

Notas de Electrónica					
Título:	Va Jalisco por el 85% de industria de chips				
Encabezado:					
Fecha:	09/06/25	Fuente:	MURAL	Por:	Luis Pablo Segundo
Link:	<a href="https://www.mural.com.mx/va-jalisco-por-el-85-de-industria-de-chips/ar3018823">https://www.mural.com.mx/va-jalisco-por-el-85-de-industria-de-chips/ar3018823</a>				

Antes de terminar el actual Gobierno estatal (2024-2030), Jalisco espera contar con 85 por ciento de las empresas instaladas en tecnología dedicada en la industria de los semiconductores -o chips, usados en la industria automotriz y en dispositivos electrónicos-, 15 puntos porcentuales por encima de lo que se tiene ahora, aseveró el Gobernador Pablo Lemus Navarro.

"Hoy tenemos 70 por ciento del mercado nacional de la producción de semiconductores; nosotros estamos planteando que para fin de este sexenio tenemos que superar 85 por ciento.

"Es decir, vamos a seguir creciendo en el ámbito de los semiconductores", comentó Lemus en entrevista concedida la semana pasada en el marco de un foro de la Asociación de Desarrolladores Inmobiliarios (ADI), en la Ciudad de México.

El Gobernador resaltó que se trabaja en diversas áreas, como infraestructura carretera, hídrica y energética, con el fin de que la Iniciativa Privada (IP) apueste por la entidad en el desarrollo de toda la cadena de semiconductores.

"La decisión de Estados Unidos de no imponer nuevos aranceles a semiconductores nos pone en una situación competitiva enorme. Le comentaba a la Presidenta (Claudia Sheinbaum Pardo) que no sólo tenemos que hablar de manufactura", dijo Lemus.

En un contexto macroeconómico donde Estados Unidos busca capitalizar inversiones de manufactura y diseño a nivel local de semiconductores, el Gobernador aseveró que trabaja de la mano con el Gobierno federal, en el marco del Plan México, para que este sector económico cuente con una expansión en la entidad.

"Hay dos inversiones (en la entidad) que se han hecho públicas: Foxconn, en su joint venture con Nvidia, y ASE (Group), que también es una empresa de semiconductores", añadió el funcionario.

De manera adicional y a fin de consolidar más inversiones, se trabaja en el despliegue de infraestructura hídrica y eléctrica en otras regiones del Estado, con el fin de que estas empresas cuenten con los recursos necesarios para instalarse en cualquier parte de la entidad.

"Los municipios de la zona Altos Norte: Lagos de Moreno, San Juan de los Lagos, Encarnación de Díaz, etcétera, hace toda la lógica que las nuevas plantas de semiconductores se instalen en la zona Altos Norte", explicó.

Esto se debe a la cercanía que hay con Aguascalientes, que cuenta con un gran número de empresas de manufactura automotriz.

Recordó que además se trabaja con la Comisión Federal de Electricidad (CFE) en la construcción de una planta de ciclo combinado, proyecto que se estima será el más grande de todo el sexenio que podrá iniciar operaciones en 2028.

Lo que ya está...

Varias empresas de semiconductores tienen operaciones en Jalisco, enfocadas en el diseño o la validación. Algunas son:

ASE Group/Taiwán  
 Bosch/Alemania  
 Foxconn/Taiwán  
 Intel/EU  
 Micron/EU  
 NXP Semiconductors/Países Bajos  
 SK Hynix/Corea del Sur

...Y lo que viene

- El Gobierno de Jalisco, Iniciativa Privada (IP), universidades y centros de investigación planean crear un parque industrial enfocado en el diseño de semiconductores.

- En dicho parque también podría ubicarse Kutsari, proyecto anunciado en febrero por el Gobierno federal para que empresas y centros de investigación impulsen el diseño de semiconductores.

Notas de Electrónica					
Título:	Qualcomm comprará Alphawave por 2.105 millones				
Encabezado:					
Fecha:	09/06/25	Fuente:	LA VANGUARDIA	Por:	
Link:	<a href="https://www.lavanguardia.com/ciencia/20250609/10768047/qualcomm-comprara-alphawave-2-105-millones-ep-agenciaslv20250609.html">https://www.lavanguardia.com/ciencia/20250609/10768047/qualcomm-comprara-alphawave-2-105-millones-ep-agenciaslv20250609.html</a>				

El fabricante estadounidense de semiconductores Qualcomm ha llegado a un acuerdo para adquirir a la empresa tecnológica británica Alphawave por 2.400 millones de dólares (2.105 millones de euros) en una operación que podría completarse en el primer trimestre de 2026.

Los accionistas de Alphawave tendrá derecho a recibir 183 peniques en efectivo por cada acción de la compañía en su poder, aunque podrán optar también por percibir 0,01662 acciones de Qualcomm o 0,00964 de un nuevo valor intercambiable de Qualcomm Serie A y 0,00698 de un nuevo valor intercambiable de Qualcomm Serie B.

La cúpula directiva de Alphawave considera que las condiciones de la propuesta de Qualcomm “son justas y razonables” y, en consecuencia, tiene la intención de recomendar por unanimidad que los accionistas de Alphawave voten a favor en la junta general.

El cierre de la transacción está sujeto, entre otras cosas, a la aprobación por parte de los accionistas de Alphawave, así como al cumplimiento o exención de las aprobaciones antimonopolio pertinentes y las aprobaciones de inversión extranjera directa, incluyendo las del Reino Unido.

“La adquisición de Alphawave por parte de Qualcomm representa un hito significativo para nosotros y una oportunidad para que nuestra empresa aúne fuerzas con un líder respetado del sector y genere valor para nuestros clientes”, declaró Tony Pialis, presidente y consejero delegado de Alphawave.

De su lado, Cristiano Amon, presidente y CEO de Qualcomm, afirmó que los equipos combinados comparten el objetivo de desarrollar soluciones tecnológicas avanzadas y permitir un rendimiento de computación conectada de vanguardia en una amplia gama de áreas de alto crecimiento, incluida la infraestructura de centros de datos.

Notas de Electrónica					
Título:	El presidente de Estados Unidos prohíbe la venta de software de diseño de chips a China				
Encabezado:					
Fecha:	08/06/25 (por la tarde)	Fuente:	MSN	Por:	
Link:	<a href="https://www.msn.com/es-es/noticias/tecnologia/el-presidente-de-estados-unidos-proh%C3%ADbe-la-venta-de-software-de-dise%C3%B1o-de-chips-a-china/ar-AA1GhiqH">https://www.msn.com/es-es/noticias/tecnologia/el-presidente-de-estados-unidos-proh%C3%ADbe-la-venta-de-software-de-dise%C3%B1o-de-chips-a-china/ar-AA1GhiqH</a>				

Puede que Trump haya rebajado los aranceles a las importaciones chinas, pero eso no significa que las dos grandes potencias mundiales hayan enterrado el hacha de guerra. De hecho, la guerra comercial entre ambas naciones continúa, y el presidente de los Estados Unidos de América quiere evitar a toda costa que el país asiático acceda a software estadounidense para diseñar semiconductores.

Estados Unidos quiere evitar a toda costa que China se convierta en un referente tecnológico, sobre todo en el sector de la inteligencia artificial. Es por eso que NVIDIA, principal proveedora de semiconductores para inteligencia artificial, tiene prohibida ofrecer sus chips a Xi Jinping y compañía, llevándose una denuncia por prácticas antimonopolio.

La última medida de Trump para que China no pueda acceder a su tecnología (aunque existen maneras de saltársela) es prohibiendo a las empresas estadounidenses la venta de software de diseño de chips, lo que, en teoría, debería provocar ciertas dificultades al país asiático. Habrá que ver si sirve para algo o no.

Una medida para obstaculizar el avance de China en IA

Donald Trump y su equipo han ordenado a las empresas estadounidenses especializadas en software para diseño de semiconductores que no vendan sus servicios a China, con el objetivo de dificultar el desarrollo de soluciones que puedan poner en peligro el liderazgo de Estados Unidos.

Varias personas familiarizadas con el tema aseguran que el Departamento de Comercio de los Estados Unidos de América había ordenado a los llamados grupos de automatización de diseño electrónico (en los que se incluyen a Cadence, Synopsys y Siemens EDA) que dejen de suministrar su tecnología a China.

La Oficina de Industria y Seguridad, la rama del Departamento de Comercio de Estados Unidos que supervisa los controles de exportación, emitió la directiva a las empresas mediante cartas, según las fuentes. No estaba claro si todas las empresas estadounidenses de la EDA habían recibido una carta.

Esta medida representa un nuevo esfuerzo de la administración para obstaculizar la capacidad de China de desarrollar chips de IA de alto nivel. Como mencionamos anteriormente, a NVIDIA ya se le prohibió hace unos meses la exportación de chips a China. Sassine Ghazi, director ejecutivo de Synopsys, durante la presentación de resultados del segundo trimestre, comentó que:

Estamos al tanto de los informes y las especulaciones, pero Synopsys no ha recibido ninguna notificación del BIS. Por lo tanto, la previsión que reiteramos para todo el año refleja nuestra comprensión actual de las restricciones a la exportación del BIS, así como nuestras expectativas de una disminución interanual de los ingresos en China

Un funcionario del Departamento de Comercio afirmó que estaba revisando las exportaciones de importancia estratégica para China. En algunos, casos el departamento ha suspendido las licencias de exportación existentes o ha impuesto requisitos adicionales mientras la revisión está pendiente.

El software EDA, si bien representa una parte relativamente pequeña de la industria general de semiconductores, permite a los diseñadores y fabricantes de chips desarrollar u probar la próxima generación de chips, convirtiéndolo en una parte importante de la cadena de suministro.

Notas de Telecomunicaciones					
Título:	¿Una Reforma que Podría Asfixiar a las MiPyMEs Digitales de México?				
Encabezado:					
Fecha:	08/06/25 (por la tarde)	Fuente:	CAMBIO 22	Por:	Renato Consuegra
Link:	<a href="https://diariocambio22.mx/una-reforma-que-podria-asfixiar-a-las-mipymes-digitales-de-mexico/">https://diariocambio22.mx/una-reforma-que-podria-asfixiar-a-las-mipymes-digitales-de-mexico/</a>				

En medio del avance del nearshoring, la transformación digital y la necesidad urgente de modernizar al Estado, el gobierno mexicano ha presentado una iniciativa para reformar la Ley Federal de Telecomunicaciones y Radiodifusión, donde en el discurso oficial, se habla de “soberanía digital”, “simplificación” y “eficiencia”; sin embargo, bajo esa superficie, existe un riesgo real: que miles de micro, pequeñas y medianas empresas (MiPyMEs) sufran un golpe letal en su operación diaria, en su visibilidad digital y en su libertad para competir.

