad efectiva para impulsar la prosperidad.

El constante flujo de inversión en el sector, que por ejemplo en Europa, y según los datos de Connect Europe, alcanza más de 50.000 millones de euros anuales, permite que continuamente se pongan a disposición de los ciudadanos y las empresas experiencias digitales avanzadas, abriendo al mismo tiempo nuevas oportunidades de innovación tecnológica en todos los sectores, contribuyendo así a la transformación y a la prosperidad de las sociedades.

Retos

La innovación en el sector de telecomunicaciones no puede detenerse ante la continua evolución de las necesidades y demandas digitales de ciudadanos y empresas.

Los servicios digitales basados en tecnologías como el 5G, IoT, computación *cloud*, inteligencia artificial o los mundos virtuales, crearán nuevas oportunidades económicas y de bienestar. Sin embargo, para aprovechar al máximo este potencial, se requieren mejoras en las capacidades de las redes, como un mayor poder de procesamiento de datos y niveles de latencia más bajos.

En este contexto, el sector de las telecomunicaciones se enfrenta a un desafío fundamental: la inversión. Sin ella, la innovación se estanca. Es imperativo invertir en la modernización de las redes fijas y móviles para anticipar y satisfacer la creciente demanda digital, impulsando así una nueva era de oportunidades digitales.

Open Gateway representa la siguiente evolución de las infraestructuras al estandarizar las capacidades de red mediante la "softwarización" y virtualización, convirtiendo las infraestructuras de telecomunicaciones en plataformas digitales programables. Esto abrirá un entorno de innovación accesible para todos los desarrolladores, generando nuevas oportunidades económicas y fomentando su adopción y la transformación digital continua.

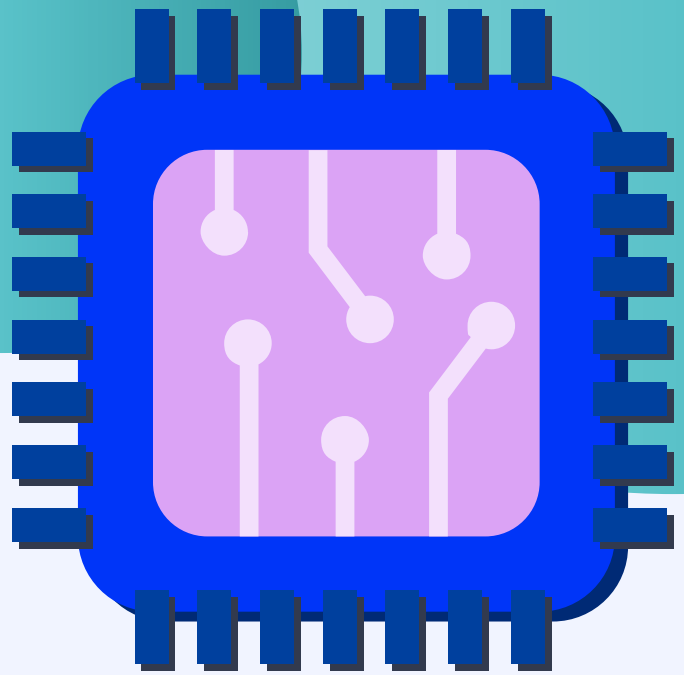
Los operadores consideran tres áreas clave de inversión para la transformación de las redes: *edge computing* para un procesamiento eficiente cerca de los usuarios; tecnologías de baja latencia como el 5G y la fibra; y redes programables a través de APIs globales y estandarizadas. Para lograrlo, se necesita un entorno que permita a los operadores sostener su esfuerzo inversor, transformarse e innovar, contribuyendo así a impulsar el liderazgo y la innovación digital en beneficio de la sociedad.

Recomendaciones

La transformación de las redes en plataformas programables para la innovación digital necesita un entorno favorable a la inversión. Esto comienza con el reconocimiento del papel estratégico del sector de las telecomunicaciones en el impulso de la innovación digital, la competitividad y el bienestar. Por ello, se recomienda:

1. **Promover estructuras de mercados sostenibles.** Reducir la fragmentación de los mercados a nivel nacional para permitir a los operadores alcanzar la escala necesaria para fortalecer la capacidad de inversión y, por tanto, de innovación del sector.
2. **Establecer un marco regulatorio que permita liberar recursos para agilizar el despliegue y la transformación de las redes.** Reducir la carga administrativa y los costes asociados, incluidas las fiscales. y simplificar los trámites burocráticos al despliegue y la transformación.
3. **Promover una política de espectro favorable a la inversión.** Generar certidumbre sobre la renovación de las licencias e incrementar la oferta armonizada de espectro en bandas medias y bajas para redes terrestres celulares y asegurar su asignación en condiciones razonables, buscando la maximización del valor del espectro para los usuarios finales.
4. **Evolucionar el marco regulatorio para impulsar la innovación y la igualdad de condiciones en el ecosistema digital.** Abordar las asimetrías con marcos horizontales que cubran aspectos como competencia, derechos del consumidor, o fiscales, eliminando enfoques sectoriales. Además, restablecer el equilibrio de la cadena de valor digital mediante el fomento de una relación justa entre los agentes y proporcionar directrices adicionales sobre la neutralidad de la red para habilitar casos de uso innovadores como los habilitados por 5G u Open Gateway.
5. **Reconocer el papel clave de la conectividad para impulsar la transición verde.** Fomentar la reorientación del flujo de inversiones hacia el despliegue de redes más eficientes, como son la fibra y el 5G.

08



Una gobernanza de la *inteligencia artificial* para el futuro

Telefónica

La IA tiene el potencial de mejorar el bienestar de la población y su inclusión, la sostenibilidad y preservar el patrimonio cultural, además de ser una palanca de competitividad fundamental en economías digitales.

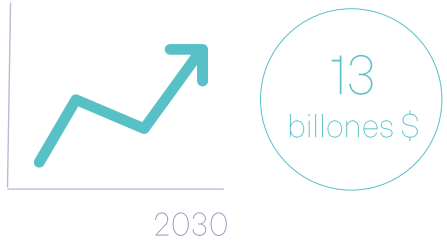
La IA como factor de la competitividad

La inteligencia artificial permite...

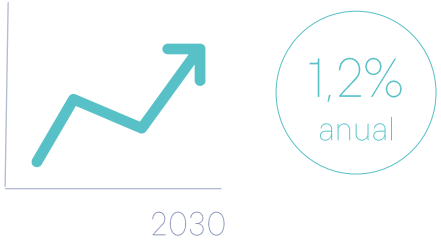
- Personalizar la experiencia
- Minimizar costes operativos
- Aumentar la productividad

+ Competitividad empresarial + Crecimiento económico

Actividad económica mundial adicional [1]



Crecimiento adicional del PIB mundial [1]



Los desafíos de la gobernanza de la IA

Necesidad de un modelo de gobernanza armonizado

Para poder desarrollar y adoptar una inteligencia artificial responsable, centrada en el ser humano y de forma confiable, es necesaria una visión holística que combine la cooperación internacional, la autorregulación, el establecimiento de políticas públicas adecuadas y un enfoque regulador basado en el riesgo.

Fragmentación global

La preocupación global ante los desafíos de la IA y la necesidad de dar una respuesta rápida para asegurar un diseño y uso responsable ha dado lugar a un entorno de políticas públicas complejo.

Brechas socioeconómicas

Un acceso desigual a la IA, ya sea a nivel micro o macro, puede agravar las brechas socioeconómicas ya que no todos los individuos o países podrán beneficiarse por igual de sus oportunidades.

