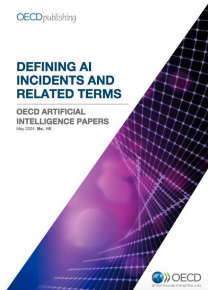


Boletín de Novedades del Centro de Documentación

5 de junio de 2024 - Nº 46

Economía del Dato e IA



[Definición de incidentes de IA y términos relacionados](#)

Organización de Cooperación y Desarrollo Económico (OCDE)

20 páginas

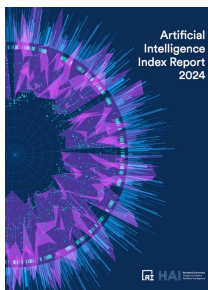
Este informe propone definiciones de los potenciales daños reales ("incidentes de IA") que puede provocar la inteligencia artificial (IA), así como sus potenciales peligros ("riesgos de IA") y términos relacionados. Estas definiciones pretenden fomentar la interoperabilidad internacional, al tiempo que ofrecen flexibilidad a las jurisdicciones para determinar el alcance de los incidentes y peligros de IA que desean abordar. El documento servirá de base para el desarrollo de un marco común de notificación de incidentes de IA y su aplicación a través del Monitor de Incidentes de IA (AIM) de la OCDE.

Este trabajo y sus versiones anteriores fueron debatidos y revisados por los miembros del antiguo Grupo de Expertos en Clasificación de Sistemas de Inteligencia Artificial de la OCDE durante una serie de talleres informales celebrados entre julio y octubre de 2022. También fue debatido por el Grupo de Expertos en Incidentes de IA de la OCDE.AI en sus reuniones de marzo, abril, junio, agosto y noviembre de 2023 y en su reunión de febrero de 2024. El Grupo de Trabajo de la OCDE sobre Inteligencia Artificial (AIGO) debatió este informe y versiones anteriores del mismo en sus reuniones de noviembre de 2022; abril, julio y noviembre de 2023; y febrero de 2024.

El marco propuesto ayudará a identificar los principales tipos de daños, como los daños físicos, medioambientales, económicos y de reputación, los daños al interés público y los daños a los derechos fundamentales. También abordará otras dimensiones del daño, como el nivel de gravedad, el alcance, la escala geográfica, la tangibilidad, la cuantificabilidad, la materialización, la reversibilidad, la recurrencia, el impacto y el calendario. Otro paso sería establecer taxonomías claras para clasificar los incidentes en función de cada dimensión del daño. La evaluación de la "gravedad" de un incidente, daño, perjuicio o perturbación de la IA (por ejemplo, para determinar si un suceso se clasifica como incidente o incidente grave) depende del contexto y también se deja para un debate posterior.

Maslej, Nestor ; Fattorini, Loredana ; Perrault, Raymond ; Parli, Vanessa ; Reuel, Anka ; Brynjolfsson, Erik ; Etchemendy, John ; Ligett, Katrina ; Lyons, Terah ; Manyika, James ; Niebles, Juan Carlos ; Shoham, Yoav ; Wald, Russell ; Clark, Jack

502 páginas



[Informe sobre el Índice de Inteligencia Artificial 2024](#)

El informe presenta una evaluación exhaustiva y multifacética del estado y las tendencias emergentes en el campo de la inteligencia artificial (IA) a nivel global a fecha de mayo de 2024. Aborda temas clave como los avances tecnológicos, el impacto económico, la educación en IA, las políticas de regulación y la percepción pública de la tecnología. Se destacan desarrollos notables como el aumento en la inversión en IA generativa, la proliferación de nuevos modelos y el crecimiento en la adopción de IA en sectores corporativos y gubernamentales. Además, se discuten las implicaciones de estos avances en la privacidad, seguridad, y equidad, subrayando la importancia de una IA responsable y accesible.

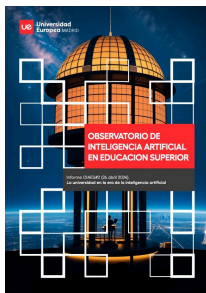
La importancia de este documento radica en su capacidad para informar y orientar a decisores, investigadores, y el público en general sobre las dinámicas actuales y futuras del desarrollo de la IA. Al proporcionar datos detallados y comparativos,

permite una mejor comprensión del rápido avance tecnológico y sus efectos en la sociedad. Esta información es crucial para la formulación de políticas efectivas que promuevan un desarrollo equitativo y ético de la IA, así como para anticipar desafíos futuros en la integración de estas tecnologías en todos los aspectos de la vida humana.