La iniciativa —que al momento de escribir estas líneas se encuentra en proceso de análisis en el Congreso— propone sustituir al Instituto Federal de Telecomunicaciones (IFT), un órgano autónomo, por una Agencia de Transformación Digital y Telecomunicaciones (ATDT), dependiente del Ejecutivo. A esta nueva entidad se le otorgarían facultades para bloquear plataformas digitales,

sancionar contenidos y regular el acceso a herramientas tecnológicas, con base en criterios amplios y poco definidos, como “seguridad nacional” o “estabilidad social”.

En paralelo, la propuesta incluye la creación de una identidad digital única (“Llave MX”) y un número nacional de atención ciudadana. A simple vista, parecen avances. Pero el diablo está en los detalles. La gran mayoría de las MiPyMEs en México ya opera en desventaja: con acceso limitado a crédito, asesoría legal, herramientas digitales y publicidad.

Inmersas en este oscuro panorama, muchas han encontrado en plataformas como WhatsApp, Facebook, TikTok, Stripe, Amazon o Mercado Libre, un canal vital para sobrevivir y, para muchas, es el único canal.

¿Qué pasará si una de esas plataformas es bloqueada “por razones de Estado”? ¿Quién responderá por las ventas perdidas? ¿A dónde acudirán los emprendedores que no pueden pagar un abogado ni comprender el laberinto legal que viene?

La iniciativa eleva el riesgo regulatorio y lo hace de manera opaca porque bajo el nuevo esquema, una microempresa podría quedar expuesta a medidas discrecionales que afecten su operación digital, incluyendo censura, restricciones publicitarias o sanciones fiscales sin mecanismos claros de defensa. Dentro de la propuesta no hay reglas precisas, no hay recursos inmediatos y, lo más preocupante: no hay garantías de equidad frente a las grandes empresas.

Mientras las corporaciones multinacionales tienen la capacidad de negociar excepciones o acuerdos técnicos, las MiPyMEs quedarán solas ante un aparato regulador centralizado y poderoso.

El Tratado entre México, Estados Unidos y Canadá (T-MEC) protege principios como la neutralidad de la red, la libre competencia y el acceso no discriminatorio a servicios digitales, mientras que, al contrario, esta iniciativa, tal como está planteada, puede entrar en conflicto con esos principios. Y si México recibe sanciones o pierde competitividad internacional, las primeras en resentirlo serán —una vez más— las MiPyMEs, que dependen de la estabilidad económica para operar en un entorno ya complejo.

Este debate no puede reducirse a trincheras ideológicas. Se trata de entender que sin un ecosistema digital predecible, abierto y justo, el emprendimiento no es viable en el siglo XXI. Las MiPyMEs, como lo han demostrado históricamente, no piden privilegios: solo demandan un entorno donde puedan competir sin miedo a que su canal de ventas desaparezca por decreto.

Ante este panorama, es momento de actuar y preguntarnos qué hacer.

Primero, exigir claridad normativa: las reglas para bloquear o sancionar plataformas deben estar definidas con precisión y sujetas a supervisión judicial.

Segundo, defender la autonomía de los órganos reguladores: concentrar todo el poder en una sola agencia del Ejecutivo es una receta para la discrecionalidad.

Tercero, incorporar a las MiPyMEs en la discusión legislativa: hoy, su voz está ausente, como casi siempre frente a los temas que más las afectan.

La digitalización de la economía no puede construirse bajo amenazas latentes de censura, bloqueos o sanciones sin explicación. Si queremos un país donde emprender sea posible, no bastan los discursos sobre “soberanía digital”, necesitamos leyes que garanticen estabilidad, equidad y transparencia.

Y, en eso, esta reforma —hasta ahora— aún queda muy lejos.

De emprendimientos y más...

Notas de Telecomunicaciones					
Título:	Tráfico impulsado por OTTs eleva a 49 mil mdd inversión en redes de AL				
Encabezado:					
Fecha:	09/06/25	Fuente:	CONSUMOTIC	Por:	Guadalupe Michaca
Link:	<a href="https://consumotic.mx/telecom/trafico-impulsado-por-otts-eleva-a-49-mil-mdd-inversion-en-redes-de-al/#google_vignette">https://consumotic.mx/telecom/trafico-impulsado-por-otts-eleva-a-49-mil-mdd-inversion-en-redes-de-al/#google_vignette</a>				

En América Latina, donde 74 por ciento del tráfico móvil es generado por sólo cuatro proveedores de servicios Over The Top (OTT), será necesario que hacia el 2030 se inviertan 49 mil millones de dólares adicionales a los previstos, y de los cuales 32 mil millones de dólares tendrían que ser destinados a ampliar la capacidad de las redes de telecomunicaciones.

“En un contexto de capacidad de inversión limitada por parte de los operadores, el aumento del tráfico de internet presenta un reto adicional. Cada dólar que los operadores invierten en ampliar la capacidad de sus redes para cursar el nuevo tráfico es un dólar que deja de estar disponible para invertir en el cierre de la brecha digital”, señala un reciente informe del Centro de Estudios de Telecomunicaciones de América Latina (cet.la).

El documento “Contribución del conjunto del ecosistema digital al desarrollo sostenible de infraestructura de telecomunicaciones”, elaborado por Nera, detalla que de la inversión total en infraestructura de telecomunicaciones estimada en 49 mil 100 millones de dólares, 17 mil millones de dólares serían necesarios para cerrar las brechas digitales y modernizar las redes.

Los otros 32 mil millones de dólares son los estimados para ampliar la capacidad de las redes para poder cursar el aumento del tráfico de internet en un contexto en el que es evidente la capacidad que tiene cada uno de los OTTs para influir en el ritmo de crecimiento del tráfico.

De hecho, en 2024, dos terceras partes del tráfico global fueron generadas por sólo ocho plataformas: Google, Meta, Netflix, Microsoft, TikTok, Apple, Amazon y Disney, mientras que a nivel América Latina, cuatro de ellas generan 74 por ciento del tráfico móvil.

“Las redes de telecomunicaciones tienen elementos y subsistemas cuyo dimensionado depende del tráfico de datos cursado, y esperado. Por ese motivo, el aumento del tráfico que transita una red provoca un aumento de los costes de dicha infraestructura, tanto de inversión como de operación y mantenimiento”.

Y es que algunos servicios sobre internet son competidores de los operadores en los mercados de servicios finales a los usuarios, donde aplicaciones OTT (que ofrecen contenido de audio y video a

través de internet), compiten con los servicios basados en red, así como las Big Tech, que son grandes usuarios del servicio de transporte de las redes de los operadores en los mercados de conectividad.

Dado que tanto los proveedores OTT, como sus clientes, utilizan la red para transmitir información, esto convierte a las redes de telecomunicaciones de acceso a Internet en un mercado de doble cara con dos tipos diferentes de usuarios: los usuarios finales para comunicarse entre ellos y con sus proveedores de servicios en línea, y proveedores de servicios over-the-top (OTT) para conectarse con sus clientes (los usuarios finales).

“Menores ingresos, altos costos de cumplimiento regulatorio, altos precios de espectro y elevados impuestos y tasas sectoriales han deteriorado la rentabilidad de los operadores latinoamericanos desde 2010, mientras que la de los proveedores OTT aumentaba, al captar la mayor parte del valor generado sobre Internet. Las asimetrías regulatorias generan fuertes distorsiones en los mercados”.

El Cet.la apunta que como consecuencia de estos efectos, la posición relativa en el mercado de los operadores latinoamericanos frente a los proveedores OTT se ha deteriorado continuamente durante los últimos 15 años.

Si hacia 2010 ambos tipos de empresas tenían posiciones similares en el mercado, la posición financiera y competitiva de los operadores se ha degradado, mientras que los OTT líderes se han convertido en las empresas de mayor valor en bolsa de todo el mundo.

“Aquellas empresas que tienen una regulación ligera y presión fiscal moderada han visto sus negocios crecer y prosperar”.

De acuerdo con el reporte, existen alternativas para asegurar la sostenibilidad de las inversiones en conectividad en Latinoamérica:

- Modelo de libertad general: No se aplica regulación sectorial ni a operadores ni a los OTT. Es el que se aplica en Estados Unidos con desregulación de los operadores, no regulación de los OTT y control ex post de la neutralidad de red.
- Modelo de regulación universal: Se aplica regulación sectorial tanto a los operadores como a los OTT. Es el aplicado en la Unión Europea, donde se ha mantenido la regulación ex ante de los operadores y se empieza a aplicar también regulación ex ante a los OTT.
- Modelo de regulación funcional: La regulación aplicable a algunos servicios OTT sería equilibrada respecto a otros agentes con servicios de funcionalidad similar. Este modelo se observa como tendencia incipiente en algunos países de la región y el mundo. Los servicios de ambos son parte del mismo mercado y las Big Tech son considerados grandes usuarios de las redes, como otros usuarios empresariales.

Para Maryleana Méndez, Secretaria General de la Asociación Interamericana de Empresas de Telecomunicaciones (ASJET), el reporte arroja “cifras alarmantes”, pero también deja en claro los posibles pasos: desregulación y reducción de cargas fiscales sectoriales, actualización de las definiciones de mercado de conectividad como mercado de dos caras, disposición de espectro suficiente y en condiciones adecuadas, y apoyo en programas de expansión de cobertura y asequibilidad.

Notas de Telecomunicaciones					
Título:	Reporta IFT resultados de estrategia de Gobierno de Datos				
Encabezado:					
Fecha:	09/06/25	Fuente:	CONSUMOTIC	Por:	Guadalupe Michaca
Link:	<a href="https://consumotic.mx/telecom/reporta-ift-resultados-de-estrategia-de-gobierno-de-datos/">https://consumotic.mx/telecom/reporta-ift-resultados-de-estrategia-de-gobierno-de-datos/</a>				

Con el objetivo de aportar una guía práctica y replicable para otras organizaciones que busquen profesionalizar su gestión de datos, el Instituto Federal de Telecomunicaciones (IFT) presentó los resultados de la experiencia obtenida en la implementación del marco de Gobierno de Datos, que tuvo como primer caso de negocio piloto el Registro Público de Concesiones (RPC).

El Gobierno de Datos es la función de gestión que permite asegurar la calidad, integridad, seguridad y usabilidad de los datos con los que cuente una organización de modo que se incremente la confianza en el uso de esa información, e incluya los procesos, roles, políticas, estándares y métricas que garanticen que una organización alcance sus objetivos.

“La definición de un caso de negocio piloto para la implementación de la estrategia de Gobierno de Datos fue un paso fundamental, permitiendo aplicar los principios y metodologías de manera controlada y demostrando valor rápidamente”, detalla el Reporte de Resultados del Caso de Negocio: Registro Público de Concesiones (RPC).