Desarrollar una gobernanza de la IA que asegure el equilibrio entre la innovación, el crecimiento económico y el uso responsable de la IA

1 Impulsar una definición internacional, gobernanza y cooperación global

Adoptar una definición de IA reconocida internacionalmente, como la de la OCDE, y reforzar la cooperación internacional para establecer principios comunes y evitar la fragmentación normativa. Una definición de IA ampliamente aceptada proporciona seguridad jurídica en el enfoque normativo y de políticas públicas global, a la vez que promueve la convergencia regulatoria.

2 Promover una regulación horizontal y basada en el riesgo

Desarrollar una regulación uniforme que abarque todos los sectores y se centre en el uso de la IA, no en la tecnología misma. Esta regulación debe ser basada en el riesgo, enfocándose en mitigar los riesgos elevados mientras fomenta la innovación.

Establecer sandboxes regulatorios y testbeds para probar nuevas tecnologías y regulaciones en entornos controlados.

3 Fomentar la autorregulación y gobernanza ética

Promover la autorregulación para que las empresas asuman la responsabilidad ética y la transparencia desde el diseño de los sistemas de IA, apoyando iniciativas que establezcan estándares internos y procesos de supervisión para garantizar un desarrollo y uso responsable.

4 Fortalecer la gobernanza institucional, seguridad jurídica y coherencia regulatoria

Definir una gobernanza clara para evitar incertidumbres jurídicas y la fragmentación de la aplicación de las regulaciones que podría redundar negativamente en la competitividad de las empresas y la protección de los derechos de las personas.

Garantizar una coherencia entre la regulación de la IA y otras (GDPR, Diligencia Debida, etc.)

5 Mantener un diálogo continuo entre el sector público y privado

Mantener un diálogo continuo entre el sector público y privado que fomente la innovación continua a la vez que se proteja los derechos de las personas, la democracia y el Estado de derecho. Buscar un equilibrio entre la innovación y la regulación.

¿Quieres saber más?
Lee nuestro posicionamiento
Accede a contenido relacionado

Contexto

La inteligencia artificial (IA) se erige como la tecnología más influyente del siglo XXI, con un potencial sin precedentes. A través de técnicas avanzadas de *machine learning*, la IA puede analizar grandes volúmenes de datos de manera autónoma, facilitando la toma de decisiones y aportando soluciones innovadoras y eficaces.

Su impacto es clave para impulsar la innovación y la competitividad industrial, transformando sectores, posibilitando nuevos modelos de negocio, y redefiniendo las capacidades laborales. La IA optimiza procesos, minimiza costes operativos, personaliza la experiencia del consumidor, y aumenta la productividad, impulsando así la competitividad empresarial.

En términos globales, la IA podría incrementar la actividad económica mundial en 13 billones de dólares para 2030, lo que supondría un aumento del PIB mundial del 1,2% anual, aproximadamente. La IA tiene el potencial de mejorar el bienestar de la población –por ejemplo, a través de la optimización de la sanidad o facilitando la inclusión educativa y laboral- promover la sostenibilidad –mediante la maximización de eficiencias-, agilizar la acción humanitaria –por ejemplo, a través del análisis de datos y la elaboración de escenarios que permitan maximizar el impacto de la acción con el mínimo uso de recursos-, y preservar el patrimonio cultural –mediante una gestión inteligente y el análisis predictivo-. Las aplicaciones sectoriales son múltiples.

Por su parte, los operadores de telecomunicaciones emplean la IA para mejorar la calidad del servicio y de atención al cliente, así como la seguridad y eficiencia de sus redes.

Retos

La IA presenta oportunidades y desafíos, especialmente en cuanto a su diseño y uso responsable. Desde el inicio, ha existido un debate público donde el mayor reto es suscitar el desarrollo y la adopción de una inteligencia artificial responsable, centrada en el ser humano y de forma confiable. Es decir, promover la innovación, a la vez que se garantiza un alto nivel de protección de la salud, la seguridad, los derechos fundamentales, la democracia, el Estado de Derecho y el medio ambiente frente a potenciales efectos nocivos, fomentando así la confianza en la tecnología.

Por otra parte, el debate de la regulación requiere de una visión holística que combine la cooperación internacional, la autorregulación, el establecimiento de políticas públicas adecuadas y un enfoque regulador basado en el riesgo.

La automatización impulsada por la IA también conlleva el riesgo de desplazamiento laboral en sectores fácilmente automatizables, lo que podría tener un impacto socioeconómico significativo en los trabajadores y en la economía en general.

Asimismo, la desigualdad digital podría agravarse por el acceso desigual a la tecnología de IA, ampliando las brechas socioeconómicas existentes y limitando el acceso equitativo a sus beneficios.

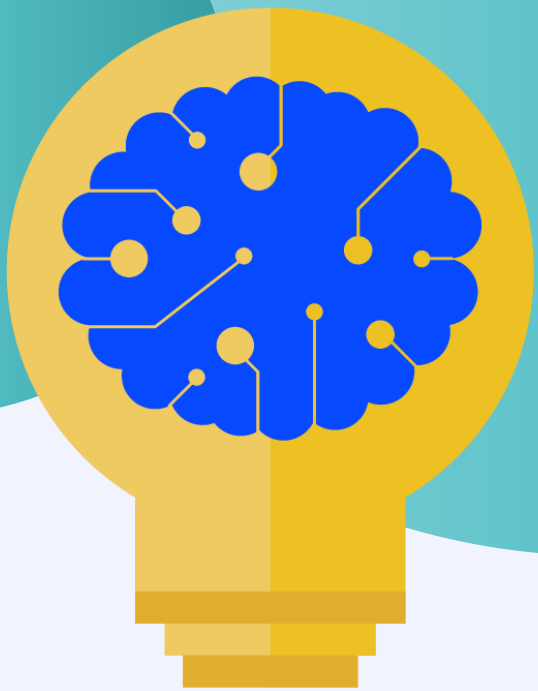
Finalmente, la preocupación sobre los desafíos, especialmente en cuanto a su diseño y uso responsable, ha dado lugar a un entorno de políticas públicas de gobernanza complejo. Entre otras propuestas figuran, a nivel multilateral, los acuerdos de la UNESCO, las definiciones de estándares ISO o propuestas en la Asamblea General de las ONU. A nivel plurilateral, se cuenta con los trabajos de la OCDE, la UE (incl. la Ley de Inteligencia Artificial) o el Consejo de Europa, el G7, el G20 o la Hoja de Ruta Conjunta sobre IA del TTC entre EE.UU. y la UE. Y, a nivel nacional, hay iniciativas como la Orden Ejecutiva de la Casa Blanca de EE.UU. sobre IA, el Marco de Gestión de Riesgos del NIST de EE.UU. o los Principios de IA del Reino Unido.

