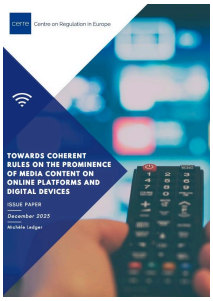
# Boletín de Novedades del Centro de Documentación

*15 de diciembre de 2023 - Nº 25*

## Transformación digital sectorial y sostenible



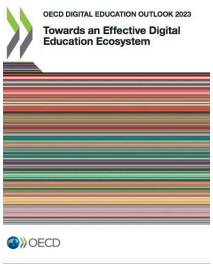

[Hacia normas coherentes sobre la prominencia de los contenidos audiovisuales en las plataformas en línea y los servicios digitales]

Ledger, Michèle — 41 páginas

Este informe presenta un mapa de las normas e iniciativas europeas y de la UE relacionadas directa o indirectamente con la prominencia de los contenidos de interés general. Para ello analiza los casos de Alemania, Francia, Italia y el Reino Unido ofreciendo una reflexión crítica y recomendaciones sobre cómo llegar a un marco más coherente.

Tomando como referencia la Nota Orientativa del Consejo de Europa (CdE) sobre la Priorización de los Contenidos de Interés Público en Línea, el documento examina las distintas normas nacionales derivadas del artículo 7 bis de la Directiva de Servicios de Comunicación Audiovisual, así como otras disposiciones de ámbito comunitario, entre ellas las aplicables a los intermediarios. En general, el estudio revela un enfoque poco sistemático, con normas dispersas en varios instrumentos legislativos que crean una situación compleja para todas las partes interesadas.

El documento recomienda una aplicación más sistemática de las directrices del CdE a escala nacional y de la UE. El artículo 7 bis debería detallarse más para incluir normas de procedimiento o aclarar el papel de los reguladores independientes. También destaca que debe abordarse la relación entre las normas de prominencia impuestas a nivel nacional a las plataformas establecidas en otros Estados miembros, ya que constituye un ámbito de inseguridad jurídica que puede acarrear graves consecuencias negativas para el funcionamiento del mercado interior.




[OCDE Panorama de la Educación Digital 2023]

Organización para la Cooperación y el Desarrollo Económicos — 410 páginas

El documento ofrece un análisis comparativo y temático de cómo los países configuran o podrían configurar su ecosistema educativo digital. Establece cuáles son los diferentes componentes en los países analizados. Así mismo se determina cómo y en qué medida aprovechan los países las competencias digitales de los profesores y las últimas oportunidades que ofrece la inteligencia artificial (IA). El objetivo es determinar cómo pueden los países aprovechar al máximo su ecosistema digital para que sea fiable, útil, eficaz y equitativo, y hacia dónde podrían dirigirse para beneficiarse de la transformación digital. Consta de dos partes principales: una sobre el ecosistema educativo digital de los países, incluido su componente humano, y otra sobre su gobernanza.

El informe abarca la mayoría de los países de la OCDE y algunos países asociados. Se basa en tres tipos de fuentes: documentos, sitios web y documentos oficiales de los países incluidos en el análisis; documentos políticos e informes de organizaciones internacionales; y artículos de investigación publicados en revistas nacionales e internacionales.

Entre las prioridades que se establecen de cara a los próximos años para la construcción del ecosistema educativo digital, en el caso de España se destacan tres acciones principales: aumentar el suministro de dispositivos digitales y mejorar la conectividad; implantar plataformas basadas en IA para permitir el aprendizaje personalizado; y mejorar las competencias del profesorado y reforzar sus habilidades digitales para impartir educación digital.

Organización para la Cooperación y el Desarrollo Económicos — 332 páginas


Ecosistemas y gobernanza de la educación digital en los países

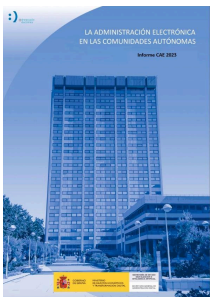
Este documento, vinculado al informe "Panorama de la Educación Digital 2023", ofrece una visión general del ecosistema y la gobernanza de la educación digital en 29 países (o jurisdicciones). Cada capítulo abarca la delegación de responsabilidades dentro de los países; cómo afecta a la educación digital; qué herramientas digitales para la gestión y la enseñanza y el aprendizaje se ponen a disposición pública de las escuelas, los profesores y los estudiantes; cómo se proporcionan o adquieren; o cómo garantizan los países la seguridad, la privacidad, la equidad y la eficacia de este ecosistema digital, manteniendo al mismo tiempo los incentivos para las empresas privadas de tecnología educativa (EdTech).