La elección del Registro Público de Concesiones (RPC) obedeció a una naturaleza estratégica y transversal dentro del IFT, pues concentra la información central de los títulos (Concesiones, Permisos y Autorizaciones) otorgados por el órgano regulador en materia de telecomunicaciones y radiodifusión, así como los datos de los operadores y la acreditación de sus representantes legales.

En esencia, el RPC funciona como el repositorio maestro de la información de los “sujetos regulados del IFT, o “clientes” si se viera desde una perspectiva empresarial.

“Este paralelismo con una empresa privada es crucial: al igual que la información de los clientes es vital para áreas de marketing (para ofertas enfocadas), ventas (para mantener la relación y ofrecer nuevos productos), facturación y cobranza, o atención al cliente (para un trato personalizado), la información contenida en el RPC es un insumo de alto valor estratégico para las diversas tareas sustantivas de las Unidades Administrativas del IFT”.

El informe detalla cómo la calidad y accesibilidad de estos datos impacta directamente la capacidad del IFT para realizar sus funciones de supervisión y promoción del desarrollo eficiente de los sectores regulados.

Así, la implementación del Gobierno de Datos en el RPC representa un fortalecimiento directo en la regulatoria laboral y de gestión interna del IFT, alineándose con diversas líneas de acción regulatoria de su hoja de ruta 2021-2025, como el asegurar la eficiencia interna en el desarrollo de las funciones regulatorias y de competencia, fortalecer el diseño institucional y el análisis de las políticas internas con el fin de mejorar los procesos y procedimientos a cargo del Instituto.

De igual forma fomenta la sistematización y digitalización de los procesos de trabajo internos y externos, minimizando el impacto administrativo y promoviendo un gobierno digital y abierto, dentro y fuera del instituto, además de diseñar e implementar capacidades de inteligencia de datos para mejorar los procesos de análisis y generar una política regulatoria y política de competencia más eficiente.

El IFT recordó que hasta antes del 2023, no se contaba con una estructura formal de Gobierno de Datos, carencia que en ocasiones generaba duplicidades, falta de estandarización, y dificultades en el acceso y aprovechamiento de la información.

“Ante esta situación, el Pleno del IFT reconoció la importancia estratégica de los datos para potenciar su rol como órgano regulador en el desarrollo de las telecomunicaciones y la radiodifusión, y la necesidad de fortalecer su capacidad técnica para responder a las demandas actuales con eficiencia, transparencia, acceso a la información y rendición de cuentas”.

Notas de Telecomunicaciones					
Título:	Apuestan empresas de telecom a la nube.- ASW				
Encabezado:					
Fecha:	09/06/25	Fuente:	REFORMA	Por:	Luis Pablo Segundo
Link:	<a href="https://www.reforma.com/apuestan-empresas-de-telecom-a-la-nube-asw/ar3018810">https://www.reforma.com/apuestan-empresas-de-telecom-a-la-nube-asw/ar3018810</a>				

En México, además de las industrias de comercio electrónico y los bancos, la de telecomunicaciones es la que más está migrando parte de su infraestructura física a los servicios de la nube, informó Rubén Mugártegui, director general de Amazon Web Services (AWS) en México.

**\*\*SE REQUIERE SUSCRIPCIÓN**

Notas de Telecomunicaciones					
Título:	La Agencia de Transformación Digital “nos afectará a todos”, no solo a concesionarios de radio y TV				
Encabezado:					
Fecha:	08/06/25 (por la tarde)	Fuente:	CRÓNICA	Por:	Ignacio Pérez Vega
Link:	<a href="https://www.cronica.com.mx/jalisco/guadalajara/2025/06/08/la-agencia-de-transformacion-digital-nos-afectara-a-todos-no-solo-a-concesionarios-de-radio-y-tv/">https://www.cronica.com.mx/jalisco/guadalajara/2025/06/08/la-agencia-de-transformacion-digital-nos-afectara-a-todos-no-solo-a-concesionarios-de-radio-y-tv/</a>				

Medios de comunicación, académicos y defensores de derechos humanos en Jalisco y en el país deben ejercer presión para que los diputados federales y senadores de Morena no aprueben la Ley de Telecomunicaciones (Ley Telecom), que busca crear la Agencia de Transformación Digital y Telecomunicaciones (ATDT), advirtió el líder de la bancada del PRI en la Cámara de Diputados, Rubén Moreira.

El líder legislativo del PRI, junto con el economista Mario Di Costanzo, ex diputado federal, estuvieron en Guadalajara para participar en la conferencia “Ley Mordaza. Implicaciones y Desafíos para la Libertad de Expresión en México”, a invitación de la Fundación Colosio en Jalisco, que preside Hortensia Noroña.

La iniciativa enviada por la presidenta Claudia Sheinbaum se presentó el 26 de abril, cinco meses después de que se eliminó al Instituto Federal de Telecomunicaciones (IFT) y crea la ATDT, una “supersecretaría” por las facultades que tendrá, pero que no incluye temas de competencia económica en telecomunicaciones. Esta Agencia ha generado polémica porque el Estado será jugador y árbitro en el mercado.

Moreira señaló que este tema, que está próximo a votarse en el Congreso de la Unión, afecta no solo a los periodistas o a los concesionarios de radio y televisión, sino a todo aquel que use las redes sociales. La Agencia de Transformación Digital tendría atribuciones para llevar el registro de nuestro uso de aparatos digitales, lo cual viola la privacidad.

“Un registro telefónico puede ser una llamada que yo les haga a ustedes y se vaya al buzón de voz. O por ejemplo, la ubicación en tiempo real de donde están ustedes y por lo tanto, los datos que emiten nuestros teléfonos permiten saber que todos estamos juntos aquí. Ni siquiera que te intervengan el teléfono, con que conozcan tus datos, tus registros, tus ubicaciones, tus traslados, con eso hay un montón de violaciones a la vida privada de las personas y esto sería sin la intervención de jueces y ahí está la Agencia”, explicó Moreira.

Mario Di Costanzo señaló que la reforma a la Ley de Telecomunicaciones afecta la libertad de expresión y de prensa, así como el derecho de los ciudadanos a estar informados. Si algún sitio digital o algún medio de comunicación es crítico del gobierno y eso no les gusta a las autoridades federales, “simplemente le van a bajar el switch” y la sacarán de circulación.

“Al tener el rango de secretaría de estado, la Agencia no puede ser un organismo autónomo, por definición de ley. Le quisieron ‘parchar’ diciendo que va a tener cinco notables o cinco ilustres, o cinco consejeros, que más allá que los va a designar la propia presidenta, lo cual no le da nada de autonomía, no está claro si sus opiniones serán vinculantes o nada más serán opiniones”, subrayó Di Costanzo.

Por ello, ambos ponentes señalaron que todos los ciudadanos deben seguir la discusión sobre la Ley de Telecomunicaciones, que busca crear entre otras cosas, la Agencia de Transformación Digital.

En el proyecto de ley se establece que las plataformas digitales con distribución de contenidos en México y que difundan campañas de gobiernos extranjeros podrán ser bloqueada temporalmente por la ATDT.

Notas de Telecomunicaciones					
Título:	Defender la libertad de expresión es garantizar una sociedad justa, informada y abierta: Rubén Moreira				
Encabezado:					
Fecha:	08/06/25 (por la tarde)	Fuente:	HOJA DE RUTA	Por:	Redacción

Link:	<a href="https://hojaderutadigital.mx/defender-la-libertad-de-expresion-es-garantizar-una-sociedad-justa-informada-y-abierta-ruben-moreira/">https://hojaderutadigital.mx/defender-la-libertad-de-expresion-es-garantizar-una-sociedad-justa-informada-y-abierta-ruben-moreira/</a>
-------	---

- En el marco de la conmemoración del “Día de la Libertad de Expresión”, el coordinador parlamentario lamentó que más de 35 analistas de este país han sido retirados de los programas de opinión.
- Insistió en eliminar la “Ley Censura” por representar un grave retroceso para la libertad de expresión en México.
- Una reforma en materia de telecomunicaciones debe surgir de la sociedad, de los medios de comunicación, de periodistas y de defensores de derechos humanos, subrayó.

La libertad de expresión es uno de los pilares esenciales de cualquier democracia que se tiene que defender para vivir en una sociedad justa y abierta, aseguró el diputado federal Rubén Moreira Valdez, por lo que advirtió que debilitarla solo significa un retroceso y un peligro directo a los derechos de los ciudadanos.

En el marco de la conmemoración del 7 de junio, “Día de la Libertad de Expresión”, el coordinador parlamentario afirmó que sin libertad de expresión no hay democracia, solo es una simulación que puede llevar al régimen a actuar con autoritarismo y limitar el derecho a la información.

Al participar este viernes en la Conferencia Magistral: “Ley Mordaza, Ley de Telecomunicaciones”, en Jalisco, el líder congresista lamentó que más de 35 analistas de este país han sido retirados de los programas de opinión y que el Canal 11, que era un espacio donde se escuchaban las voces de Sergio Aguayo, María Amparo Casar y Francisco José Paoli Bolio, ahora solo es un promotor de la Cuarta Transformación.

Acompañado del economista Mario Di Costanzo, de la presidenta del Comité Directivo Estatal del PRI en Jalisco, Laura Haro, y de Hortensia Noroña, presidenta de la Fundación Colosio en esta entidad, señaló que cerrar los espacios de opinión limita a los medios a contar con los grandes analistas que evalúan al gobierno, de tener programas de debate o noticieros donde se discuta.

Por esta razón, el legislador coahuilense alertó sobre el monstruo que se pretende crear con la Agencia de Transformación Digital. Indicó que la otra clave de todo esto, es el control del Estado en lo que se informa, se piensa, se dice, se guarda, y qué hacemos nosotros en el día a día.

Con la Ley de Telecomunicaciones, mencionó que se tiene el riesgo de que cuando los medios sean incómodos, se les podría bajar el switch. En ese sentido, puntualizó que la Agencia antes mencionada tendrá la facultad de controlar desde las concesiones de radio y televisión hasta la operación de telégrafos y correos, así como eliminar plataformas digitales.

“Oiga, pues yo tengo mi página de internet, pues según el artículo 109 se te puede dar para abajo tu página, esto puede pasar cuando haya un momento de crisis o el gobierno comience a tener dificultades”, enfatizó para después afirmar que, además, se crea una narrativa donde el régimen se apropia de palabras y las utiliza a su conveniencia, como lo ha hecho con la palabra “Pueblo”.

Por lo anterior, el coordinador Rubén Moreira insistió en eliminar la “Ley Censura” que representa un grave retroceso para la libertad de expresión en México y recordó que cualquier reforma en materia de telecomunicaciones debe surgir de la sociedad, de los medios de comunicación, de periodistas y de defensores de derechos humanos. “No hay libertad sin medios y redes libres”, concluyó.