Recomendaciones

Es imprescindible desarrollar una gobernanza de la IA que asegure el equilibrio entre la innovación, el crecimiento económico y el uso responsable de la IA, que respete y proteja los derechos y la seguridad de las personas. Por ello, se recomienda:

1. **Impulsar una definición internacional, gobernanza y cooperación global.** Adoptar una definición de IA reconocida internacionalmente, como la de la OCDE, y reforzar la cooperación internacional para establecer principios comunes y evitar la fragmentación normativa. Una definición de IA ampliamente aceptada proporciona seguridad jurídica en el enfoque normativo y de políticas públicas global, a la vez que promueve la convergencia regulatoria
2. **Promover una regulación horizontal y basada en el riesgo.** Desarrollar una regulación uniforme que abarque todos los sectores y se centre en el uso de la IA, no en la tecnología misma. Esta regulación debe ser basada en el riesgo, enfocándose en mitigar los riesgos elevados mientras fomenta la innovación y cuenta con un modelo claro de gobernanza institucional. Además, establecer *sandboxes* regulatorios y *testbeds* para probar nuevas tecnologías y regulaciones en entornos controlados.
3. **Fomentar la autorregulación y gobernanza ética.** Promover la autorregulación para que las empresas asuman la responsabilidad ética y la transparencia desde el diseño de los sistemas de IA, apoyando iniciativas que establezcan estándares internos y procesos de supervisión para garantizar un desarrollo y uso responsable.
4. **Fortalecer la gobernanza institucional, seguridad jurídica y coherencia regulatoria.** Definir una gobernanza clara para evitar incertidumbres jurídicas y la fragmentación de la aplicación de las regulaciones que podría redundar negativamente en la competitividad de las empresas y la protección de los derechos de las personas. Garantizar una coherencia entre la regulación de la IA y otras (GDPR, Diligencia Debida, etc.)
5. **Mantener un diálogo continuo entre el sector público y privado.** Fomentar la innovación continua a la vez que se los derechos de las personas, la democracia y el Estado de derecho. Buscar un equilibrio entre la innovación y la regulación.

09



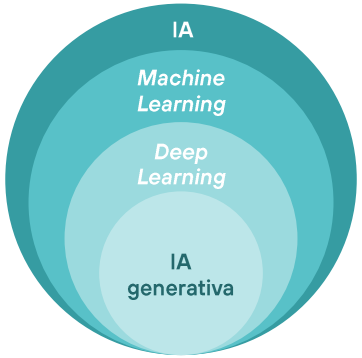
IA Generativa: competencia, propiedad intelectual y mercado laboral

La inteligencia artificial tiene el potencial de revolucionar las dinámicas sociales y económicas de los países, perfilándose como un diferenciador competitivo clave.

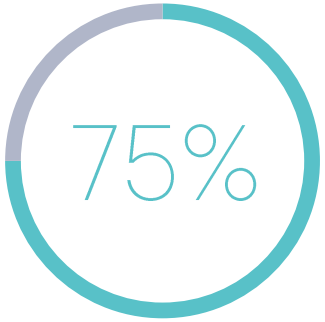
La llegada de la inteligencia artificial generativa

La IA impulsa la innovación y la productividad, abriendo la puerta a nuevas oportunidades de negocio y a un crecimiento económico de empresas y países.

Los modelos generativos son el último avance en el campo de la inteligencia artificial. No obstante, aún estamos en las primeras fases. Estamos lejos de ver todo su potencial.



Se estima que la IA generativa tiene el potencial de generar anualmente un valor equivalente a entre 2.600 y 4.400 miles de millones de dólares [1] en beneficios empresariales a escala mundial.



El 75% del valor creado [1] por la IA Generativa procederá de:

- Operaciones con clientes
- Marketing y ventas
- I+D
- Ingeniería de software

Los desafíos de la inteligencia artificial generativa

Garantizar los derechos humanos y valores democráticos

Un uso irresponsable de la IA Generativa puede socavar los derechos humanos y principios democráticos en los que se basan nuestras sociedades a través de la desinformación, ataques a la privacidad o la vigilancia masiva, entre otros.

Competencia justa en los mercados y competitividad

Con acceso a recursos como los datos, la capacidad de computación, financiación y personal especializado concentrados en pocas empresas existe el riesgo de abuso de dominancia, limitando la innovación.

Debate de propiedad industrial y derechos de autor

Input Entrenamiento masivo de la IA con obras preexistentes protegidas por copyright

Output Protección y titularidad de la obra o patente creada con IA

Impacto en el mercado laboral

Automatización de tareas rutinarias y repetitivas + Reentrenamiento para usar la IA como herramienta

Desarrollar políticas y normas que impulsen un impacto positivo en la propiedad intelectual, la competencia justa en los mercados y el ámbito laboral

1 Establecer políticas que promuevan una competencia justa, fomenten la innovación, y fortalezcan las capacidades regionales

Garantizar el cumplimiento de normas de derecho de la competencia para evitar abusos de posición dominante.

Promover diferentes modelos de negocio y la innovación a través del apoyo a empresas emergentes.

Fortalecer las capacidades locales mediante programas de formación.

Estimular la inversión.

2 Fomentar entornos normativos flexibles y promover el diálogo público-privado en el ámbito de la propiedad intelectual e industrial

Comprender los retos relacionados con la propiedad intelectual e industrial en el desarrollo de la IA Generativa, promoviendo entornos flexibles y adaptables en los distintos marcos normativos.

Incentivar el diálogo continuo entre el sector público y privado para equilibrar y abordar los desafíos que surgen de la implementación de esta tecnología.

3 Priorizar la inversión en desarrollo de competencias y establecer políticas para limitar la brecha en habilidades digitales en el ámbito laboral

Poner foco en la educación, formación y programas de aprendizaje permanente para equipar a la mano de obra con habilidades necesarias para una economía impulsada por la IA.

Desarrollar políticas a favor de la inclusión digital y programas de reciclaje para apoyar a los trabajadores afectados por la automatización, garantizando una transición hacia nuevas oportunidades de empleo.

¿Quieres saber más?
Lee nuestro posicionamiento
Accede a contenido relacionado

Contexto

Los modelos generativos de inteligencia artificial (IAGen) representan el último avance en el campo del aprendizaje automático, permitiendo la generación de una amplia variedad de contenido, desde texto e imágenes hasta música y vídeo, mediante la identificación de patrones en enormes conjuntos de datos.

Esta evolución tecnológica ha despertado un gran interés debido a su potencial para impulsar la innovación y generar nuevas oportunidades de negocio en todos los sectores. Según estimaciones, la IA generativa tiene el potencial de generar anualmente un valor equivalente a entre 2.600 y 4.400 miles de millones de dólares en beneficios empresariales a escala mundial, siendo el 75% de este valor atribuido a casos de uso en operaciones con clientes, marketing y ventas, ingeniería de software e investigación y desarrollo (I+D).

Sin embargo, a pesar del entusiasmo generado por las capacidades de la IA generativa, aún nos encontramos en las primeras fases de su desarrollo y aplicación práctica. Se ha identificado una serie de desafíos y preocupaciones, que van desde cuestiones éticas y de privacidad hasta posibles sesgos en los datos y la necesidad de comprender y mitigar los riesgos asociados con el uso generalizado de estas tecnologías.

En este contexto, la importancia de una gobernanza efectiva de la IA y la IAGen se vuelve fundamental. Este marco de gobernanza incluye una variedad de enfoques, desde la regulación gubernamental hasta la autorregulación por parte de las entidades involucradas en el desarrollo y uso de la IA. La regulación gubernamental busca establecer estándares y directrices claras para el uso ético y responsable de la IA, mientras que la autorregulación por parte de las empresas y organizaciones promueve la adopción de prácticas éticas y transparentes en el desarrollo y despliegue de sistemas de IA.

Retos

Si bien la IAGen puede ser una herramienta poderosa para mejorar el acceso a la educación, la atención médica y otros servicios vitales, también nos enfrentamos a una serie de desafíos éticos, regulatorios y sociales que debemos abordar con urgencia y determinación.

Un uso irresponsable de esta tecnología puede socavar los derechos humanos y principios democráticos en los que se basan nuestras sociedades a través de la desinformación, ataques a la privacidad o la vigilancia masiva, entre otros.