Las principales conclusiones apuntan a que la IA ha superado el rendimiento humano en varias pruebas de referencia, como la clasificación de imágenes, el razonamiento visual y la comprensión del inglés. Sin embargo, se queda atrás en tareas más complejas, como las matemáticas de competición, el razonamiento visual de sentido común y la planificación. Por otra parte, Estados Unidos se sitúa por delante de China, la UE y el Reino Unido como principal fuente de los mejores modelos de IA. Asimismo, a pesar del descenso de la inversión privada en IA en 2023, la financiación de la IA generativa se disparó, casi octuplicándose desde 2022 hasta alcanzar los 25.200 millones de dólares.

Universidad Europea de Madrid. Observatorio de inteligencia artificial en educación superior

27 páginas



La universidad en la era de la inteligencia artificial

Este informe pretende anticipar cómo podría ser el panorama universitario en el futuro, una vez que la inteligencia artificial (IA) esté suficientemente desarrollada e implementada. El objetivo de este ejercicio prospectivo es proporcionar una visión sobre un futuro plausible de la educación superior, para que cada institución pueda establecer su propia hoja de ruta para una transición racional y ordenada.

Entre las reflexiones y propuestas de futuras acciones el documento destaca la importancia de considerar los formatos en los cuales se incorporarán los conocimientos obtenidos por los profesores a través de la investigación a un mundo cada vez más digital y menos físico y con una línea divisoria progresivamente más difusa. Esto, sin duda, obligará a una reflexión profunda del modo en que los estudiantes aprenden y de cómo los profesores participan en ese proceso para facilitar la transmisión del conocimiento a los estudiantes. Discernir entre la verdad y la falsedad se convertirá en un verdadero desafío y será vital que la universidad mantenga su integridad como un lugar de confianza. En un entorno donde la IA está omnipresente, la necesidad de garantizar la confiabilidad es aún más evidente y el papel de la universidad para asegurar la explicabilidad y transparencia de esta tecnología será fundamental. Desde el punto de vista del estudiante, la formación que buscará será mucho más personalizada, pero no solo en la forma en la que se relacionará con sus profesores, sino también en la manera en la que diseñará su propio itinerario formativo apostando, cuando así lo desee, por caminos más flexibles o adaptados a sus necesidades.

Competencias digitales



[Tech & Society 2023. Sociedad digital y valores humanos](#)

Fundación Telefónica ; Aspen Institute España

88 páginas

Este volumen constituye el séptimo de la serie y corresponde a la edición de 2023 de las conferencias organizadas por la Fundación Telefónica en torno al papel de la tecnología en la sociedad actual. La visión que aportan los ponentes reconoce las ventajas de la tecnología pero sin ignorar los retos que puede suponer si no se gestiona de manera adecuada. En este sentido, se trata de aportar explicaciones y certezas ante un escenario desconocido que permitan adaptarse al nuevo entorno emergente.

Por su parte, Monique Morrow, presidenta y cofundadora de *The Humanized Internet*, expuso los retos asociados al mundo digital y cómo se debe defender la creación de un ciberespacio centrado en las personas y basado en valores y consideraciones éticas, en el marco de una innovación responsable y una regulación que refleje tales principios. 2023 fue el año de la inteligencia artificial (IA), y el experto Darío Gil, director de IBM Research, detalla los pormenores del funcionamiento de esta tecnología y ofrece una serie de consejos para las organizaciones que deseen implantarla o trabajar con ella. La última intervención estuvo a cargo de Anu Bradford, catedrática de Derecho y profesora de Derecho Internacional y Organizaciones en la Facultad de Derecho de la Universidad de Columbia, quien planteó los conflictos que existen en el mundo actual entre los tres modelos de ecosistema digital —los de Estados Unidos, la Unión Europea y China—, que ella denomina «imperios digitales».

Asociación Española para la Digitalización (DigitalES). Grupo de trabajo Formación y Empleo

46 páginas



[Anatomía de la brecha de talento tecnológico](#)

El documento conforma el primer estudio cualitativo que aborda uno de los problemas más acuciantes de la economía española: la falta de profesionales en un sector demandante de empleo que no cubre sus vacantes: el sector tecnológico. El objetivo reside en profundizar en el análisis del desajuste entre talento y empleo, y proponer soluciones que permitan a España generar y retener los profesionales que necesita para afrontar los desafíos del presente y del futuro. Para ello recurre al uso de herramientas de inteligencia artificial (IA) y un modelo predictivo que detecta necesidades y establece recomendaciones.