Notas de Telecomunicaciones					
Título:	Cofece e IFT, camino al cadalso				
Encabezado:					
Fecha:	09/06/25 (por la tarde)	Fuente:	YAHOO NEWS	Por:	Marco A. Mares
Link:	<a href="https://es-us.noticias.yahoo.com/cofece-ift-camino-cadalso-060910151.html?guccounter=1&amp;guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&amp;guce_referrer_sig=AQAAAK2hi8FK41eXelFcORdmQh5u7bThsrWKyax1ZRPmovUrO59FnKLuNMxgufuipu20ONfoRfUcYPdoB_t_nBBgujP_DmCtPeUl4xEyYF35Rwk5aSiS3pD0VeultBRUt8NnSyPv35VkAxOXgW0iOsYHShJdliv_2ANbJljqDBwdzL0">https://es-us.noticias.yahoo.com/cofece-ift-camino-cadalso-060910151.html?guccounter=1&amp;guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&amp;guce_referrer_sig=AQAAAK2hi8FK41eXelFcORdmQh5u7bThsrWKyax1ZRPmovUrO59FnKLuNMxgufuipu20ONfoRfUcYPdoB_t_nBBgujP_DmCtPeUl4xEyYF35Rwk5aSiS3pD0VeultBRUt8NnSyPv35VkAxOXgW0iOsYHShJdliv_2ANbJljqDBwdzL0</a>				

Aunque todavía no hay una fecha específica, la Comisión Federal de Competencia Económica (Cofece) y el Instituto Federal de Telecomunicaciones (IFT), están condenadas a su extinción.

Están en camino al cadalso.

Son acusadas de ser parte del entramado neoliberal.

Lo que quede de ellas será parte de la “transformación”, como ahora se le dice a aquello que retrocede al pasado y en aquellos años se llamó “estatismo”.

En la simulación de foros democráticos se hace toda clase de “malabares” para encubrir que serán parte del engranaje centralista gubernamental.

Lo más probable es que sean relevadas a finales de este o principios del próximo año.

No se sabe, cómo serán las instituciones que las sustituyan.

La reconstitución de Cofece, como el del IFT, está todavía a discusión y en definición.

De alguna forma, al final de sus respectivas vidas institucionales, la suerte de ambos organismos está ligada.

Paradójicamente, por razones de especialización, el tema de la competencia económica, las mantuvo separadas.

La competencia económica en materia de telecomunicaciones la mantuvo el IFT.

La competencia económica, en general en prácticamente todos los mercados y, en el de las telecomunicaciones, es el quid de los dos órganos que a la fecha, por ley, siguen siendo autónomos.

Hasta ahora, hay una mucho mayor discusión y preocupación por la redefinición del IFT.

Sobre la reconfiguración de la Cofece, el debate ha sido menos acalorado.

Sin embargo, también se ha registrado enorme preocupación por los cambios que podría tener.

En el avance hacia el cadalso, Cofece e IFT y sus respectivos y mermados cuerpos colegiados, han dado muestras de institucionalidad.

Se han manifestado dispuestos a cooperar hacia un cambio ordenado.

Cofece y el IFT recibieron para éste año 2025, presupuestos ínfimos.

La Cofece, ejerce un presupuesto equivalente a menos de la tercera parte del que originalmente solicitó.

El IFT cuenta con una cantidad que representa un 70% menos de lo que pidió.

Con todo y la asfixia económica y su famélica condición, Cofece e IFT cerraron el 2024, con avances importantes.

Cofece intervino en sectores prioritarios como agroalimentario, financiero, energético, salud, transporte y compras públicas.

Logró un impacto estimado en el 40% de la economía mexicana, según datos del Banco Mundial.

Cofece continúa gestionando más de 150 operaciones de fusiones, equivalentes al 10% del PIB, y 25 investigaciones por prácticas anticompetitivas en mercados clave, como servicios financieros digitales y gas natural.

En 2023, la Cofece reportó beneficios para los consumidores por 30,697 millones de pesos mediante la corrección de prácticas anticompetitivas.

Aunque no hay una cifra específica para 2024, se estima que el impacto es significativo.

Especialmente en sectores como el de salud, donde se evitaron sobrepagos que afectan al erario público y a los consumidores.

El IFT resolvió 823 asuntos de relevancia, 50% más que en 2023.

Atendió temas como la regulación del espectro radioeléctrico, la supervisión de concesiones y la promoción de la competencia en telecomunicaciones y radiodifusión.

En la última década, el IFT ha impuesto sanciones significativas a empresas como América Móvil, Televisa y Megacable.

Logró reducir la participación de mercado de Telcel en telecomunicaciones móviles de 69% a 59% y en internet fijo de 72% a 37%.

En el 2024, el IFT recaudó 18,412.33 millones de pesos (aproximadamente 901 millones de dólares) por su vigilancia del espectro radioeléctrico, la asignación y refrendo de concesiones, sanciones a concesionarios y otros trámites regulatorios.

En el gobierno lopezobradorista, del 2019 hasta el 2024, el IFT recaudó cerca de 5,000 millones de dólares por su trabajo regulatorio, incluyendo la supervisión del espectro y la competencia económica en telecomunicaciones y radiodifusión.

La Cofece y el IFT tienen los días contados. Viene el fin de los órganos autónomos colegiados.

La extinción de la autonomía de los órganos reguladores, podría implicar el retorno a los tiempos de la discrecionalidad regulatoria y el probable acendramiento del predominio monopólico y oligopólico.

Notas de TI					
Título:	Diseñar las políticas más preferenciales para promover el desarrollo de la inteligencia artificial				
Encabezado:	Se espera que se legalicen muchas políticas innovadoras para atraer recursos humanos de tecnología digital de alta calidad (vietnamitas, vietnamitas de ultramar y extranjeros).				
Fecha:	09/06/25	Fuente:	VIETNAM	Por:	
Link:	<a href="https://www.vietnam.vn/es/thiet-ke-nhung-chinh-sach-uu-dai-cao-nhat-de-thuc-day-phat-trien-tri-tue-nhan-tao">https://www.vietnam.vn/es/thiet-ke-nhung-chinh-sach-uu-dai-cao-nhat-de-thuc-day-phat-trien-tri-tue-nhan-tao</a>				

El presidente del Comité de Ciencia, Tecnología y Medio Ambiente, Le Quang Huy, informó en la reunión.

Al informar sobre la recepción, explicación y revisión del proyecto de Ley de la Industria de Tecnología Digital en la reunión del Comité Permanente de la Asamblea Nacional (NASC) en la mañana del 9 de junio, el presidente del Comité de Ciencia, Tecnología y Medio Ambiente, Le Quang Huy, enfatizó que el Estado tendrá las más altas políticas preferenciales para promover el desarrollo, despliegue y uso de la inteligencia artificial (IA) y políticas preferenciales sobresalientes para desarrollar la industria de semiconductores, formando un ecosistema de semiconductores vietnamita.

“La producción de productos y servicios clave de tecnología digital; la producción de software; el desarrollo de sistemas de inteligencia artificial; la investigación, el desarrollo, el diseño y la producción de chips semiconductores; y la construcción de centros de datos de inteligencia artificial se consideran industrias y ocupaciones con incentivos especiales para la inversión”, afirmó el Sr. Le Quang Huy.

El proyecto de ley, tras ser revisado, ha estipulado un mecanismo para excluir la responsabilidad en las pruebas de productos y servicios que aplican tecnología digital.

Con el fin de fomentar la innovación y reducir los riesgos para las empresas al implementar nuevas tecnologías, ayudando a que los productos de tecnología digital lleguen rápidamente al mercado y a los usuarios, el proyecto de ley revisado ha estipulado un mecanismo de prueba controlado

(sandbox) para productos y servicios que apliquen tecnología digital, incluyendo un mecanismo para excluir la responsabilidad en las pruebas.

Entre las políticas que apoyan el desarrollo de recursos humanos, cabe destacar la política para atraer recursos humanos de alta calidad en tecnología digital (vietnamitas, vietnamitas en el extranjero y extranjeros). En concreto, se prevé que el proyecto estipule la emisión de tarjetas de residencia temporal de 5 años y sus prórrogas para extranjeros y familiares (padre, madre, cónyuge e hijos menores de 18 años), así como apoyo para la búsqueda de empleo y estudios en Vietnam para sus familias. Además, el proyecto estipula la exención de permisos de trabajo para extranjeros de alta cualificación; incentivos para el impuesto sobre la renta de las personas físicas, etc.

El borrador establece principios para el desarrollo responsable y ético de la IA

En cuanto a la gestión y el desarrollo de la IA, el proyecto de ley establece los principios del desarrollo de la IA centrados en los seres humanos, garantizando la transparencia, la explicabilidad, la rendición de cuentas, no exceder el control humano, la seguridad, la protección, el cumplimiento de las leyes sobre datos personales y protección del consumidor, el control de riesgos, etc. para garantizar un desarrollo de la IA responsable y ético en la sociedad; exigiendo marcas de identificación para los sistemas de IA que interactúan directamente con los seres humanos (deben notificar a los usuarios que están interactuando con la IA) y los productos de tecnología digital creados por la IA (deben tener marcas de identificación); las responsabilidades de los sujetos que desarrollan, proporcionan, implementan y utilizan los sistemas de IA también son contenidos importantes en el proyecto de ley.

En cuanto a los activos digitales, el proyecto de ley los divide en activos virtuales (que pueden utilizarse para intercambio o inversión, excluyendo valores, monedas fiduciarias digitales y otros activos financieros) y criptoactivos (que utilizan tecnología criptográfica para la autenticación, excluyendo también valores, monedas fiduciarias digitales y otros activos financieros). La gestión de activos digitales incluye la creación, emisión, almacenamiento, transferencia, determinación de la propiedad, derechos y obligaciones de las partes, medidas para garantizar la seguridad de la información, seguridad de la red, prevención del blanqueo de capitales, lucha contra la financiación del terrorismo y las condiciones para operar en servicios de criptoactivos.

Notas de TI					
Título:	Aumentan estafas digitales: ciberdelincuentes usan correo falso y páginas clones				
Encabezado:					
Fecha:	09/06/25	Fuente:	DIARIO YUCATÁN	DEPor:	Redacción
Link:	<a href="https://www.yucatan.com.mx/mexico/2025/06/09/aumentan-estafas-digitales-ciberdelincuentes-usan-correo-falso-y-paginas-clones.html">https://www.yucatan.com.mx/mexico/2025/06/09/aumentan-estafas-digitales-ciberdelincuentes-usan-correo-falso-y-paginas-clones.html</a>				

CIUDAD DE MÉXICO (El Universal).— Plataformas en línea utilizadas para firmar documentos de forma remota están siendo aprovechadas por ciberdelincuentes para lanzar ataques dirigidos que buscan robar contraseñas, información y obtener acceso a redes corporativas.