En términos de desarrollo y despliegue de modelos y aplicaciones de IA, incluido IAGen, solo unas pocas empresas tecnológicas tienen las capacidades técnicas y los recursos financieros necesarios para desarrollar los modelos más avanzados. Esto puede generar desequilibrios al crear barreras de entrada para empresas más pequeñas y concentrar el poder en manos de unas pocas grandes corporaciones.

En el ámbito de la propiedad intelectual e industrial, los rápidos avances en IAGen han dado lugar a una amplia gama de herramientas asequibles y de fácil acceso para la generación de contenidos de toda clase. No obstante, plantea desafíos relacionados tanto con sus formas de entrenamiento masivo de la IA por la utilización que pueda hacer de obras preexistentes (input) protegidas por copyright, como con la protección y titularidad de los resultados o patentes obtenidos por su uso (output). Esto ha dado lugar a un debate sobre los derechos de autor de los contenidos creados y sobre la propiedad de las patentes de productos industriales.

Finalmente, la IAGen tiene el potencial de automatizar tareas rutinarias y repetitivas, lo que puede aumentar la eficiencia, pero también generar preocupaciones sobre la pérdida de empleos y la necesidad de reentrenamiento para puestos más especializados.

Recomendaciones

El modelo de gobernanza de la IA, incluida la IAGen, debe asegurar el equilibrio entre la innovación, el crecimiento económico y el uso responsable de la IA. Por ello, se recomienda:

1. **Establecer políticas que promuevan una competencia justa, fomenten la innovación, y fortalezcan las capacidades regionales.** Garantizar el cumplimiento de normas de derecho de la competencia para evitar abusos de posición dominante, promover diferentes modelos de negocio y la innovación a través del apoyo a empresas emergentes, fortalecer las capacidades locales mediante programas de formación, y estimular la inversión.

2. **Fomentar entornos normativos flexibles y promover el diálogo público-privado en el ámbito de la propiedad intelectual e industrial.** Comprender los retos relacionados con la propiedad intelectual e industrial en el desarrollo de la IA Generativa, promoviendo entornos flexibles y adaptables en los distintos marcos normativos. Además, se debe incentivar el diálogo continuo entre el sector público y privado para equilibrar y abordar los desafíos que surgen de la implementación de esta tecnología.

3. **Priorizar la inversión en desarrollo de competencias y establecer políticas para limitar la brecha digital en el ámbito laboral.** Poner foco en la educación, formación y programas de aprendizaje permanente para equipar a la mano de obra con habilidades necesarias para una economía impulsada por la IA, al tiempo que se desarrollan políticas a favor de la inclusión digital y programas de reciclaje para apoyar a los trabajadores afectados por la automatización, garantizando una transición hacia nuevas oportunidades de empleo.

10

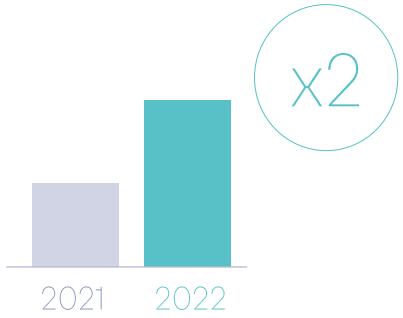
Las redes de telecomunicaciones y los *Mundos Virtuales*: una nueva era de Internet

Expectativas de crecimiento del Metaverso [1]

El 59% de los consumidores trasladarían su actividad diaria (interacción social, gaming, viajes, comercio...) al Metaverso.

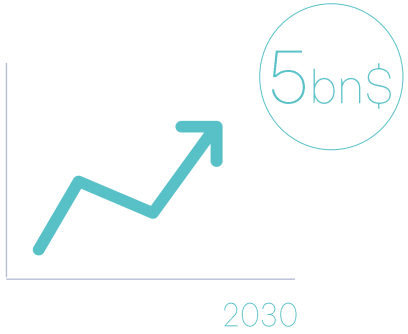
2022

Se duplicó la cantidad invertida en el desarrollo del Metaverso respecto al año anterior, alcanzando los 120.000 millones de dólares a nivel global.



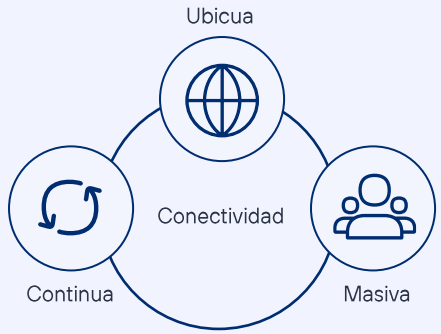
2030

Se estima que el Metaverso podría generar hasta 5 millones de millones de dólares a nivel global en aplicaciones empresariales y de consumo.



Para que los Mundos Virtuales alcancen todo su potencial es necesario poder ofrecer una experiencia continua, ubicua y masiva.

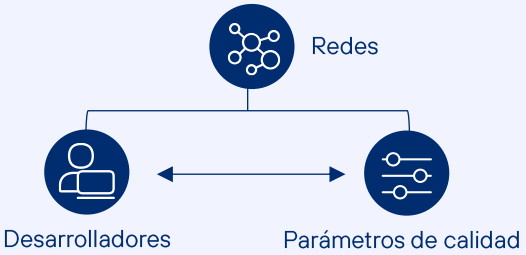
Para ello, las redes deberán evolucionar hacia un modelo programable, descentralizado y próximo al usuario final.



Evolución de las redes de telecomunicaciones

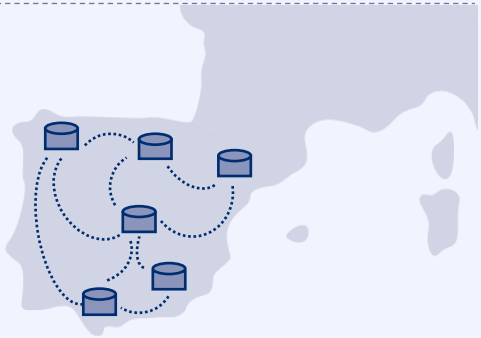
API-ficación de las redes

Los desarrolladores de aplicaciones y servicios del Metaverso podrán programar y definir los parámetros de calidad que necesitan para su servicio gracias a interfaces (APIs).



Modelo de Content Delivery Networks (CDN)

Para acercar el contenido al usuario desde diferentes puntos geográficos. Esto da lugar a nuevos modelos de negocio en los que se retribuye al proveedor de la CDN por entregar el contenido con mayor calidad.



Evolucionar las redes de telecomunicaciones para que el Metaverso y los Mundos Virtuales sean una realidad

1. Evitar la extensión automática de la regulación tradicional al nuevo paradigma tecnológico de los Mundos Virtuales

   Diseñar una regulación adaptada a las nuevas tecnologías, servicios y modelos de negocio. Interpretaciones incorrectas, o sesgadas por criterios no meramente técnicos podrían crear incertidumbre.

2. Promover un level playing field para el desarrollo armónico de los Mundos Virtuales

   Establecer un level playing field para todos los agentes de la cadena de valor digital que se encuentren en situaciones regulatorias similares, permitiéndoles encontrar incentivos adecuados a todos ellos.

3. Evitar la precipitación en las decisiones regulatorias

   Redoblar la cautela en las decisiones regulatorias previas a cualquier intervención que se tome en este mercado, teniendo en cuenta los efectos de la misma sobre la eficiencia y eficacia en la asignación de recursos a que dan lugar las APIs.

4. Facilitar la colaboración entre los operadores en la estandarización

   Poner a disposición interfaces homogéneos por parte de los operadores a los desarrolladores de los Mundos Virtuales es una condición indispensable para el éxito esta nueva era.

