Notas de CANIETI					
Título:	Ley de Telecomunicaciones favorece sólo al Estado, advierte Canieti				
Encabezado:	El uso de recursos públicos para ofrecer diferentes servicios pone en desventaja a pequeños participantes del sector privado, según Canieti				
Fecha:	26/05/25	Fuente:	OEM	Por:	Rubén Romero
Link:	https://oem.com.mx/elsoldemexico/finanzas/ley-de-telecom-favorece-solo-al-estado-23764637				

La propuesta de reforma en la Ley de Telecomunicaciones y Radiodifusión pone en riesgo la competencia en el sector y abre la puerta a que el propio Estado se convierta en un competidor con ventajas, afirmó Alfredo Pacheco Vásquez, director nacional de la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (Canieti).

“Esta iniciativa trastoca principios constitucionales al permitir que el gobierno entre a competir en el mercado minorista, con beneficios que ningún privado podría obtener. Se trata de una distorsión completa del modelo de competencia”, indicó en entrevista con El Sol de México.

Explicó que uno de los puntos más preocupantes es que se permitiría al gobierno operar servicios de telecomunicaciones comerciales, ya sea directamente o mediante asociaciones público-privadas, con el uso de recursos públicos, lo cual pondría a los competidores privados en desventaja desde el inicio.

Además, la iniciativa plantea entregar espectro radioeléctrico, recurso clave para ofrecer servicio móvil e internet, sin necesidad de licitación pública y sin pagar contraprestaciones, pero solo a dependencias del gobierno.

Según Canieti, esto violaría el principio de neutralidad en la competencia establecido en la Constitución y en tratados internacionales como el T-MEC.

Otro elemento que genera inquietud es que las entidades gubernamentales quedarían exentas de muchas de las obligaciones regulatorias que sí aplican a los operadores privados.

“No puede haber un doble estándar en el cumplimiento de reglas. Si se abre la puerta a que el Estado participe en el mercado, debe hacerlo bajo las mismas condiciones”, insistió Pacheco.

De hecho, aunque la reforma constitucional reciente permite al gobierno brindar acceso a internet como una actividad estratégica, Canieti aclara que esto no lo exime de respetar la competencia.

“Promover el acceso no es sinónimo de destruir el mercado”, añadió.

Un análisis de The Competitive Intelligence Unit (The CIU) coincide con el diagnóstico de Canieti, ya que la reforma, tal como está planteada, provocaría pérdidas por más de 76 mil millones de pesos al año, al frenar la inversión, encarecer los servicios y reducir la competencia.

El reporte advierte que desaparecer al Instituto Federal de Telecomunicaciones (IFT) para sustituirlo por una agencia bajo control del Ejecutivo acabaría con la autonomía técnica y regulatoria que ha sido clave para el desarrollo del sector.

“La reforma provocaría pérdidas por más de 76 mil millones de pesos al año, al frenar la inversión, encarecer los servicios y reducir la competencia”

Estiman que solo este cambio restaría 0.5 por ciento de productividad al año, con pérdidas por 2.8 mil millones de pesos anuales.

Además, señalan que la posible relajación de la regulación sobre América Móvil podría revertir años de avances en precios y competencia. Desde 2013, los servicios móviles han bajado 49 por ciento, pero la eliminación de restricciones permitiría que el mercado vuelva a concentrarse.

Otros puntos críticos incluyen el riesgo de censura a contenidos digitales, una caída de 10 por ciento en el mercado publicitario en línea, costos excesivos por soterramiento de infraestructura y nuevos impuestos a dispositivos como celulares y routers.

“El sector enfrenta ya una tormenta perfecta: inversión débil, presión por cobertura y riesgos externos. Lo último que necesitamos es un cambio legal que ahuyente a quienes apuestan por México”, advirtió The CIU.

Pacheco reiteró que Canieti no está en contra de que el Estado participe, pero debe hacerlo respetando las reglas del juego.

“Queremos más cobertura, más servicios y mejores precios. Pero eso se logra con competencia real, no con un gobierno que compite desde arriba y con ventaja”, concluyó.