En los últimos meses, se ha identificado un aumento en el uso de facturas falsas, códigos QR maliciosos y páginas web que suplantan portales legítimos como Microsoft o servicios internos de empresas, de acuerdo con la advertencia de la firma de ciberseguridad ESET.

La firma explicó que el ataque inicia cuando la víctima recibe un correo electrónico con la apariencia de una notificación oficial. En el cuerpo del mensaje se incluye un botón con la leyenda “revisar documento” o un archivo adjunto con un código QR. Al hacer clic o escanear, el usuario es redirigido a una página falsa de inicio de sesión, diseñada con el objetivo de capturar datos personales o las credenciales corporativas.

La firma de ciberseguridad agregó que el uso de códigos QR se ha vuelto cada vez más común como táctica para eludir filtros de seguridad. Estos códigos son escaneados desde teléfonos móviles, dispositivos que muchas veces no cuentan con protección contra enlaces maliciosos, lo que facilita la ejecución del fraude sin alertas visibles para el usuario.

La firma también documentó el uso de cuentas reales registradas en plataformas de firma digital. Los atacantes emplean las herramientas oficiales para enviar sobres legítimos que contienen facturas falsas con la imagen de proveedores conocidos o dependencias gubernamentales. El objetivo es inducir a empresas a realizar transferencias a cuentas de los delincuentes.

Otro tipo de ataque identificado consiste en correos de ‘phishing’ que simulan ser comunicaciones de áreas de recursos humanos, nóminas o autoridades locales. Estas páginas buscan obtener accesos que permiten a los atacantes desplazarse dentro de redes empresariales, escalar privilegios y ejecutar ataques más graves, como robo de información o despliegue de ‘ransomware’.

Según el informe más reciente de Verizon, el ‘phishing’ fue el punto de entrada en 19% de los incidentes analizados, y el 60% de los casos incluyó errores humanos.

#### Consejos preventivos.

Como prevención, se recomienda verificar la autenticidad de todos los documentos electrónicos recibidos, evitar escanear códigos QR sin confirmar su origen y mantener actualizados los sistemas de seguridad, especialmente en dispositivos móviles.

#### Aumento Ciberataques

Ciberdelincuentes aprovechan servicios digitales para robar datos y dinero.

#### Ataques dirigidos

Plataformas de firma digital están siendo explotadas por ciberdelincuentes para ejecutar ataques dirigidos.

#### Objetivo ilícito

Estos buscan robar contraseñas, información confidencial y obtener acceso a redes corporativas mediante engaños sofisticados.

#### Tácticas comunes

Se ha observado un aumento en el uso de facturas falsas, códigos QR maliciosos y páginas fraudulentas que imitan portales o servicios internos de empresas.

Notas de TI					
Título:	Ciberseguridad para todos: protegiendo tus datos personales en la era de las filtraciones				
Encabezado:	La exposición de información confidencial puede derivarse de fallos tecnológicos, negligencia humana o ataques maliciosos				
Fecha:	08/06/25 (por la tarde)	Fuente:	INFOBAE	Por:	Juan Ríos
Link:	<a href="https://www.infobae.com/tecnologia/2025/06/08/ciberseguridad-para-todos-protegiendo-tus-datos-personales-en-la-era-de-las-filtraciones/">https://www.infobae.com/tecnologia/2025/06/08/ciberseguridad-para-todos-protegiendo-tus-datos-personales-en-la-era-de-las-filtraciones/</a>				

Las filtraciones de datos se han convertido en un tema de creciente preocupación tanto para usuarios como para organizaciones. Estos incidentes representan una amenaza inmediata para la privacidad y pueden tener repercusiones a largo plazo que afectan la vida personal y profesional de aquellos involucrados.

El fenómeno de las filtraciones de datos se ha intensificado, obligando a reevaluar las prácticas de seguridad y la gestión de la información en todo el mundo y plataformas.

Qué son las filtraciones de datos y cómo suceden

Una filtración de datos es un evento en el que información confidencial, protegida o sensible se expone a personas no autorizadas. Este suceso puede desencadenarse debido a diversos factores tales como negligencias humanas, fallos tecnológicos o ataques malintencionados.

En términos específicos, las filtraciones pueden involucrar cualquier tipo de información, desde detalles personales como nombres y direcciones, hasta información corporativa crítica y secretos gubernamentales.

El auge de la tecnología digital ha multiplicado los puntos de vulnerabilidad. Los dispositivos IoT (Internet de las Cosas), por ejemplo, plantean un riesgo significativo, ya que a menudo carecen de medidas de seguridad robustas, facilitando así el acceso no autorizado a datos sensibles. Asimismo, la interdependencia de sistemas conectados amplifica los riesgos asociados a una gestión deficiente de la ciberseguridad.

Ejemplos reales de la actualidad de las filtraciones

En México, el sector salud ha enfrentado un incremento alarmante en ciberataques, con un 50% de los centros médicos reportando violaciones de datos personales, según un informe de SOTI.

Estos ataques a menudo utilizan ransomware, bloqueando el acceso a registros médicos, lo que no solo compromete la privacidad del paciente sino también la operatividad de las instalaciones. La exposición de esta información puede llevar a graves interrupciones en los servicios de salud y afectar directamente la vida de los pacientes.

Aunque las filtraciones de datos son una preocupación global, la industria aseguradora también ha sido un blanco frecuente. Según Fasecolda (organización de gestión de datos en Colombia), en 2024,

la industria en Colombia reportó 30.739 casos de fraude relacionados con seguros, resultando en pérdidas económicas superiores a \$272 mil millones.

Estas actividades fraudulentas, que utilizan desde suplantación de identidades hasta el uso de phishing para obtener información sensible, destacan la sofisticación creciente de las operaciones delictivas.

Cuál es el impacto de las filtraciones de datos

Desde el punto de vista individual, la exposición de datos personales puede resultar en robo de identidad, lo que conlleva problemas legales y financieros. Las empresas, a su vez, pueden experimentar una pérdida significativa de reputación y confianza, afectando su imagen y estabilidad financiera a largo plazo.

Las filtraciones en instituciones gubernamentales pueden comprometer la seguridad nacional, exponiendo información crítica de procedimientos y operaciones.

Cómo prevenir las filtraciones de datos

A la luz de los crecientes riesgos, es esencial implementar estrategias de prevención robustas que aborden tanto aspectos tecnológicos como de comportamiento humano. Los expertos en seguridad recomiendan las siguientes prácticas:

1. Actualización y seguridad de sistemas: es crucial mantener actualizado el software y hardware utilizado, aplicando los parches de seguridad más recientes para cerrar cualquier vulnerabilidad que pueda ser aprovechada por los atacantes.
2. Uso de contraseñas fuertes y autenticación de dos factores: adoptar contraseñas complejas y únicas para cada servicio, además de implementar la autenticación de múltiples factores, reduce significativamente el riesgo de acceso no autorizado.
3. Encriptación de datos: el cifrado de información sensible es una medida eficiente para garantizar que, incluso en caso de filtración, los datos no sean fácilmente accesibles para los intrusos.
4. Educación y conciencia del usuario: capacitar a trabajadores y usuarios sobre las amenazas de ciberseguridad y fomentar buenos hábitos digitales, incluyendo el reconocimiento de phishing y otras tácticas comunes, es fundamental para minimizar errores humanos.

Notas de TI					
Título:	Ransomware, ¿por qué es la cúspide del cibercrimen global?				
Encabezado:					
Fecha:	08/06/25 (por la tarde)	Fuente:	THE STANDARD CIO	Por:	Elibeth Eduardo G.
Link:	<a href="https://thestandardcio.com/2025/06/08/ransomware-cuspide-cibercrimen-global/">https://thestandardcio.com/2025/06/08/ransomware-cuspide-cibercrimen-global/</a>				

¿Sabía usted que el caso más temprano de ciberextorsión ocurrió en 1989? El concepto de ransomware se remonta a cuando, en ese año, el Dr. Joseph Popp distribuyó el troyano del SIDA: un malware que cifraba archivos en computadoras infectadas y exigía un pago por su recuperación.

Aunque usted no lo crea, la infección ocurría mediante el uso de un disquete. Sin duda, era un método rudimentario en comparación con los sofisticados mecanismos actuales.

Pero ese disquete pasó a la historia como el pionero en el modelo de extorsión digital.

De hecho, sólo en 2024, este tipo de ataques logró estafar a empresas por más de US\$ 1.100 millones en todo el mundo.

“El ransomware es la ciberamenaza que más ha evolucionado en los últimos 10 a 15 años. Si bien comenzó con un pago por correo, hoy es un negocio global”, refirió el estratega de seguridad global de Splunk, empresa de Cisco, Mick Baccio.

Se sabe, agregó el especialista, que este tipo de infección es utilizada por bandas cibernéticas organizadas. También que algunas actividades que conducen a estos ataques son patrocinadas por estados de países como Rusia y Corea del Norte.

Dicho de otro modo, el ransomware es una de las más poderosas armas conocidas de las actuales ciberguerras.

Volvamos al disquete

Lo cierto es que, a lo largo de estos 35 años, el ransomware ha refinado sus técnicas de ataque y ampliando tanto sus alcances como su sofisticación.

¿Cómo pasó de un disquete a la amenaza que es hoy? Le llevó tiempo. La investigación histórica encuentra, en 2004, al malware GPCode como punto de inflexión al distribuirse masivamente por correo electrónico.

¿Con qué cubierta? Una que siempre funciona: se disfrazó de oferta de trabajo. Su éxito radicó en la capacidad de engañar a usuarios desprevenidos, lo cual le permitió propagarse sin grandes dificultades.

Todavía por aquel entonces las bandas dependían de las tarjetas de regalo para lograr su desafío más importante: lograr un mecanismo de pago que sea, esencialmente, irrastreado.

Por ello el año 2010 es un nuevo punto de inflexión gracias, nada más y nada menos, que a las criptomonedas.

Todo esto cambió, según el experto, cuando las criptos hicieron su irrupción, facilitando los pagos transfronterizos, tornándolos, prácticamente, en imposibles de rastrear.

Con este nuevo recurso evolucionando rápidamente, a partir de 2016, el ransomware alcanzó una nueva escala con ataques dirigidos a grandes empresas:

- SamSam fue uno de los primeros en explotar vulnerabilidades en redes corporativas, exigiendo rescates de cifras millonarias.
- Posteriormente, el ransomware \*Maze\* introdujo el concepto de doble extorsión, amenazando con divulgar información robada si el rescate no era pagado.

En la última década: Infraestructura crítica bajo ataque

Hoy en día, los grupos de ransomware han refinado sus estrategias, especializándose en sectores vulnerables como el financiero, el de salud y el de infraestructura crítica.