¿Quieres saber más?
Lee nuestro posicionamiento
Accede a contenido relacionado

Contexto

En 2021, el cambio de nombre de Facebook a Meta inició el "boom" del metaverso. Hasta el momento, el Metaverso era un concepto de ciencia ficción lejano a la realidad. No obstante, la ola de innovación desatada por Meta llevó a grandes empresas tecnológicas a una carrera por crear el primer mundo virtual en el metaverso.

El metaverso es una red de entornos virtuales a los que se accede a través de diferentes dispositivos y en los que los usuarios pueden interactuar, socializar, trabajar, jugar y consumir en un entorno digital inmersivo que refleja muchos de los hábitos en el mundo real.

A día de hoy, las empresas continúan innovando e invirtiendo en tecnologías en las que se apoyará en metaverso, como la realidad virtual y aumentada, acercándonos poco a poco a una primera versión de lo que serán los Mundos Virtuales.

Se espera que el valor económico de los Mundos Virtuales aumente en los próximos años debido a mejoras tecnológicas, la demanda de los consumidores hacia nuevas experiencias y las nuevas oportunidades de negocio para las empresas. De acuerdo a un estudio realizado por McKinsey, el 59% de los consumidores trasladarían su actividad diaria (interacción social, *gaming*, viajes, comercio...) al metaverso. Por otra parte, la inversión en metaverso se duplicó en 2022 respecto a 2021, alcanzando los 120.000 millones de dólares. En 2030, se estima que el metaverso podría generar entre 4 y 5 billones de dólares en casos de uso empresarial y de consumo.

La iniciativa de la Comisión Europea *Virtual Worlds* busca posicionar a Europa a la cabeza del desarrollo de los Mundos Virtuales. La Comisión velará por que se reflejen los valores y derechos fundamentales de la UE y se fomente la innovación para las empresas y la sociedad europea.

Retos

El metaverso debe ofrecer una experiencia continua, ubicua y masiva. Ello supone para las redes de telecomunicaciones el tener que asegurar calidades de servicio con las mismas exigencias de continuidad, ubiquidad y predictibilidad.

Por tanto, la nueva era de Internet estará caracterizada por una experiencia personalizada, más rápida y con una menor latencia. Sin embargo, actualmente, el modelo de Internet está limitado por los requisitos de *best effort* (no necesitan asegurar ninguna calidad concreta) y *service agnosticism* (no necesitan conocer los servicios que se ofrecen sobre ellas).

Las redes de telecomunicaciones necesitarán evolucionar hacia un modelo programable, descentralizado y próximo al usuario final.

En primer lugar, la "API-ficación" de las redes permitirán una nueva relación entre las redes de telecomunicaciones y las aplicaciones y servicios. En este sentido, los desarrolladores de aplicaciones y servicios de los Mundos Virtuales podrán programar y definir los parámetros de calidad que necesitan para que su servicio funcione correctamente.

En segundo lugar, aplicando el actual modelo de *Content Delivery Networks* (CDNs), se puede acercar el contenido al usuario desde diferentes puntos geográficos, mejorando la calidad del servicio. Esto también da lugar a nuevos modelos de negocio donde los dueños del contenido pagan a terceros (CDNs) por entregar dicho contenido más cerca de los usuarios. Así, no es el usuario final quien paga por tener los contenidos cerca y mejorar la calidad de los mismos, sino que delega dicha decisión (y pago) en los oferentes de dichos servicios.

Recomendaciones

Para que una nueva era de Internet caracterizada por la proliferación de Mundos Virtuales o metaversos sea posible, se necesita evolucionar las redes de telecomunicaciones. Por ello, se recomienda:

1. **Evitar la extensión automática de la regulación tradicional al nuevo paradigma tecnológico requerido por los Mundos Virtuales.** Diseñar una regulación adaptada a las nuevas tecnologías, servicios y modelos de negocio. Interpretaciones incorrectas, o sesgadas por criterios no meramente técnicos podrían crear incertidumbre.

2. **Promover un level playing field para el desarrollo armónico de los Mundos Virtuales.** Establecer un *level playing field* para todos los agentes de la cadena de valor digital que se encuentren en situaciones regulatorias similares, permitiéndoles encontrar incentivos adecuados a todos ellos.

3. **Evitar la precipitación en las decisiones regulatorias para no distorsionar el funcionamiento de los Mundos Virtuales.** Redoblar la cautela en las decisiones regulatorias previas a cualquier intervención que se tome en este mercado, teniendo en cuenta los efectos de la misma sobre la eficiencia y eficacia en la asignación de recursos a que dan lugar las APIs.

4. **Facilitar la colaboración entre los operadores en la estandarización.** Poner a disposición interfaces homogéneos por parte de los operadores a los desarrolladores de los Mundos Virtuales es una condición indispensable para el éxito esta nueva era.

11

Ciberseguridad: fortaleciendo la resiliencia y la confianza en un mundo digital global

La importancia de la ciberseguridad

Top 10

La ciber-inseguridad, uno de los 10 riesgos principales [1]

x2

Los ciberataques se duplicaron desde la pandemia [2]

9,5bn $

... es el coste mundial de ciberataques en 2024 [3]

29%

... de las organizaciones sufrieron un ciber-incidente en el último año [2]

41%

... de los ciber-incidentes proceden de la cadena de suministro [2]

91%

... de los directivos prevén un ciber-incidente de alto impacto en los próximos dos años [2]

Hay una brecha creciente entre las organizaciones que son ciber-resilientes y las que no lo son

Piensan que carecen de la ciber-resiliencia necesaria [2]

x2 pymes vs grandes empresas

Cuentan con un ciber-seguro [2]

< 25% pymes vs 75% grandes empresas

En este nuevo mundo, la ciberseguridad desempeña un papel clave en la protección de empresas y gobiernos contra los riesgos.

Los obstáculos para lograr un entorno ciberseguro

Las empresas que presentan mayor exposición al riesgo son las que:

están en sectores digitalizados y conectados, pero sin protección adecuada

cuentan con activos más interesantes para los atacantes

están en países con mayor riesgo estratégico y/o peor ciber-legislación

No se perciben los beneficios de las inversiones en ciberseguridad

A diferencia de otras inversiones, y como en el caso de I+D, no es sencillo justificar la rentabilidad de inversiones en mejora de resiliencia que ofrece la ciberseguridad.

Los marcos regulatorios están fragmentados y son complejos

Las políticas y la regulación se perfilan en la actualidad como un marco fragmentado, complejo, transversal y en constante evolución.

Hay escasez de personal especializado

En 2023, la brecha de profesionales en ciberseguridad ascendió a 4 millones, aproximadamente, en todo el mundo [4]. La profesión necesita casi duplicarse para estar a plena capacidad.