Notas de Electrónica					
Título:	En seis meses, centro de diseño de semiconductores en Jalisco				
Encabezado:	Claudia Sheinbaum, ya ha aprobado la propuesta de Jalisco para la construcción del Centro de Diseño de Semiconductores "Kutsari" (en purépecha, 'arena'), aseguró Pablo Lemus				
Fecha:	25/05/25 (por la tarde)	Fuente:	INFORMADOR	Por:	Rubí Bobadilla
Link:	https://www.informador.mx/jalisco/En-seis-meses-centro-de-diseno-de-semiconductores-en-Jalisco-20250525-0084.html				

Este domingo el gobernador de Jalisco, Pablo Lemus Navarro, dio a conocer que la Presidenta de México, Claudia Sheinbaum, ya ha aprobado la propuesta de Jalisco para la construcción del Centro de Diseño de Semiconductores "Kutsari" (en purépecha, 'arena') que se impulsa en la entidad, y se prevé que este quede listo en un plazo de seis meses.

"Ya me lo aprobó, y esto es bien importante. Ya me aprobó la Presidenta, ahora, el centro de diseño de semiconductores, que tiene la estrategia principal del diseño y desarrollo de patentes. Lo más probable es que éste se vaya a hacer en un edificio que tiene CONACYT, que está en Periférico y avenida Valle Real. Ahí se va a hacer el centro de diseño de semiconductores", indicó Lemus Navarro

a medios de comunicación al concluir el evento de arranque de la estrategia federal de "Salud Casa por Casa".

Dijo que para el desarrollo de este centro se pretende una inversión de 150 millones de pesos y se espera que pueda estar listo "en alrededor de seis meses más".

"La Presidenta está encantada. La Presidenta está, pero muy, muy contenta y comprometida con el proyecto del centro de diseño de semiconductores", añadió el gobernador de Jalisco.

De hecho, durante su intervención en el arranque de esta estrategia, que se llevó a cabo en el Almacén del IMSS en Tlaquepaque, la Presidenta destacó el trabajo conjunto que se tiene con la entidad en temas como la seguridad, pero también en la inversión privada, rubro en el cual, refirió, "Jalisco se está volviendo el principal receptor de la inversión en semiconductores, de alta relevancia para México y para todo el mundo".

En este sentido, recordó que para el desarrollo de esta materia "se pusieron aquí a los mejores investigadores de México, del Politécnico, del CINVESTAV, de instituciones de Jalisco, de Puebla, de Sonora, el Tecnológico Nacional de México, juntos al diseño de semiconductores, para que también sea la inteligencia y el desarrollo científico de nuestro país, lo que produzca no sólo para México, sino para todo el mundo. Y ese es el gran proyecto de desarrollo nacional", expresó Sheinbaum Pardo durante el evento.

Se trata del grupo de científicos cuya misión "es consolidar las capacidades de desarrollo de dispositivos basados en semiconductores en México", y que fue anunciado en febrero pasado por Sheinbaum Pardo en su rueda de prensa mañanera.

Este centro apostará por la viabilidad comercial inmediata y, a mediano plazo, un centro de fabricación con una visión estratégica, además de que se buscará proponer un nuevo marco legal y normativo "para fortalecer la maduración y transferencia de tecnología en el tema.

Para Lemus Navarro, el impulso de este centro de diseño será clave para Jalisco, especialmente considerando que siete de cada 10 semiconductores que se fabrican en el país, se producen en la entidad.

Lemus impulsa chips y agro ante Sheinbaum Pardo

En su intervención durante el arranque en Jalisco de "Salud Casa por Casa", Lemus Navarro aprovechó para destacar a la entidad como "un Estado productivo gracias a sus sectores estratégicos", en los que por supuesto nombró al área de los semiconductores.

"Usted nos ha apoyado para tener el primer centro de diseño de semiconductores a nivel nacional que yo espero, pronto le podamos presentar. Los semiconductores, para quienes no están muy enterados, son muchos chips que se ponen en una tableta y sirven para hacer teléfonos celulares computadoras, automóviles eléctricos y Jalisco tiene el 70% del mercado de los semiconductores a nivel nacional", refirió el mandatario estatal.

Recordó que ya hay varias empresas que han mostrado su interés de establecerse en Jalisco, entre ellas Foxconn y Nvidia, que tendrán dos plantas nuevas en la entidad.

Por otra parte, mencionó también al sector Agroalimentario, donde Jalisco es líder nacional, considerando que 17.8% de los alimentos que consumen las y los mexicanos, se producen en Jalisco.

"Entonces Jalisco va a ser muy importante, en producción de maíz, de leche, de huevo y de muchos otros sectores que son fundamentales. Sobre todo, para la seguridad alimentaria y autonomía de nuestro país", destacó el mandatario estatal.

Por último, Lemus Navarro aprovechó para felicitar las negociaciones que ha impulsado Claudia Sheinbaum con su homólogo en Estados Unidos, Donald Trump, para evitar afectaciones económicas a las remesas, donde Jalisco es la segunda Entidad de todo el País en recibir este tipo de transferencias.