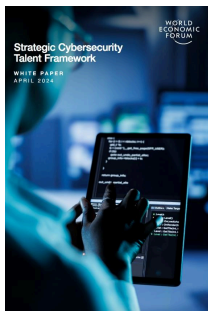
Para la investigación se ha llevado a cabo un análisis descriptivo que se nutre de las respuestas obtenidas mediante preguntas estratégicamente planteadas. Para ello, se ha seleccionado un periodo aproximado de entre 4 y 5 años desde 2018 y 2022 (según la disponibilidad de los datos), que cubre todo el territorio nacional desagregando los datos por las distintas CC. AA. A continuación, se presenta una descripción del perfil de los trabajadores dentro del sector tecnológico. Asimismo, se examina el proceso formativo de estos trabajadores, analizando las vías educativas y de capacitación que han contribuido a su desarrollo y preparación en el ámbito tecnológico. Como resultado de este análisis, DigitalES ha creado un cuadro de mandos interactivo que recopila y visualiza los datos más destacados obtenidos. Una herramienta que ofrece una representación gráfica y dinámica de la presencia de vacantes sin cubrir en el sector de la economía digital, así como de otras variables relevantes, como la distribución geográfica de los empleos y la disponibilidad de trabajadores capacitados.

Las conclusiones planteadas apuntan a que la complejidad y escasez de datos supone un obstáculo a la comprensión: si bien existe una multiplicidad de fuentes, la ausencia de un marco definido para la medición dificulta la tarea. Asimismo, la educación y la formación son pilares fundamentales para la generación de riqueza. Un modelo educativo capaz de desarrollar el talento necesario en el momento oportuno, anticipándose a las transformaciones tecnológicas, es clave para el progreso. Por otra parte, es necesario incrementar tanto los participantes como las horas de formación de la población activa. En 2023, solo se formó un 25% de población activa, lo que pone de manifiesto la falta de implementación de este tipo de formación entre las pymes y los autónomos. La superación de la complejidad actual exige un compromiso firme con la educación, la formación continua y la adaptación a las demandas del mercado laboral.

Ciberseguridad

World Economic Forum

40 páginas



Marco estratégico para el talento en ciberseguridad

El informe tiene como objetivo servir de referencia para los responsables públicos y privados preocupados por la escasez de mano de obra en el sector y comprometidos con el desarrollo y el fomento del talento en ciberseguridad en sus respectivas áreas de actividad. El documento señala que en la actualidad faltan casi cuatro millones de profesionales de la ciberseguridad en todo el mundo. La demanda de profesionales cualificados en este campo no deja de aumentar de forma constante año tras año y el déficit no muestra signos de remitir.

Consciente de que un único actor no puede hacer frente por sí solo a la escasez de mano de obra en ciberseguridad, el Foro Económico Mundial puso en marcha la iniciativa "Cerrar la brecha de las cibercapacidades". Reuniendo a más de 50 organizaciones públicas y privadas, la iniciativa desarrolló un Marco estratégico de Talento en Ciberseguridad (CTF, por sus siglas en inglés) con enfoques aplicables para ayudar a las organizaciones a crear fuentes de talento duraderas.

Entre las conclusiones el documento destaca la necesidad de que los responsables de la toma de decisiones en las organizaciones públicas y privadas colaboren en los esfuerzos por inspirar a la próxima generación de ciberdefensores y eliminar las barreras de entrada para las personas que aspiran a seguir una carrera en este campo. Al tiempo que se esfuerzan por crear un entorno de trabajo positivo, las organizaciones deben invertir en programas de educación y formación, promover la diversidad en la mano de obra de la ciberseguridad y ofrecer oportunidades de desarrollo profesional al personal existente. Por otra parte, a medida que el panorama digital sigue evolucionando, el CTF con respecto a las tecnologías emergentes, como la IA generativa, se vuelve esencial para garantizar su relevancia y adaptabilidad.

Derechos digitales

Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI). Grupo de Regulación

39 páginas

Metaverso,
desafíos legales

autelsi



Elaborado por el Grupo de Regulación de AUTELSI
Mayo 2021

Metaverso, desafíos legales

El objetivo de este informe reside en realizar un análisis de los aspectos legales que deben abordarse de manera adecuada en el metaverso para garantizar un entorno seguro, ético y confiable. En este trabajo también se dan respuestas a las preguntas planteadas en relación con varios casos de uso como los servicios al ciudadano, la selección de personal, los servicios educativos, los servicios financieros, y la comercialización de puntos de servicio, que permiten comprender mejor los aspectos legales implicados en esta tecnología.

Uno de los principales desafíos que presenta el metaverso está relacionado con la identidad digital de los avatares. En este entorno, las personas crean representaciones digitales de sí mismos con el fin de interactuar con otros usuarios. Por ello, es esencial proteger y gestionar su identidad digital. Otro reto regulatorio lo conforman la privacidad y seguridad de los avatares. En el metaverso, los usuarios se relacionan entre sí como si del mundo real se tratara, lo que puede conllevar significativas interacciones sociales, económicas, políticas o emocionales. Todo esto, unido a la utilización de tecnologías altamente invasivas para la privacidad, permite a los prestadores de servicios recabar datos con una granularidad y precisión sin precedentes. Asimismo, el aumento de los ciberataques y su complejidad plantea grandes desafíos para la seguridad de estos. Así pues, resulta fundamental promover la colaboración entre los diferentes actores del metaverso (desarrolladores, proveedores, entidades reguladoras, usuarios...) para establecer estándares y mejoras prácticas que ayuden a combatir estos riesgos. Más allá de las implicaciones sociales, tecnológicas y económicas, uno de los mayores desafíos para un adecuado funcionamiento es su correcta regulación, y para ello el metaverso debe fundamentarse en estándares abiertos (*open source*).