La información y el análisis se basan en una encuesta sobre infraestructura y gobernanza de la educación digital, entrevistas con funcionarios de los gobiernos nacionales y regionales e investigación documental.

En el caso de España, debido a la naturaleza altamente descentralizada de la gobernanza, garantizar la equidad en el acceso y el uso de la infraestructura digital, las herramientas y los recursos en todas las escuelas es un desafío. Sin embargo, la mayoría de las comunidades autónomas proporcionan una infraestructura digital mínima que incluye herramientas para la gestión de sistemas e instituciones, y el gobierno central proporciona importantes recursos educativos abiertos para apoyar la enseñanza y el aprendizaje. Las iniciativas nacionales también pretenden conectar todas las escuelas a Internet de alta velocidad y proporcionar acceso a dispositivos digitales a los grupos de estudiantes vulnerables. A nivel central, el Ministerio proporciona importantes recursos para apoyar a los profesores en el uso de herramientas y recursos digitales en la educación y en el desarrollo de las competencias digitales de los profesores, incluidos recursos de información, directrices prácticas y cursos abiertos en línea.

## Transformación digital del Sector Público

Ministerio de Asuntos Económicos y Transformación Digital. Secretaria General de Administración Digital (SGAD) — 61 páginas




La administración digital en las comunidades autónomas

El informe CAE 2023 analiza el grado de la transformación digital en el ámbito de la Administración Autonómica. El objetivo es poner en valor los esfuerzos en transformar digitalmente los procesos internos y externos de este tipo de administración y servir de referencia para la mejora continua de los servicios de cara a los ciudadanos.

La Administración autonómica está formada por 17 comunidades autónomas (CCAA) más las dos ciudades autónomas de Ceuta y Melilla. Para elaborar el informe se ha invitado a las 19 entidades y han respondido al cuestionario el 100% de ellas. Respecto a los datos de personal se ha utilizado el Boletín estadístico del personal al servicio de las Administraciones Públicas, Registro Central de Personal (Enero 2022).

En cuanto a las políticas de transformación digital se apunta a que el 95% de las CCAA tienen un plan de transformación digital o equivalente, y el 79% ha establecido indicadores para medir el avance del plan. En el apartado de servicios centrados en el ciudadano y la empresa se destaca que el acceso a los Servicios

Sociales por canal digital es muy bajo, a pesar de que diez comunidades están por encima del 80% en disponibilidad online de los servicios seleccionados. El promedio de portales que cumplen con el nivel AA de accesibilidad (subtítulos para audios emitidos en vivo, posibilidad de visualizar el contenido en orientación horizontal y vertical, cambiar el tamaño del texto hasta en un 200% sin perder el contenido, los encabezados y las etiquetas o proporcionar sugerencias de corrección ante errores de entrada) es de un 27%. Así mismo, el 70% de los trámites analizados funcionan en dispositivos móviles. El promedio de los trámites digitales que contemplan la dimensión transfronteriza en la Comunidades Autónomas es de 67%. Sobre el impulso a la transformación digital interna, se apunta que en los servicios de Sanidad, Empleo y empresas hay un mayor porcentaje de CCAA que tiene tramitación digital completa. En torno a las iniciativas impulsadas en relación a gobierno abierto destaca que la mayoría de las comunidades tiene planes de acción orientados a reducir la brecha digital.

## Transformación digital de la empresa y emprendimiento digital

NTT DATA ; Observatorio Industria 4.0 ; Club Excelencia en Gestión ; Centro Español de Logística (CEL) ; Fundación Empresa y Sociedad

43 páginas


Smart Industry 4.0. Los retos en el camino hacia la Transformación Digital

El estudio, en su sexta edición, tiene como objetivo analizar la situación actual y la evolución en los próximos años de la transformación digital, así como su impacto en la toma de decisiones de la industria. Pretende facilitar a las empresas criterios objetivos para realizar una autoevaluación de su preparación para llevar a cabo esta adopción. Así mismo, se identifican la situación y oportunidades de tres tecnologías (Internet of Things –IoT–, Inteligencia Artificial, Gemelo Digital) y se analiza su impacto en la cadena de valor industrial y en el parque de sistemas de gestión empresarial.

Para la metodología se ha empleado una encuesta online en forma de cuestionario que sirve como base para la elaboración del análisis y posterior informe. Respecto al análisis de la información obtenida se han contemplado aspectos como la demografía de los encuestados, o los paradigmas de cada bloque de Industria 4.0, y se han analizado individualmente. Una vez analizados los datos de la encuesta, se comparan con los de los años anteriores con el fin de encontrar tendencias y patrones que muestren la evolución de las empresas hacia la Industria 4.0.