A menudo, estos objetivos carecen de recursos tecnológicos avanzados, lo cual facilita la ejecución de ataques devastadores.

Para agravar este escenario, los actores estatales también han intensificado su participación en estos ataques en la última década. Los conflictos bélicos abiertos en el mundo han sido detonante de esta nueva etapa.

En el último trimestre, Cisco Talos Incident Response identificó nuevas variantes como RansomHub, RCRU64 y DragonForce, además de la persistencia de amenazas como BlackByte y Cerber.

Blindaje básico

Ciertamente, el ransomware luce casi imbatible. No obstante, existen medidas clave para mitigar el impacto del ransomware.

La creación de copias de seguridad seguras sigue siendo una de las herramientas más eficaces contra el cifrado malicioso de archivos.

“El ransomware tiene un enorme talón de Aquiles: las copias de seguridad. Si existe una copia de respaldo de tus datos, puedes restaurarlos fácilmente en caso de un ataque”, señala el líder de Cisco Talos EMEA, Martin Lee.

Sin embargo, la protección efectiva no depende únicamente de respaldos de datos. La actualización de software, la segmentación de redes y la educación del personal en ciberseguridad desempeñan un papel fundamental.

A medida que los cibercriminales recurren a técnicas avanzadas de ingeniería social y falsificación digital, la conciencia humana se convierte en una línea de defensa crucial.

“Será cada vez más difícil confiar en lo que se ve y se escucha. Por lo tanto, es fundamental garantizar que las personas estén al tanto y preparadas para este tipo de ataques”, alerta el jefe de divulgación de Cisco Talos, Nick Biasini.

El ransomware no es una amenaza aislada, sino un problema global que requiere una estrategia coordinada.

La cooperación entre el sector público y privado, junto con políticas internacionales enfocadas en la seguridad digital, son esenciales para reducir su impacto y proteger a organizaciones vulnerables.

Notas de TI					
Título:	Neurodatos, nuevo oro digital, advierte Anahiby Becerril				
Encabezado:					
Fecha:	08/06/25 (por la tarde)	Fuente:	QUADRATIN	Por:	Redacción
Link:	<a href="https://mexico.quadratin.com.mx/neurodatos-nuevo-oro-digital-advierte-anahiby-becerril/">https://mexico.quadratin.com.mx/neurodatos-nuevo-oro-digital-advierte-anahiby-becerril/</a>				

CIUDAD DE MÉXICO, 8 de junio de 2025.- Ante la llegada de neurotecnologías que prometen ayudar contra la depresión o implantar chips en el cerebro para conectarlos a computadoras, hay que ser conscientes de la necesidad de proteger nuestros datos biométricos, que incluyen las ondas cerebrales, para evitar su uso indebido.

Así lo sugirió la académica de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM, Anahiby Becerril Gil, quien precisó:

“Cada vez más se ha normalizado la entrega de la identificación del rostro, voz, iris y huella digital al usar los llamados equipos inteligentes (celulares, relojes, tabletas, audífonos), sin cuestionar a quién se envía, para qué se utiliza, cuánto tiempo los conservarán o cuáles son los fines.”

Al ofrecer la conferencia Del dato al cerebro: privacidad y seguridad en un mundo conectado, la coordinadora académica del Diplomado Ciberseguridad manifestó que, desde hace tiempo, este último tema ha rebasado el campo técnico y ahora implica la protección de los derechos humanos.

A decir de la especialista, la gente debe dejar de pensar que es normal otorgarlos. La ley nos protege, la tecnología debe servirnos a nosotros y no al revés. Por ejemplo, si los bancos niegan la atención obligando a sus clientes a descargar una aplicación y usar datos biométricos, la persona puede ampararse en la legislación y exigir se le otorgue identificándose oficialmente.

Becerril Gil expresó: “Necesitamos anticiparnos a los riesgos, las neurotecnologías ya vienen, principalmente para usos médicos, pero se piensa en lúdicos con videojuegos. Lo anterior conlleva educarnos en materia de riesgos personales, resguardar la información biométrica, a quién se la comparto, por qué hacerlo, de lo contrario probablemente pueda generar problemas».”

En el encuentro realizado a distancia como parte del Seminario TIC, de la DGTIC, la experta en garantías fundamentales mencionó que el resguardo de neurodatos no es hablar del futuro, es una urgencia del mundo actual, más allá de likes en las redes sociales.

Aclaró que las neurotecnologías se refieren a dispositivos o procedimientos que ayudan a acceder a nuestra información mental y del sistema nervioso para controlar, investigar, evaluar y/o manipular la estructura y función de los sistemas neuronales de animales o seres humanos. Se crearon con el objetivo de ayudar ante padecimientos o enfermedades mentales.

Los casos famosos son las empresas Neuralink (Estados Unidos) que desarrolla chips llamados Link para monitorear y estimular la actividad cerebral, así como Flow Neuroscience (Suecia) con su

diadema Flow que promete incentivar regiones de este órgano para apoyar a aliviar los síntomas de la depresión.

Si se dice que los datos personales son el nuevo petróleo, los neurodatos serán el oro digital, porque con ellos se elaboran perfiles de usuario a los cuales carecemos de acceso; no es que sea malo, el problema es que tampoco sabemos si nos beneficia o perjudica, resaltó Becerril Gil.

Y recordó: en el caso de México, el artículo 16 de la Constitución determina que toda persona tiene derecho a la protección de sus datos personales y esto implica cualquier información, sin importar su formato (físico o digital); se hace distinción de los sensibles, los cuales se refieren a la intimidad.

Si de la actividad cerebral una compañía obtiene referencias que me hacen identificable, es un dato personal sensible, como es el caso de los biométricos. Tienen esa categoría porque se refieren a propiedades físicas, fisiológicas (cara, voz, iris, huella digital, información de ADN y datos neuronales), de comportamiento, o rasgos de la personalidad.

Esto ha llevado al surgimiento de una nueva tendencia impulsada por la Organización de las Naciones Unidas para la custodia de la neuroinformación, donde la educación en ciberseguridad es un elemento clave, destacó la investigadora.

A ello se ha llamado ciberneuroseguridad; se encarga específicamente de sugerir medidas, sistemas, herramientas y políticas para proteger la integridad, confidencialidad y disponibilidad del contenido de las neurotecnologías y su conexión con los seres humanos.

De acuerdo con Becerril Gil no significa estar en contra de la tecnología y la innovación, pero se necesita encontrar un balance entre lo que nos proporcionan y lo que damos a cambio.

Notas de TI					
Título:	La ciberseguridad industrial condiciona el avance digital de las empresas				
Encabezado:					
Fecha:	09/06/25	Fuente:	INTEREMPRESAS	Por:	
Link:	<a href="https://www.interempresas.net/Ciberseguridad/Articulos/600013-La-ciberseguridad-industrial-condiciona-el-avance-digital-de-las-empresas.html">https://www.interempresas.net/Ciberseguridad/Articulos/600013-La-ciberseguridad-industrial-condiciona-el-avance-digital-de-las-empresas.html</a>				

El 63,6% de las organizaciones industriales tiene previsto alcanzar una transformación digital completa en los próximos dos años. No obstante, los riesgos asociados a la ciberseguridad en entornos de tecnología operativa (OT) amenazan con ralentizar esta transición. Así lo recoge el informe 'Securing OT with Purpose-built Solutions', elaborado por Kaspersky en colaboración con VDC Research.

El documento refleja la coexistencia de distintos niveles de madurez digital en el sector: mientras un 31,1% de las empresas aún depende en gran medida de procesos manuales o se encuentra en fases iniciales de digitalización, un 22,7% ha implementado parcialmente tecnologías conectadas. El informe también constata una voluntad generalizada por adoptar modelos de mejora continua y capacidades digitales avanzadas.

La expansión de la conectividad entre sistemas IT y OT ha intensificado las preocupaciones relacionadas con la protección de infraestructuras críticas. Un 39,3% de los encuestados señala la ciberseguridad como el principal factor que dificulta la implantación de nuevas tecnologías en entornos OT. Esta inquietud se desglosa en varias causas: un 46,6% apunta a carencias en las medidas de protección existentes y otro 46,6% menciona la falta de recursos técnicos y humanos dedicados a ciberseguridad industrial.

Por otro lado, un 42,7% identifica barreras derivadas del cumplimiento normativo, mientras que un 41,7% alude a la dificultad de integrar de forma eficaz sistemas OT con infraestructuras IT, un aspecto clave para mantener la operatividad y proteger la integridad de los activos digitales.

#### Soluciones específicas para proteger entornos industriales

La investigación pone especial énfasis en la necesidad de garantizar la seguridad de los sistemas OT, ya que resulta imprescindible para que las iniciativas de transformación digital alcancen su potencial. Sin una protección adecuada, las organizaciones industriales se exponen a riesgos que pueden comprometer tanto la continuidad operativa como la seguridad de los datos.

Según Andrey Strelkov, responsable de la línea de producto de Ciberseguridad Industrial en Kaspersky, “es fundamental que las organizaciones adopten soluciones robustas que les permitan mitigar amenazas que podrían causar interrupciones graves y pérdidas económicas significativas”.

El informe concluye que el éxito de la digitalización industrial dependerá de la capacidad de las organizaciones para incorporar herramientas de ciberseguridad eficaces desde las fases iniciales de desarrollo. La confianza en los sistemas conectados, la resiliencia frente a ataques y el cumplimiento de las exigencias regulatorias marcarán el ritmo del cambio tecnológico en el ámbito OT durante los próximos años.

Notas de TI					
Título:	¿Están tus datos seguros? Las nuevas amenazas de ciberseguridad que todo usuario debe conocer				
Encabezado:	La seguridad en línea depende del conocimiento de las amenazas cibernéticas y de implementar medidas preventivas adecuadas				
Fecha:	08/06/25 (por la tarde)	Fuente:	INFOBAE	Por:	Juan Ríos
Link:	<a href="https://www.infobae.com/tecnologia/2025/06/08/estan-tus-datos-seguros-las-nuevas-amenazas-de-ciberseguridad-que-todo-usuario-debe-conocer/">https://www.infobae.com/tecnologia/2025/06/08/estan-tus-datos-seguros-las-nuevas-amenazas-de-ciberseguridad-que-todo-usuario-debe-conocer/</a>				

Todo usuario que tenga acceso a internet y esté continuamente en redes sociales debe entender los riesgos a los que está expuesto. Todos nuestros datos tienen un alto valor para los ciberdelincuentes, sin importar que no seamos famosos, influencers o millonarios. Y para robarlos, los ciberdelincuentes tienen una gran variedad de tácticas.

Ya sean desde modalidades conocidas como el phishing como otras más complejas como la denegación de servicio (DoS), es fundamental que los usuarios y organizaciones sepan cómo funcionan y cuáles son los riesgos que hay en cada una de las amenazas.