"Esos mexicanos. Esos jaliscienses, en nuestro caso, trabajan muchísimo, y lo hacen de una manera honorable, de una manera que verdaderamente es ejemplar en los Estados Unidos. Ellos pagan sus impuestos y no se vale que ahora les quieran poner un doble impuesto por su trabajo. Usted Presidenta, lo ha defendido muy bien y quiero decirle algo, cuente con las y los jaliscienses, para defender también a nuestros paisanos que viven en los Estados Unidos y que merecen respeto a su trabajo", finalizó el mandatario estatal.

Notas de Electrónica					
Título:	Oferta CETis 18 las carreras técnicas de Semiconductores y Mecánica Industrial				
Encabezado:	Los egresados tendrán la capacidad de diseñar microchips, así como piezas estructurales				
Fecha:	25/05/25 (por la tarde)	Fuente:	OEM	Por:	Alejandro Domínguez del Hoyo
Link:	https://oem.com.mx/lavozdelafrontera/local/oferta-cetis-18-las-carreras-tecnicas-de-semiconductores-y-mecanica-industrial-23760339				

Para cumplir con lo establecido por la presidenta Claudia Sheinbaum Pardo, en el sentido de fortalecer las áreas tecnológicas en la educación, el próximo ciclo escolar, el Centro de Estudios Tecnológicos, Industrial y de Servicios (CETis) número 18, ofrecerá las carreras de Semiconductores y Mecánica Industrial.

Lo anterior lo informó Luz Alicia Suárez, encargada de despacho de la dirección del CETis 18 que señala que estas carreras las oferta la Dirección General de Educación Tecnológica e Industrial (DGETi), en esta nueva dinámica de renovar las carretas en los CETis y CBTis, como es semiconductores, inteligencia artificial, movilidad, entre otras.

Evelyn Delgado Law, encargada del Departamento de Vinculación del CETis 18, explicó que en lo referente a la carrera de Técnico Profesional en Semiconductores y Microelectrónica, trata de llevar la electrónica a su mínima dimensión, y sus egresados son los asistentes de los ingenieros, que requieren de técnicos especializados.

“Todo lo que sea para brindarnos comodidad y soporte en la actualidad, cada vez disminuyen más sus tamaños para mayor comodidad de nosotros, entonces, de eso se trata la carrera.

“Entonces el técnico en electrónica se encarga de diseñar esos dispositivos en micro, en pequeñito, hacer el diseño, hacerlos funcionar, y arreglarlos una vez que ya están funcionando y presentan una falla”.

Delgado Law expuso que los jóvenes trabajarán con maquinaria especializada para el diseño de los semiconductores o microchips, que es lo que trabaja la empresa Skyworks.

En lo referente a la carrera de Técnico en Mecánica Industrial, dijo, esta se encuentra enfocada al maquinado de piezas metálicas, de ahí salen las estructuras para diversas empresas.

“En Mecánica Industrial manejan maquinado a través de CNC´s (fresadoras, tornos, soldadura por electrodos) y también se encargan de las piezas que se van a maquinar”.

En el CETis 18 se ofertan otras carreras como Enfermería que en este caso dura 4 años, ya que son los 3 años de bachillerato y el cuarto año, van a pasantías a hospitales, escuelas y empresas a prestar sus servicios los 3 años anteriores, expuso Delgado Law.

También ofrecen carreras tradicionales como Contabilidad, Soporte y Mantenimiento de Equipo de Cómputo, señaló la docente.

Notas de Electrónica					
Título:	El chip específico para China que proyecta Nvidia señala un cambio en la dinámica de la competencia en semiconductores				
Encabezado:					
Fecha:	26/05/25	Fuente:	SPANISH PEOPLE DAILY	Por:	
Link:	http://spanish.peopledaily.com.cn/n3/2025/0526/c92121-20319810.html				

Nvidia parece estar lista para desvelar otro chip diseñado explícitamente para el mercado chino. De acuerdo a reportajes aparecidos en los medios de comunicación, la prestigiosa empresa proyecta presentar en breve un chip específico para China que esté basado en su última arquitectura Blackwell. Los observadores vaticinan que esta grata noticia se podría materializar en junio de este año.

El chip dedicado podría costar la mitad del H20, un modelo anterior.

De concretarse, sería la tercera vez que Nvidia ajusta drásticamente su estrategia de producción para cumplir con los controles de exportación de EE.UU., lo que resalta las cambiantes dinámicas en la competencia de semiconductores entre China y EE.UU.