Desarrollar la ciber-resiliencia y aumentar la confianza digital para una digitalización integradora, mediante una mejor colaboración, marcos adecuados, desarrollo de capacidades e incentivos

1	Potenciar la cooperación multilateral contra la ciberdelincuencia	Prevenir, identificar y contener incidentes, desde la investigación hasta la acción legal, mejorando la coordinación internacional y multilateral contra la ciberdelincuencia y proporcionando recursos y capacidades necesarios.
2	Fomentar mejores prácticas en ciberseguridad	Promover unos estándares de mínimos que incluyan el desarrollo de agencias independientes de ciberseguridad dotadas de recursos, estrategias y planes de ciberseguridad, incentivando el uso privado y público de marcos internacionales de seguridad (ej. ISO) y de certificados reconocidos para facilitar la transparencia y armonización.
3	Mejorar la armonización, la coherencia y la coordinación multi-stakeholder	Evitar solapamiento o incoherencia de normativas e implementaciones y abordar la coordinación entre autoridades competentes y con las empresas, la coherencia en los sistemas de notificación de incidentes, así como la compartición de ciber-inteligencia.
4	Explorar nuevos mecanismos de financiación e incentivos fiscales	Explorar nuevos mecanismos de financiación e incentivos, entre ellos fiscales, para inversión en ciberseguridad, resiliencia, capacitación y cultura de ciberseguridad.
5	Definir y supervisar nuevos indicadores clave a nivel internacional	Definir y supervisar a nivel internacional nuevos indicadores de inversión en ciberseguridad y personal especializado, frente a la ausencia de estadísticas fiables de seguimiento en el ámbito de la ciberseguridad.
6	Establecer requisitos mínimos para reforzar la calidad de las ciber-agencias de calificación	Definir requisitos de transparencia, información, metodología sólida para reforzar la calidad de las ciber-agencias de calificación, con una regulación similar a la de las agencias de calificación crediticia y constituir un registro oficial de agencias de ciberrating autorizadas para dar más confianza a todo el ecosistema.

¿Quieres saber más?
Lee nuestro posicionamiento
Accede a contenido relacionado

Telefónica

Contexto

La acelerada digitalización, combinada con el crecimiento de las tensiones geopolíticas, ha venido acompañada de un aumento de la polarización, la erosión de la confianza y la ciber-inseguridad. El Foro Económico Mundial identifica la ciber-inseguridad como uno de los 10 principales riesgos, y los ciberataques son una de las tres mayores preocupaciones de los sectores público y privado a nivel global.

Desde la pandemia, el número de ciberataques se ha duplicado. El 29% de las organizaciones ha sufrido uno en el último año y el 91% de los directivos cree que podría producirse un ciber-incidente de alto impacto en los próximos dos años. La cadena de suministro y el ecosistema de las organizaciones son especialmente relevantes, ya que el 41% de los ciber-incidentes tienen su origen en terceros. Y lo que es más preocupante, existe una brecha cada vez mayor entre las organizaciones que son ciber-resilientes y las que no lo son, como demuestra el hecho de que menos de una cuarta parte de las PYMEs cuenten con un ciber-seguro, frente al 75% de las de mayor tamaño y que más del doble de PYMEs que de grandes organizaciones afirman carecer de la ciber-resiliencia necesaria para satisfacer sus requisitos operativos críticos, lo que puede retrasar su progreso en el mundo digital.

El coste de los ciberataques o de las filtraciones es cada vez más elevado: el coste medio por incidente en grandes organizaciones asciende a 4 millones de dólares El coste mundial está en torno a 9,5 millones de millones de dólares para 2024, lo que equivale a la tercera economía mundial después de Estados Unidos y China.

La ciber-inseguridad conlleva costes directos e indirectos, riesgos para la seguridad y la privacidad de las personas, costes derivados de la interrupción de los servicios, incluidos servicios críticos para la sociedad, pago de rescates, pérdida de datos e información relevante, responsabilidad legal ante terceros, sanciones o pérdida de reputación con el consecuente impacto en la valoración o incluso viabilidad empresarial.

Retos

Los avances en la digitalización sólo pueden ir de la mano de una adecuada ciber-resiliencia, fomentando la confianza y la inclusión de todo el tejido productivo. Las empresas en sectores más conectados o con activos más interesantes para los atacantes, con peor protección (como las PYMEs), en países de mayor riesgo geoestratégico o con peor regulación, son las que presentan una mayor exposición al riesgo.

El mayor éxito de la ciberseguridad es silencioso, por lo que las empresas pueden tener dificultades para justificar la rentabilidad de inversión en resiliencia. En efecto, los agentes tienden a reforzar sus ciberdefensas después de un incidente, lo que indica que se produce un proceso de aprendizaje dinámico. Al igual que en otras inversiones como la I+D, los incentivos privados para hacer frente a los riesgos de ciberseguridad pueden diferir del óptimo social.

Las políticas y la regulación en materia de ciberseguridad para aumentar la ciber-resiliencia se perfilan en la actualidad como un marco fragmentado, complejo, transversal y en constante evolución, que busca orientarse a los riesgos, en un mundo digital global con tensiones geopolíticas, en el que surgen nuevas tecnologías.

Los motivos de los ataques varían, si bien los atacantes suelen estar movidos por el dinero (bandas organizadas), pero también por el reconocimiento y las causas políticas o sociales. No es suficiente aumentar la ciber-resiliencia (mejorar el escudo), sino que es imprescindible avanzar de forma efectiva en la lucha contra el cibercrimen que trasciende las fronteras nacionales.

En este entorno, el ciberseguro desempeña un papel clave en la protección contra los riesgos. Los costes del ciberseguro están aumentando y las agencias de calificación de ciberseguridad están ganando protagonismo en un contexto de falta de transparencia y de regulación, a diferencia de las agencias de calificación crediticia.

Por último, existe una grave carencia de profesionales expertos y de cultura de la ciberseguridad. La mejora de la ciber resiliencia necesita casi del doble de profesionales de los actuales.

Recomendaciones

En un mundo cada vez más conectado, desarrollar la ciber-resiliencia y aumentar la confianza digital, para una digitalización integradora, requiere de una mejor colaboración, marcos adecuados, desarrollo de capacidades e incentivos. Por ello, se recomienda:

1. **Potenciar la cooperación multilateral contra la ciberdelincuencia,** Prevenir, identificar y contener incidentes, desde la investigación hasta la acción legal, mejorando la coordinación internacional y multilateral y proporcionando recursos y capacidades necesarios.
2. **Fomentar mejores prácticas en ciberseguridad.** Promover unos estándares de mínimos que incluyan el desarrollo de agencias independientes de ciberseguridad con recursos, estrategias y planes de ciberseguridad, incentivando uso de marcos internacionales de seguridad (ej. ISO) y de certificados reconocidos, promoviendo transparencia y armonización.
3. **Mejorar la armonización, la coherencia y la coordinación multi-stakeholder.** Evitar solapamiento o incoherencia de normativas e implementaciones y abordar la coordinación entre autoridades competentes y las empresas, la coherencia en los sistemas de notificación de incidentes, y la compartición de ciber-inteligencia.
4. **Explorar nuevos mecanismos de financiación e incentivos fiscales para la mejora de la ciber-resiliencia, capacitación, y cultura** para afrontar las inversiones necesarias y escasez de ciber-profesionales.
5. **Definir y supervisar nuevos indicadores clave a nivel internacional.** De inversión en ciberseguridad y personal especializado, frente a la ausencia de estadísticas fiables.
6. **Establecer unos requisitos mínimos para reforzar la calidad de las ciber-agencias de calificación.** Definir requisitos de transparencia, información, metodología, con una regulación similar a la de calificación crediticia y constituir un registro oficial de agencias de *ciberrating* autorizadas para mayor confianza.