El informe concluye que la transformación digital de la industria se consolida: tres de cada cuatro empresas considera que ya tiene un nivel adecuado o elevado de digitalización. Esto supone un alto porcentaje y una tendencia positiva respecto a años anteriores. Sin embargo, desvela que más de un tercio de las compañías siguen teniendo dudas sobre los beneficios derivados de las inversiones en tecnología (34%), lo que representa la mayor barrera para su implementación. En cuanto a las tecnologías más significativas, big data & analytics, ciberseguridad, IoT, cloud e inteligencia artificial/machine learning se encuentran en cabeza. El ecosistema también augura grandes expectativas con la inteligencia artificial. Casi el 65% de las empresas que aún no la han implementado piensa que será beneficiosa para sus procesos de negocio.

## Derechos digitales


Moderación de contenidos en línea

Agencia de los Derechos Fundamentales de la Unión Europea — 98 páginas

El informe presenta los retos a la hora de identificar y detectar el odio en línea. Explora las dificultades de su investigación y la compleja tarea a la que se enfrentan los responsables políticos y las plataformas tecnológicas para tratar de atajarlo. Analiza las implicaciones de los derechos fundamentales para apoyar la creación de un entorno digital respetuoso con los derechos.

Los datos se recopilaron en X, Reddit, YouTube y Telegram. Estas plataformas se seleccionaron en función de su relevancia en los cuatro países que conforman la muestra (Alemania, Bulgaria, Italia y Suecia) y de consideraciones de viabilidad relativas al acceso a los datos. En total, se seleccionaron 344.132 mensajes y comentarios en las redes sociales de los cuales se analizaron 400 ejemplos aleatorios de cada país.

Los resultados muestran que es fácil encontrar una cantidad significativa de misoginia y odio contra afrodescendientes, judíos y gitanos al buscar en las plataformas analizadas. Más de la mitad de los mensajes analizados (53%) pertenecen al menos a una de las categorías identificadas. Éstas incluyen elementos de incitación a la violencia, la discriminación o el odio; denigración; lenguaje ofensivo; estereotipos negativos; o cualquier otro contenido que parta de este sentimiento. De todos los mensajes codificados como odiosos, casi el 85% contenían lenguaje ofensivo. Los codificadores consideraron que el 55% de los mensajes de incitación al odio expresaban odio hacia las personas por sus características protegidas. El hecho de que la investigación fuera capaz de marcar publicaciones que potencialmente podrían clasificarse como odio en línea indica que los sistemas de moderación de contenidos no están captando todas las formas de odio.


Derecho a la desconexión: Aplicación e impacto a nivel de empresa

Eurofound ; Weber, Tina ; Adăscălițe, Dragoș — 66 páginas

Este informe explora la legislación de los Estados miembros de la UE en torno al derecho a desconectar y evalúa el impacto de las políticas de las empresas en este ámbito sobre las horas de conexión de los empleados, el tiempo de trabajo, el equilibrio entre vida laboral y personal, la salud y el bienestar, y la satisfacción general en el lugar de trabajo.

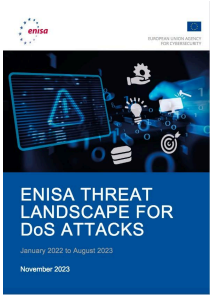
La metodología se basa en el análisis de los resultados de una encuesta realizada a personal de dirección de Recursos Humanos y empleados de cuatro países de la UE (Bélgica, España, Francia e Italia).

Alrededor del 45% de quienes respondieron y trabajan en sectores con un elevado porcentaje de teletrabajo y en países en los que la legislación sobre el derecho a la desconexión se aplica a través del diálogo social afirmaron que en su empresa existe una política sobre el derecho a la desconexión. Por otra parte, más del 80% declararon haber recibido comunicaciones relacionadas con el trabajo fuera de su horario laboral contractual durante una semana laboral típica. Casi la mitad trabaja regularmente más horas de las que tienen contratadas, la mayoría de las veces para completar tareas que no pudieron terminar durante las horas de trabajo contractuales (37%). Así mismo, más del 70% de quienes trabajan en empresas con una política de derecho a la desconexión considera que su impacto ha sido muy o

algo positivo; el 26% considera que no ha tenido ningún impacto.