Cuáles son las modalidades de ciberataque

- Phishing y smishing

Según Check Point, empresa de ciberseguridad, el phishing continúa siendo uno de los métodos de ataque más reportados. Este delito cibernético busca robar información sensible, como credenciales de inicio de sesión y detalles financieros, mediante correos electrónicos u otros métodos de comunicación donde el atacante se disfraza de una entidad confiable.

En su variante conocida como smishing, los atacantes recurren a mensajes de texto SMS para atraer a los usuarios desprevenidos. A través de estos médiums, los criminales pueden engañar a sus víctimas para instalar malware o proporcionar acceso a terceros a redes internas, comprometiendo así no solo datos personales, sino también información de nivel corporativo.

- Malware

El malware, o software malicioso, abarca una variedad de amenazas diseñadas para introducirse en los sistemas y causar estragos. Entre los más notables se encuentra el ransomware, que cifra los archivos de una víctima, exigiendo un rescate por la clave para descifrarlos.

Otros tipos de malware incluyen los troyanos, que se presentan como software legítimo, y el spyware, que recopila datos sobre el usuario inadvertidamente. Este tipo de software puede extender su impacto a toda una red, convirtiéndose en una plaga empresarial que roba recursos informáticos y datos críticos con fines de lucro, como el cryptojacking, donde el sistema es utilizado para minar criptomonedas sin el conocimiento de la víctima.

- Ingeniería social

La ingeniería social es una técnica de manipulación psicológica destinada a extraer información crítica o instigar acciones específicas. Este tipo de ataques aprovechan las vulnerabilidades humanas, utilizando truco, coerción o instigación para engañar a personas para que abran puertas que, de otro modo, estarían firmemente cerradas.

Las formas incluyen desde el phishing (mediante correos electrónicos o mensajes sociales) hasta el vishing, o phishing telefónico, donde los atacantes buscan información confidencial directamente del individuo desprevenido.

- Ataques en la infraestructura de aplicaciones web

Con la virtualización de los servicios, las aplicaciones web se convierten en objetivos de alto valor. Ataques como la inyección SQL permiten a los actores maliciosos controlar las bases de datos, mientras que scripts entre sitios (XSS) pueden interceptar datos confidenciales al aprovechar vulnerabilidades en páginas web.

Las vulnerabilidades en estas aplicaciones presentan amenazas que requieren reconocimiento constante y respuesta inmediata para impedir que los atacantes exploten debilidades no parchadas.

- Denegación de servicio

Los ataques de denegación de servicio (DoS) tienen como objetivo interrumpir la disponibilidad de recursos en línea legítimos. Esta táctica respalda campañas de extorsión de rescate o sirve como diversiones mientras se producen otras intrusiones, como parte de una campaña más amplia de ransomware.

En su variante distribuida (DDoS), donde varios dispositivos son simultáneamente comprometidos, estas campañas sobrecargan servicios con solicitudes falsas, haciéndolos inaccesibles para usuarios autorizados.

- La intercepción en el medio del camino

Los ataques de hombre-en-el-medio (MitM) representan una amenaza insidiosa, interceptando comunicaciones entre usuario y destino para filtrar, modificar o espiar información.

Al controlar el flujo de datos, los atacantes pueden reconfigurar instrucciones, robar credenciales, o manipular transacciones de manera invisible al usuario afectado. Este tipo de amenazas es especialmente pernicioso si las comunicaciones interceptadas no están adecuadamente cifradas.

Notas de TI					
Título:	La inteligencia artificial mejora la detección del cáncer de mama en México, según la UNAM				
Encabezado:	Investigadores de la UNAM confirman que el uso de inteligencia artificial optimiza la detección temprana del cáncer de mama				
Fecha:	08/06/25 (por la tarde)	Fuente:	RÉCORD	Por:	Mariana Alcántara Contreras
Link:	<a href="https://www.record.com.mx/contra/la-inteligencia-artificial-mejora-la-deteccion-del-cancer-de-mama-en-mexico-segun-la-unam#google_vignette">https://www.record.com.mx/contra/la-inteligencia-artificial-mejora-la-deteccion-del-cancer-de-mama-en-mexico-segun-la-unam#google_vignette</a>				

Especialistas del Instituto de Ingeniería de la UNAM destacaron los beneficios de integrar inteligencia artificial (IA) en el sistema de salud durante el encuentro “Salud 5.0 y cáncer de mama: inteligencia artificial para la detección temprana y precisa.”

Oscar Pilloni Choreño señaló que la IA “no busca reemplazar al personal médico, sino potenciar sus capacidades clínicas”, y Rosa María Ramírez Zamora, directora del instituto, afirmó que esta tecnología permite realizar valoraciones “mucho más precisas”, además de reducir costos y facilitar tratamientos personalizados

En México, la escasez de recursos para la detección del cáncer de mama es crítica, con solo 689 mastógrafos y 352 radiólogos certificados, lo que limita la detección temprana en hasta el 85% de los casos. En 2022, se registraron 31,043 casos femeninos y en 2020 hubo 685,000 muertes, lo que resalta la necesidad urgente de implementar nuevos métodos de detección.

“Hay que perderle el miedo, sobre todo en aplicaciones médicas, y a su vez, hacer esfuerzos conjuntos entre academia y empresas para demostrar su fiabilidad”, destacó Pilloni.

La inteligencia artificial como aliada del diagnóstico clínico

La Universidad Nacional Autónoma de México sostiene que la inteligencia artificial representa una herramienta de apoyo clínico para los especialistas en radiología, no un reemplazo.

La herramienta de IA en mamografías puede disminuir en un 30% el subdiagnóstico de tumores "de intervalo", mejorando la detección de casos que podrían ser pasados por alto por el ojo humano.

En México, la desconfianza del personal médico hacia la IA, debido a su fiabilidad y falta de formación, limita su implementación. Pilloni Choreño sugiere formar alianzas entre universidades, empresas y el gobierno para demostrar la fiabilidad, seguridad y eficiencia de la IA.

Notas de TI					
Título:	El “superciclo de la Inteligencia Artificial”, el uso continuo de pantallas, el bienestar y la sostenibilidad: ¿cómo están cambiando las oficinas?				
Encabezado:	Claves para entender cómo y por qué están cambiando las oficinas en las que trabajamos				
Fecha:	09/06/25	Fuente:	RRHH DIGITAL	Por:	Redacción
Link:	<a href="https://www.rrhhdigital.com/secciones/actualidad/774464/el-superciclo-de-la-inteligencia-artificial-el-uso-continuo-de-pantallas-el-bienestar-y-la-sostenibilidad-como-estan-cambiando-las-oficinas/">https://www.rrhhdigital.com/secciones/actualidad/774464/el-superciclo-de-la-inteligencia-artificial-el-uso-continuo-de-pantallas-el-bienestar-y-la-sostenibilidad-como-estan-cambiando-las-oficinas/</a>				

El entorno laboral está evolucionando a gran velocidad, impulsado por cambios tecnológicos, sociales y culturales que redefinen la forma en que trabajamos. Steelcase, líder en consultoría estratégica de espacios de trabajo, ha identificado en su última investigación cuatro macro tendencias que están transformando el futuro del trabajo, y que marcarán el rumbo de las organizaciones más innovadoras para seguir siendo competitivas y atraer el mejor talento.

«Estas macro tendencias están redefiniendo la forma en que las personas trabajan, colaboran y se relacionan con su entorno laboral. En medio de tantos cambios, las organizaciones se están dando cuenta de la importancia de transformar sus espacios de trabajo para alcanzar sus objetivos. Para adaptarse, atraer talento y crecer deben dar respuesta a las nuevas necesidades de los trabajadores. En un entorno tan competitivo como el actual es necesario avanzar para no quedarse atrás.», afirma Teo Manzano, director de Marketing de Steelcase.

### 1.El superciclo de la Inteligencia Artificial

Según el Microsoft Work Trends Index, el 75% de los trabajadores ya utiliza IA para su trabajo diario, mientras que el 60% de los directivos teme que sus organizaciones carezcan de un plan para implementarla. Un cambio que está creando tanto oportunidades como desafíos para las empresas, que deben rediseñar sus espacios para apoyar esta transformación tecnológica.

Para ayudar a las empresas a adaptarse, Steelcase está desarrollando los AI-Ready Spaces, espacios especialmente diseñados para adaptarse a las necesidades del trabajo, tanto de forma individual como en equipo y con colaboradores remotos, optimizando la productividad y alineándose con los objetivos cambiantes de la organización. Al mismo tiempo, Steelcase está implementado su metodología Data-Driven Design, un enfoque de diseño de espacios de trabajo impulsado por inteligencia artificial. Este se basa en el análisis de datos de millones de aplicaciones reales para identificar necesidades y tendencias en la utilización de espacios, lo que permite construir de forma rápida diferentes escenarios que den respuesta a las nuevas necesidades de las organizaciones, en el menor tiempo posible. Este modelo permite a las organizaciones tomar decisiones más informadas y estratégicas, creando entornos flexibles, colaborativos y preparados para los desafíos de la era digital. De esta manera, los clientes pueden tomar mejores decisiones, garantizando que los diseños darán respuesta a las necesidades futuras.

## 2. La vida a través de una pantalla

En la última década, la forma de trabajar ha cambiado radicalmente y las videollamadas dominan la jornada laboral. Según la investigación del equipo de Steelcase WorkSpace Futures de, el 56% de las reuniones incluyen participantes en remoto, mientras que solo el 44% son totalmente presenciales. Las pantallas han reemplazado en gran parte las interacciones cara a cara y, según el informe, la mitad de los trabajadores prefieren asistir a estas reuniones desde sus propios escritorios por comodidad, rapidez o por no tener tiempo de desplazarse a una sala.

Sin embargo, el aumento del tiempo frente a pantallas ha traído efectos negativos como la falta de interacción humana, sobrecarga cognitiva y aislamiento social. Para mitigar estos efectos, es necesario rediseñar las oficinas con espacios colaborativos, sistemas eficientes de reserva de salas y entornos que equilibren privacidad y tecnología, fomentando así el bienestar y la productividad en ambos formatos: presencial y remoto.

Hoy es necesario que las salas de colaboración permitan la interacción personal, el acceso ecuánime a los dispositivos de videoconferencia, para tener la mejor experiencia con los participantes remotos y una buena orientación hacia la pantalla para poder compartir información de la forma más eficiente posible.

## 3. La urgencia del bienestar

La salud mental y el bienestar de los empleados han emergido como prioridades críticas para las organizaciones de todo el mundo. Según el último informe de Gallup, el 69% de los menores de 25 años declara no estar prosperando en su vida. Este dato cobra aún más relevancia al considerar que, para 2030, esta generación representará un tercio de la fuerza laboral mundial. La investigación de Steelcase revela que las personas han reordenado sus prioridades: el bienestar personal ha escalado al segundo lugar en las prioridades personales, solo por detrás de la familia, mientras que el trabajo ha caído al cuarto puesto.