12

Sistemas de Alerta Temprana: un escudo vital contra desastres naturales

En 2022, se registraron 387 desastres naturales en todo el mundo, que causaron la pérdida de 30.704 vidas y afectaron a 185 millones de personas [1]

El 95% de la población global está cubierta por una red móvil y hay 5.600 millones de abonados únicos a la telefonía móvil en todo el mundo. Esta red desempeña un papel vital en la difusión y comunicación de alertas tempranas ante riesgos [1]

Sistemas de alerta temprana con la red móvil como canal

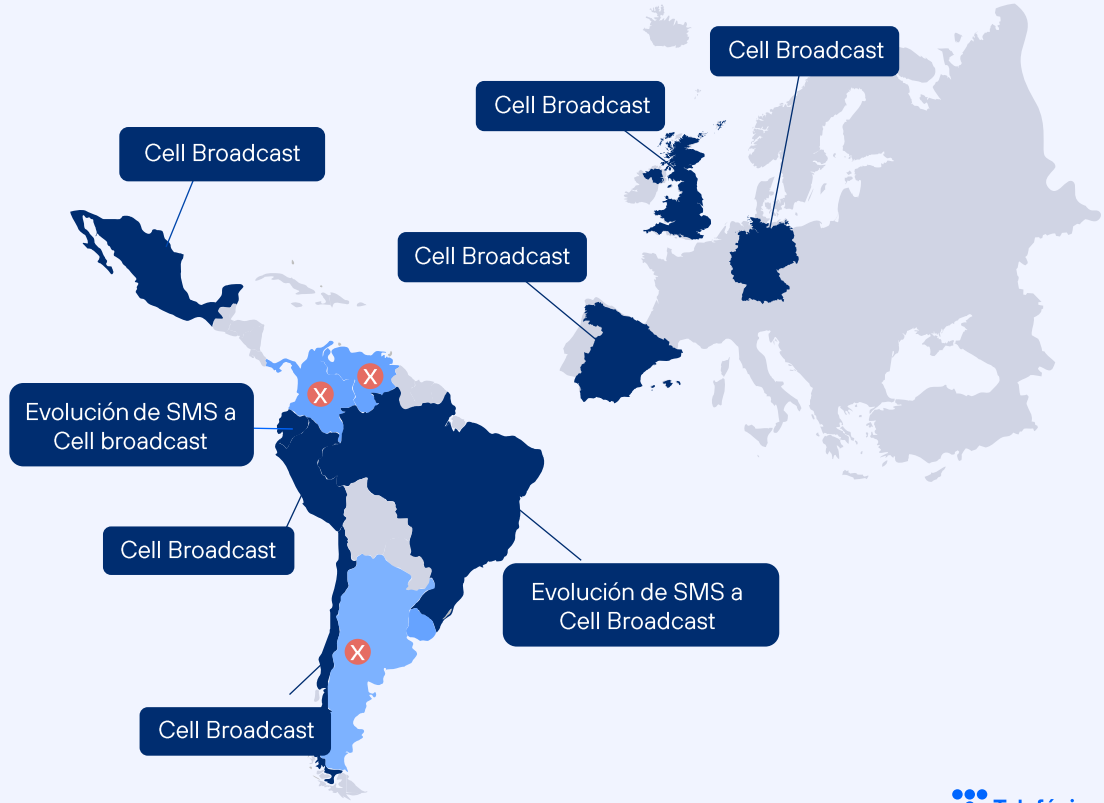
Cell broadcast es la tecnología más eficaz

Early Warnings for All

La iniciativa "Alerta Temprana para Todos" de la ONU busca que para 2027, toda la población mundial esté cubierta por un sistema de alerta temprana, garantizando la protección universal ante fenómenos hidrometeorológicos, climatológicos y ambientales peligrosos.

El compromiso de los operadores con los sistemas de alerta temprana

Cell Broadcast es la tecnología más extendida en los países Telefónica



Telefónica

Acelerar el despliegue y la eficacia de los sistemas de alerta temprana con la integración de las redes móviles como canal de comunicación crucial y complementario, dentro de un enfoque multicanal

1 Impulsar la colaboración entre el sector público y privado

Compartir conocimiento y mejores prácticas entre operadores, fabricantes de dispositivos, de software, responsables gubernamentales, organizaciones internacionales o expertos en emergencia, entre otros. En particular, los operadores móviles aportan experiencia técnica y conocimientos, y ponen sus equipos a disposición de los centros de emergencia.

2 Establecer marcos regulatorios alineados con la financiación de estos servicios

Establecer un marco normativo que genere certidumbre e incentivos al despliegue de sistemas de alerta temprana.

Explorar soluciones innovadoras de financiación viables a largo plazo que garanticen la financiación de los costes iniciales y continuos.

3 Promover la adopción de la solución tecnológica más eficaz en base a la realidad nacional, regional o local

Tener en cuenta las tecnologías y la gama de terminales disponible de cada país/zona. Sin embargo, la tecnología cell broadcast debiera de ser priorizada por sus ventajas e integrarla en los planes de emergencia existentes.

Promover la homologación de dispositivos para asegurar su compatibilidad con el servicio de alerta temprana.

Promover el enfoque multicanal para la difusión a través de distintos canales y el desarrollo de un protocolo común para la coherencia de la alerta entre canales, impulsando el alcance de la alerta.

4 Fomentar la concienciación de la población

Preparar a la población y aumentar su confianza y familiaridad con pruebas periódicas y campañas de sensibilización. Estos simulacros y campañas son clave para garantizar la efectividad del servicio de alerta y deben ser dirigidas por el Gobierno, al tratarse de un servicio público, y acentuar el papel de los operadores como un canal más en la difusión de las alertas.

¿Quieres saber más?
Lee nuestro posicionamiento
Accede a contenido relacionado

Contexto

El aumento de catástrofes naturales vinculadas al cambio climático ha resaltado la urgencia de implementar soluciones tecnológicas para alertar rápidamente a la población sobre peligros inminentes. La iniciativa "Alerta Temprana para Todos" de las Naciones Unidas, lanzada en 2022, busca asegurar que para 2027 todas las personas en el mundo estén cubiertas por un sistema de alerta temprana, garantizando protección universal ante fenómenos hidrometeorológicos, climatológicos y ambientales peligrosos.

Un sistema completo y eficiente de alerta temprana integra cuatro funciones fundamentales: la evaluación de los riesgos; la monitorización y previsión de desastres naturales; la comunicación y difusión de la alerta; y la capacidad de respuesta.

En este contexto, la disponibilidad de banda ancha y el alto uso de dispositivos móviles con acceso a Internet convierten a los operadores y su red móvil en un canal crucial para la difusión de las alertas. Hoy en día, los sistemas de alerta temprana más efectivos se caracterizan por un enfoque multicanal. Gracias al avance tecnológico, la red y los dispositivos móviles se han integrado en estos sistemas complementando a los medios tradicionales de difusión de alertas, como la radio, la TV, los periódicos, las vallas publicitarias o las sirenas, potenciando su alcance y mejorando la efectividad de este servicio público en beneficio de las comunidades y la seguridad de las personas.

Cell broadcast es la tecnología más eficaz y fiable para la entrega masiva de alertas móviles en segundos y la más implantada en todo el mundo. A diferencia de los SMS, esta tecnología envía la alerta a todos los teléfonos móviles conectados en un área geográfica determinada, incluidos los móviles itinerantes, sin necesidad de conocer el número, preservando la privacidad, salvando vidas y mitigando daños.

Retos

Impulsar el despliegue y la eficiencia de estos sistemas requiere afrontar varios desafíos. En primer lugar, muchos países, especialmente en desarrollo, carecen de la infraestructura necesaria de un sistema de alerta temprana, o, si la tienen, ésta no integra a las redes móviles como canal de difusión de la alerta.

A esto se suma, la falta de conocimiento sobre las tecnologías involucradas y/o socios tecnológicos, junto con la disparidad en la disponibilidad y calidad de las redes móviles, así como los problemas de compatibilidad de dispositivos móviles con el servicio de alerta temprana.