Transformación de la empresa y emprendimiento digital

ICEX España ; Asociación Española de la Economía Digital (Adigital)

184 páginas



Libro blanco del comercio electrónico transfronterizo

El documento profundiza en el impacto económico, barreras y soluciones para potenciar la internacionalización digital de las empresas, así como en las principales herramientas de apoyo, estrategias de marketing y promoción, plataformas tecnológicas y logística. El objetivo de este libro es doble: por un lado, convertirse en un referente para el tejido empresarial español que desee explorar las oportunidades de internacionalización a través del canal digital y, por otro lado, extraer recomendaciones para las administraciones públicas a partir de los datos y de las mejores prácticas existentes. Asimismo, también se pretende cuantificar y visibilizar la oportunidad y el potencial de crecimiento que el comercio electrónico transfronterizo puede aportar a la pyme española.

En la realización de este libro blanco, además de los dos socios impulsores del proyecto (ICEX y Adigital), han participado más de 14 autores diferentes, provenientes del mundo de la empresa y especialistas en distintas áreas del

comercio electrónico. También se realizó una encuesta a 30.000 empresas clientes de ICEX que fue cumplimentada por más de 1.750, y cerca de 50 han sido entrevistadas o han participado en distintos grupos de discusión. Además, el documento ha contado con la participación de la Secretaría de Estado de Comercio, los organismos de promoción de las Comunidades Autónomas a través del Consejo Interterritorial de Internacionalización, y otras entidades como Red.es o Cámara de Comercio de España.

Las instituciones y administraciones públicas deben jugar un papel clave para acelerar la digitalización de las pymes. Así lo expresan las conclusiones del documento. Los avances en transformación digital impulsan la importancia del canal en línea, y esto supone una oportunidad muy relevante para las empresas españolas. Además, la digitalización lleva consigo la posibilidad de la internacionalización, un aspecto clave para ampliar las oportunidades y los beneficios para las pymes así como acelerar su crecimiento. En este sentido, herramientas como la web Access-2Markets, de la Comisión Europea, ejemplifica una iniciativa muy útil por parte de las instituciones públicas, permitiendo obtener la información que se necesita al comerciar con terceros países sobre aranceles, impuestos, procedimientos, formalidades y requisitos, normas de origen, medidas de exportación, estadísticas, obstáculos al comercio y más. Otra iniciativa que podría facilitar la internacionalización de las pymes sería la activación de un observatorio para las pymes sobre las políticas de internacionalización y las ayudas existentes.

Conectividad digital

Agencia Española de Protección de Datos ; Autoridad Catalana de Protección de Datos ; Autoridad Vasca de Protección de Datos ; Consejo de Transparencia y Protección de Datos de Andalucía 52 páginas



TECNOLOGÍAS DE SEGUIMIENTO WI-FI

Esta guía analiza las implicaciones de la tecnología de seguimiento Wi-Fi o *Wi-Fi tracking*, identifica los principales riesgos y ofrece una serie de recomendaciones para un uso responsable y compatible con la normativa de protección de datos. El seguimiento Wi-Fi es una tecnología que permite identificar y rastrear dispositivos móviles a través de las señales Wi-Fi que estos emiten, detectando la presencia del dispositivo en una zona específica e identificando patrones de movimiento.

Las autoridades de protección de datos exponen que el uso de esta tecnología puede suponer un tratamiento de datos personales y, por tanto, deben someterse al conjunto de principios, derechos y obligaciones establecidos en el Reglamento General de Protección de Datos (RGPD). Además, su uso plantea serios riesgos para la privacidad, ya que podría permitir el seguimiento de los movimientos de las personas sin que estas sean conscientes de ello y sin el respaldo jurídico procedente.

Por ello, las autoridades consideran que, dados los factores y elementos de riesgo inherentes, en general, se cumplen las condiciones para que antes de llevar a cabo el tratamiento sea obligatorio realizar una Evaluación de Impacto en la Protección de Datos (EIPD). De hecho, teniendo en cuenta los factores de riesgo, recomiendan realizarla incluso cuando el responsable del tratamiento pueda no tener clara su obligatoriedad. Además, para utilizar estas tecnologías es necesario intensificar el

cumplimiento del principio de transparencia a través de una información clara y accesible, como paneles visibles con información, señalización pública, alertas de voz o campañas de información, entre otros.