La oficina capaz de extraer las mejores capacidades de las nuevas generaciones debe ser un entorno cuidado, con equilibrio y que fomente el sentido de pertenencia. Steelcase ayuda a las organizaciones a transformar sus espacios de trabajo para que reduzcan el estrés, favorezcan la salud mental y fomenten vínculos humanos significativos, mejorando así el bienestar físico, cognitivo y emocional.

## 4. Una mentalidad sostenible

En un contexto global en el que la sostenibilidad se ha convertido en un factor decisivo, cada vez más empresas están adoptando objetivos concretos para reducir su impacto ambiental, integrando principios sostenibles en el diseño y la gestión de sus oficinas. Steelcase, líder en consultoría estratégica de espacios de trabajo, destaca en su última investigación que considerar el impacto en cada elemento del entorno laboral, desde el diseño y la construcción hasta la selección de materiales y la incorporación de tecnologías eficientes, es fundamental para disminuir la huella de carbono.

Esta nueva macrotendencia no solo impulsa la optimización de recursos, sino que también genera importantes oportunidades de crecimiento, ya que fomenta la creación de nuevos puestos de trabajo y requiere la adquisición de nuevas competencias que complementan los perfiles

tradicionales. Según la iniciativa Science Based Targets (SBTi), el número de organizaciones que establecen metas científicas para reducir sus emisiones de carbono ha aumentado un 102% en el último año, representando casi el 40% de la economía mundial. Este avance refleja un compromiso colectivo por enfrentar la crisis climática y garantizar un futuro más sostenible.

En su investigación, Steelcase estima que los empleos “green collar” superarán los 300 millones en 2050. De hecho, según LinkedIn, el puesto de responsable de sostenibilidad es uno de los de mayor crecimiento en España, Reino Unido y Alemania. Estos datos reflejan cómo la sostenibilidad no solo transforma las estrategias empresariales, sino también las habilidades clave para el éxito.

Una invitación a rediseñar la oficina

El diseño de los espacios de trabajo es una poderosa herramienta de transformación organizacional. Comprender y anticipar estas tendencias clave es esencial para crear entornos donde las personas no solo trabajen mejor, sino que también se sientan mejor.

Notas de TI					
Título:	Inteligencia artificial: cómo educar para los retos del futuro				
Encabezado:	Cualquier tecnología que llegue al ámbito educativo se despliega inexorablemente sobre las desigualdades que el propio sistema genera, aumentándolas. Si lo que se produce es una revolución tecnológica, como por ejemplo la IA (Inteligencia artificial) o la Realidad Aumentada (RA) y la Realidad Virtual (RV), también el abismo de la desigualdad crecerá exponencialmente.				
Fecha:	09/06/25	Fuente:	ALKIMIA	Por:	Rafael Fenoy Rico
Link:	<a href="https://www.elsaltodiario.com/alkimia/inteligencia-artificial-educar-retos-del-futuro">https://www.elsaltodiario.com/alkimia/inteligencia-artificial-educar-retos-del-futuro</a>				

El título parece sugestivo aunque en cualquier caso la llamada Inteligencia artificial no sólo ha llegado, sino que se expande de manera exponencial. Un ejemplo de la velocidad con que el fenómeno se desarrolla puede obtenerse de un programa que rueda “aún” por internet después de 5 años con apariencia de “novedad”. Cientos de programas similares se pueden encontrar en las redes. Este en particular es una entrevista a Alex Beard, educador y escritor, dentro de una serie de programas patrocinados por un Banco, bajo el lema “Aprendemos juntos 2030”. Cuando este texto se escribe ha obtenido a lo largo de este lustro, 251.000 visualizaciones. –Oiga, en esto de la tecnología, 5 años es mucho–. Sin duda a la velocidad con que las ramas de la llamada IA avanzan, 5 años podría ser casi un siglo. Visualizar y analizar todos los vídeos que recogen entrevistas, debates, conferencias, documentales sobre la llamada IA se antoja imposible.

Desde hace varios años, muchos, se viene afirmando la necesidad de un cambio radical en el modelo educativo actual. Los procesos productivos que alientan, animan e invierten en la evolución de las tecnologías de todo tipo, han estado en constante y frenética evolución. Parece que sobre educación casi todo el mundo puede hablar, pensar, reflexionar, opinar... Y parecería que, como casi toda la población ha sido usuaria del sistema escolar, la experiencia vivida faculta para ello. No obstante de los sectores de las comunidades educativas sólo el de los trabajadores y trabajadoras de la educación -docentes y no docentes- permanecen en el tiempo. Padres, Madres, Alumnado, incluso políticos, están un tiempo, pasan y desaparecen. Por ello es preciso contar con la cualificada visión que la experiencia laboral en la educación aporta. Dos aspectos esenciales para comprender la esquizofrenia que padece el sistema educativo: a) La contradicción permanente entre las

administraciones públicas encargadas del “discurso” y las que detentan los “recursos”, b) Las propuestas idealistas y la realidad material.

Quienes tienen algunos años de docencia, o experiencia no docente, en las instituciones educativas recordarán que cualquier llegada de nuevas tecnologías promovía el surgimiento de profetas. Anunciaban cómo cada nueva innovación tecnológica debía conllevar una transformación de la educación. Avanzaban propuestas, retos, para que quienes definían las políticas educativas dieran con la tecla de producir el “cambio” necesario. La Asamblea General de las Naciones Unidas designó 1970 como el Año Internacional de la Educación para promover la colaboración y el desarrollo en el ámbito educativo. Ya ha llovido ¿podría afirmarse que se han producido cambios esenciales en los sistemas escolares? El 6 de mayo de 2025, por ejemplo, publicaba la fundación sociedad y educación una monografía titulada: Geografía del abandono escolar temprano en España. El absentismo escolar sigue siendo un caballo de batalla desde que se impuso la escolarización obligatoria. Basta recordar que en la lucha contra el analfabetismo la Junta de Andalucía en 1980, promovía aun un programa de este tipo denominado PASO A PASO. La conclusión de esta geografía del abandono escolar es idéntica a las cientos de formuladas años atrás: “Con la segunda tasa de abandono escolar más alta de la UE, España se enfrenta a un reto que exige, en palabras de los investigadores: “Adaptar las medidas a las características de cada territorio y trabajar para que la continuidad educativa no dependa del lugar de residencia ni del origen social o nacional, del alumnado”:

[https://www.SociedadYeducacion.org/noticias/nueva-monografia-geografia-del-abandono-](https://www.SociedadYeducacion.org/noticias/nueva-monografia-geografia-del-abandono-escolar-temprano-en-espana/)

[escolar-temprano-en-espana/](https://www.SociedadYeducacion.org/noticias/nueva-monografia-geografia-del-abandono-escolar-temprano-en-espana/). ¿Qué supondría, desde una concepción materialista, este “Adaptar las medidas a las características de cada territorio y trabajar para que la continuidad educativa no dependa del lugar de residencia ni del origen social o nacional del alumnado”? Es más que evidente la inexistencia de la aplicación del principio de igualdad de oportunidades. Por cierto, abandonado totalmente de la literatura administrativa. ¿Cómo conseguir que la continuidad educativa no dependa del lugar de residencia ni del origen social o nacional del alumnado? Podría pensarse desde un idealismo “comprometido” que basta dotar de sistemas de becas para permitir que “quien quiera, pueda”. Incluso becado el alumnado no parece sintonizar con las propuestas del sistema educativo. ¿Alguna propuesta para convertir la apatía, en interés? Posiblemente en la esfera material la realidad socio-económica-política se resiste a ser cambiada, sobre todo cuando las políticas estatales se abandonan a la deriva de la economía de mercado. Por ello cualquier tecnología que llegue al ámbito educativo se despliega inexorablemente sobre las desigualdades que el propio sistema genera, aumentándolas. Si lo que se produce es una revolución tecnológica, como por ejemplo la IA (Inteligencia artificial) o la Realidad Aumentada (RA) y la Realidad Virtual (RV), también el abismo de la desigualdad crecerá exponencialmente.

Es más que evidente la inexistencia de la aplicación del principio de igualdad de oportunidades. Didáctica General información sobre la presentación del VIDEO -como tecnología- en un congreso europeo y un prometedor futuro de aplicaciones en la Educación. Por primera vez se presentó el VIDEO, como instrumento pedagógico de indudable relevancia. El entusiasta profesor contaba y no paraba las bondades de este “definitivo” recurso didáctico que permitiría hacer posible el lema: “todo al alcance de todos”. Enseñar todo a todos para reformar la condición humana, la gran aspiración de Juan Amos Comenio, teólogo, filósofo y pedagogo nacido en la actual República Checa en 1592 y que publicó en 1657 su obra “Didáctica Magna”. Pretendía Comenio la democratización (llegar a todos) de la educación, donde todos los niños tengan la oportunidad de desarrollarse plenamente y contribuir positivamente a la sociedad. Sin embargo abstraerse de las condiciones materiales que sustentan la vida humana no permiten contemplar las consecuencias casi

determinantes en las formas de pensamiento. Y cuando se analiza la IA, como cualquier otra innovadora tecnología, con la educación, se hace abstracción de esas condiciones materiales. Una forma de enfocar este polémico aspecto es definir al menos los objetivos de lo que se denomina educación. Y cómo dependiendo del fin último que se persiga se podrán definir un conjunto de objetivos. En los textos académicos de Ciencias de la Educación es clásico el uso de la raíz latina de la palabra Educación: Educare y Educere. Educare se relaciona con “meter” “añadir”, informar, adoctrinar, aleccionar... Educere es otra cosa. Es “sacar”, “desarrollar lo que se tiene”, “hacer emerger” para de esta forma se despliegue las potencialidades que todo ser humano sin duda atesora.

Esa visión invocadora de la educación no está presente en la actual organización escolar que aún se resiente del enfoque cuartelario. Y cuando, ya tarde, la IA aparezca en ese escenario escolar, el abismo entre las clases sociales ya se habrá profundizado, más aún por la potencia de la tecnología. Por mucho que se enarbole la bandera de la Igualdad de Oportunidades todo quedará, como hasta ahora, en la constatación de que el sistema educativo está diseñado para justificar el seleccionar a las gentes y encuadrarlas en clases sociales subordinadas unas a otras. Ya hay cursos a miles sobre IA, ya hay escuelas adineradas que modifican sus currículum utilizando sistemáticamente en sus planes de estudio las herramientas de IA. ¿Cuándo se transformará en profundidad el sistema educativo para hacer posible, con cualquier tecnología, la real igualdad de oportunidades?