Del mismo modo, garantizar recursos financieros a largo plazo y establecer modelos de financiación sostenibles es crucial para la viabilidad de estos sistemas. Es relevante destacar que, si bien las agencias gubernamentales son responsables de emitir las alertas, los operadores de telecomunicaciones solo proveen la infraestructura de red y actúan como un canal de transmisión más. No obstante, el despliegue de estos sistemas requiere inversiones considerables en infraestructura, tecnología y recursos humanos, que afecta tanto a las agencias gubernamentales como a los operadores móviles.

Por otro lado, la ausencia de un marco normativo que fomente el despliegue de estos sistemas es otro de los retos. La dependencia de este servicio público de las redes móviles pone el foco en la regulación para agilizar su implementación e integración en los planes de emergencia. El artículo 110 del Código Europeo de Comunicaciones Electrónicas, por ejemplo, ha subrayado el papel crucial de la regulación en la aceleración del despliegue en países europeos.

Finalmente, la falta de conocimiento del servicio o sensibilización de la población puede conducir a la ineficacia de las alertas.

Recomendaciones

La modernización de los sistemas de alerta temprana ante posibles catástrofes naturales supone la integración de las redes móviles como un canal de comunicación crucial. Por ello, se recomienda:

1. **Impulsar la colaboración entre el sector público y privado.** Compartir conocimiento y mejores prácticas entre operadores, fabricantes de dispositivos, de software, responsables gubernamentales, organizaciones internacionales o expertos en emergencia, entre otros. En particular, los operadores móviles aportan experiencia técnica y conocimientos, y ponen sus equipos a disposición de los centros de emergencia.

2. **Establecer marcos regulatorios claros y de incentivos alineados con la financiación de estos servicios.** Establecer un marco normativo que genere certidumbre e incentivos al despliegue de sistemas de alerta temprana, así como explorar soluciones innovadoras de financiación viables a largo plazo que garanticen la financiación de los costes iniciales y continuos.

3. **Promover la adopción de la solución tecnológica más eficaz en base a la realidad nacional, regional o local.** Es necesario tener en cuenta las tecnologías y la gama de terminales disponible en cada zona. Sin embargo, la tecnología *cell broadcast* debiera priorizarse por sus ventajas e integrarla en los planes de emergencia existentes. También, promover la homologación de dispositivos es clave para garantizar la eficacia en la difusión de la alerta, así como combinar distintos canales (multicanal) y promover el desarrollo de un protocolo común para la coherencia de la alerta entre canales.

4. **Fomentar la concienciación de la población.** Preparar a la población y aumentar su confianza y familiaridad con pruebas periódicas y campañas de sensibilización. Estos simulacros y campañas son clave para garantizar la efectividad del servicio y deben ser dirigidas por el Gobierno, al tratarse de un servicio público, y acentuar el papel de los operadores como un canal más en la difusión de las alertas.

Referencias | Innovación tecnológica

07 *Conectividad:* El poder transformador de las telecomunicaciones y su impacto en la innovación

(1) Telefónica (2024). El poder transformador de las telecomunicaciones y su impacto en la innovación. Disponible en: https://www.telefonica.com/es/wp-content/uploads/sites/4/2023/12/Poder-transformador-telecomunicaciones-impacto-innovacion-posicionamiento-2023.pdf
(2) Telefónica: #Conectividad. Disponible en: https://www.telefonica.com/es/tag/conectividad/

08 Una gobernanza de la *inteligencia artificial* para el futuro

(1) McKinsey (2018). Notes from the AI frontier: Modeling the impact of AI on the world economy. Disponible en: https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy
(2) McKinsey (2023). AI could increase corporate profits by 4 trillion a year according to new resech. Disponible en: https://www.mckinsey.com/mgi/%20overview/in-the-news/ai-could-increase-corporate-profits-by-4-trillion-a-year-according-to-new-research
(3) Telefónica (2023). Inteligencia Artificial: Innovación, ética y educación. Disponible en: https://www.telefonica.com/es/wp-content/uploads/sites/4/2023/06/Posicionamiento-Inteligencia-Artificial-innovacion-etica-y-regulacion.pdf
(4) Telefónica: #Inteligencia Artificial. Disponible en: https://www.telefonica.com/es/tag/inteligencia-artificial/

09 *IA Generativa:* competencia, propiedad intelectual y mercado laboral

(1) Telefónica (2024). Inteligencia Artificial e IA Generativa: gobernanza, competencia, propiedad intelectual y mercado laboral. Disponible en: https://www.telefonica.com/es/wp-content/uploads/sites/4/2024/09/Inteligencia-Artificial-e-IA-Generativa.-Posicionamiento-2024-1.pdf

10 Las redes de telecomunicaciones y los *Mundos Virtuales:* una nueva era de Internet

(1) McKinsey (2022). Value creation in the metaverse. Disponible en: www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf
(2) Telefónica (2023). Las redes de telecomunicaciones y el Metaverso. Disponible en: https://www.telefonica.com/es/wp-content/uploads/sites/4/2023/02/Telefonica-Las-redes-de-telecomunicaciones-y-el-Metaverso

11 *Ciberseguridad:* fortaleciendo la resiliencia y la confianza en un mundo digital global

(1) World Economic Forum (2024). The Global Risk Report 2024. Disponible en: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
(2) World Economic Forum (2024). The Global Cybersecurity Outlook 2024. Disponible en: https://www.weforum.org/publications/global-cybersecurity-outlook-2024/
(3) Esentire (2023). 2023 Official Cybercrime Report. Disponible en: https://www.esentire.com/resources/library/2023-official-cybercrime-report
(4) World Economic Forum (2024). Bridging the cyberskills gap. Disponible en: https://initiatives.weforum.org/bridging-the-cyber-skills-gap/home
(5) International Monetary Fund (2024). The Last Mile: Financial Vulnerabilities and Risks (Chapt. 3). Disponible en: https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024
(6) Cisco (2024). Cybersecurity Readiness Index Disponible en: https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf
(7) Telefónica (2024). Ciberseguridad: desarrollando resiliencia y confianza en un mundo digital. Disponible en: https://www.telefonica.com/es/sala-comunicacion/blog/ciberseguridad-desarrollando-resiliencia-confianza-mundo-digital/
(8) Telefónica. #Ciberseguridad. Disponible en: https://www.telefonica.com/es/tag/ciberseguridad/

12 *Sistemas de Alerta Temprana:* un escudo vital contra desastres naturales

(1) OECD (2024). Towards disaster-resilient infrastructure in Latin America: financing and governance. Disponible en: https://www.oecd-events.org/infrastructure-forum/session/03b28633-64b5-ee11-bea0-000d3a49ee24/breakout-6b-towards-disaster-resilient-infrastructure-in-latin-america-financing-and-governance-
(2) Agencia Europea del Medio Ambiente (2023). Economic losses from weather- and climate-related extremes in Europe. Disponible en: https://www.eea.europa.eu/en/analysis/indicators/economic-losses-from-climate-related
(3) GSMA (2023). Cell Broadcast for Early Warning Systems. Disponible en: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2023/11/Cell-Broadcast_R.pdf
(4) Telefónica (2023). Sistemas de Alerta Temprana: un escudo vital contra desastres naturales. Disponible en: https://www.telefonica.com/es/sala-comunicacion/blog/sistemas-de-alerta-temprana-un-escudo-vital-contra-desastres-naturales/

Telefónica

Sigue la conversación en...

Blog

LinkedIn

Newsletter

2025

Políticas Públicas Digitales,
Regulación y Competencia

Telefónica