## Ciberseguridad

Agencia de la Unión Europea para la Ciberseguridad — 33 páginas



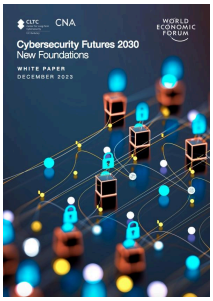

[Panorama de amenazas para ataques DoS de ENISA]

Los ataques de denegación de servicio (DoS) han sido una preocupación constante para la seguridad de las organizaciones. Sin embargo, en los últimos años, los ataques DoS se han vuelto más fáciles, baratos y agresivos que nunca. La aparición de nuevos conflictos armados en todo el mundo ha servido de combustible para nuevas oleadas de ofensivas. Este informe pretende aportar nuevas perspectivas al panorama de las amenazas DoS. A través de un cuidadoso análisis de las motivaciones y el impacto de estos ataques, el documento ayuda a las organizaciones a entender esta amenaza y cómo protegerse mejor si alguna vez son un objetivo.

Los datos compartidos en este informe son el resultado de un minucioso mapeo y análisis de los incidentes de denegación de servicio descubiertos entre enero de 2022 y agosto de 2023.

Las conclusiones de este estudio muestran que, aunque todos los sectores se ven afectados por los ataques DoS, los sectores más atacados son los relacionados con los servicios gubernamentales (46%). Se estima que el 66% de los ataques estuvieron motivados por razones políticas o agendas activistas. En general, se determinó que el 50% de los incidentes estaban relacionados con la guerra de agresión rusa contra Ucrania. El estudio muestra que el 56,8 % de los ataques causaron una interrupción total en el objetivo. También destaca la importancia de la cibernética como multiplicador de fuerzas o vector de apoyo en la guerra, los cambios que esto supone en el panorama y que es vital que las organizaciones preparen estrategias de prevención y reparación.

World Economic Forum ; UC Berkeley Center for Long-Term Cybersecurity (CLTC) ; Center for Naval Analyses - Institute for Public Research (CNA) — 16 páginas




[Ciberseguridad para el futuro 2030]

Este informe presenta las conclusiones de Cybersecurity Futures 2030, una iniciativa de investigación global centrada en explorar cómo podría evolucionar la seguridad digital en los próximos cinco a siete años. El objetivo de este proyecto es ayudar a dar forma a una agenda política y de investigación centrada en el futuro que sea ampliamente aplicable en todos los países y sectores.

Las conclusiones se basan en los debates mantenidos en una serie de talleres presenciales celebrados a lo largo de 2023 en Dubai (Emiratos Árabes Unidos), Washington DC (EE.UU.), Kigali (Ruanda), Nueva Delhi (India) y Singapur, así como en un taller virtual con participantes de varios países europeos y del Reino Unido.

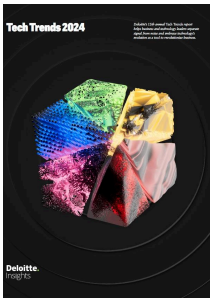
La aceleración de la innovación tecnológica y de los negocios que tienen como base la ciberseguridad sustentará el nuevo panorama de la seguridad digital para 2030. Las sociedades deben reorientar fundamentalmente sus respuestas a los retos perennes de la seguridad digital, como la privacidad de los datos, el desarrollo del talento y la sostenibilidad. La ciberseguridad consistirá cada vez menos en proteger la confidencialidad y disponibilidad de la información y más en proteger su integridad y procedencia. Los gobiernos estables que siguen

estrategias tecnológicas y de ciberseguridad a largo plazo pueden convertirse en "marcas" de confianza, obteniendo ventajas a la hora de atraer talento, aprovechar oportunidades de liderazgo en los procesos multilaterales de establecimiento de normas y contrarrestar las campañas de desinformación.

## Competencias digitales

Deloitte Insights

64 páginas




Tech Trends 2024

La decimoquinta edición anual del informe de tendencias tecnológicas emergentes presentado por Deloitte destaca historias de organizaciones pioneras en el uso de nuevas tecnologías y enfoques que se convertirán en la norma en un plazo de 18 a 24 meses. También proyecta hacia dónde podrían dirigirse las tendencias durante la próxima década.

Seis tendencias tecnológicas emergentes demuestran que, en la era de las máquinas generativas, es más importante que nunca que las organizaciones mantengan una estrategia empresarial integrada, una base tecnológica sólida y una plantilla creativa. Por una parte, la informática espacial y el metaverso industrial. En segundo lugar, la inteligencia artificial generativa como catalizador del crecimiento. En tercer lugar, el hardware de vanguardia para acelerar los procesos. Así mismo, potenciar la experiencia del perfil ingeniero. También se apunta a evitar la suplantación de la identidad y engaños mediante una combinación de políticas y tecnologías. Por último, se apuesta por potenciar la prevención para alcanzar el bienestar técnico.