Desde 2022, cuando el gobierno de EE. UU. implementó nuevas regulaciones que restringen a Nvidia la exportación de sus chips más potentes a China, culminando tres años después en los repetidos lanzamientos de productos en cumplimiento cada vez más degradados por parte de Nvidia, la relación ofensiva-defensiva en la competencia tecnológica entre EE. UU. y China ha evolucionado más allá de una simple contención y recuperación hacia una lucha compleja y dinámica.

Inicialmente, EE. UU. utilizó sanciones como arma, aprovechando su dominio en procesos de fabricación avanzada, tecnología de memoria y herramientas de automatización de diseño electrónico (EDA) para cortar el camino de avance de los semiconductores de China y mantener una brecha tecnológica.

Las primeras oleadas de restricciones a la exportación resultaron efectivas. Cortaron el suministro de chips a Huawei y obligaron a las empresas chinas de inteligencia artificial (IA) a reestructurar su infraestructura informática. Algunas startups de IA se vieron obligadas a cambiar de rumbo debido a su incapacidad para acceder a chips de alta gama. En aquel entonces, Nvidia tenía un control casi monopolístico sobre el mercado de IA en China debido a su ecosistema CUDA globalmente dominante y la tecnología de computación GPU.

Sin embargo, las dinámicas competitivas cambiaron rápidamente. A pesar de las enormes presiones en la cadena de suministro, China implementó políticas de apoyo para la industria de semiconductores mientras aumentaba sustancialmente la financiación para promover alternativas nacionales en toda la cadena de la industria. El gigante asiático trazó rápido sus caminos tecnológicos, desde equipos importados y chips de memoria hasta la fabricación de servidores, marcos de IA de código abierto y la integración especializada.

Lo más revelador es que las restricciones de exportación de chips del Departamento de Comercio de EE. UU. se han vuelto cada vez más estrictas, con detalles en su política que se vuelven cada vez más precisos hasta un punto decimal. Esto evidencia la búsqueda tecnológica reactiva y el estrechamiento de las brechas debido al acelerado ritmo de actualización industrial de China.

El espacio operativo de Nvidia se ha contraído severamente. Los chips que una vez fueron considerados como "reyes" han sido repetidamente degradados en ancho de banda y umbrales de computación, reducidos a soluciones de compromiso que apenas cumplen con las líneas rojas de Estados Unidos. Estos chips degradados no pueden proporcionar a los usuarios experiencias genuinas de computación de alto rendimiento mientras compiten directamente con alternativas nacionales en avance, como los chips Ascend 910B de China. En este sentido, Nvidia se ha convertido gradualmente en una víctima de la política de contención de Estados Unidos hacia China.

Jensen Huang, de Nvidia, afirma que China es una oportunidad de 50 mil millones de dólares para su empresa. Sin embargo, las restricciones de Estados Unidos los han mantenido frenados hasta el punto en que el CEO de Nvidia ha revelado que podrían ser reemplazados, ya que la cuota de mercado ha caído al 50 por ciento.

El núcleo de la competencia entre China y Estados Unidos ha alcanzado un punto de inflexión crítico. Inicialmente, Estados Unidos aprovechó sus ventajas tecnológicas para restringir sistemáticamente la trayectoria de mejora de China, mientras China soportó la presión y resistió los impactos. A través de un avance sincronizado en políticas, capital y tecnología, China ha superado el techo del bloqueo dirigido, buscando activamente el vuelco mediante innovaciones.

Estados Unidos continúa intentando suprimir el logro de ventajas de la escala china a través de medidas más frecuentes y detalladas: nuevas rondas de restricciones en las fundiciones de TSMC, aprobaciones de exportación de memoria avanzada y parches de herramientas de EDA. Todo ello con el objetivo de preservar ventajas temporales.

Esta estrategia probablemente persistirá a corto plazo, aunque cada vez será más difícil para Estados Unidos mantener su desfase de prioridad tecnológica debido a lo más importante del hecho: las reglas han cambiado.

Notas de Electrónica					
Título:	Samsung quiere cambiar el silicio por cristal en sus procesadores, y dicen que es mejor				
Encabezado:					
Fecha:	26/05/25	Fuente:	HARD ZONE	Por:	
Link:	https://hardzone.es/noticias/procesadores/samsung-procesadores-silicio-cristal/#:~:text=Este%20nuevo%20modelo%20se%20llamar%C3%A1,ofrece%20una%20potencia%20extremadamente%20grande.				

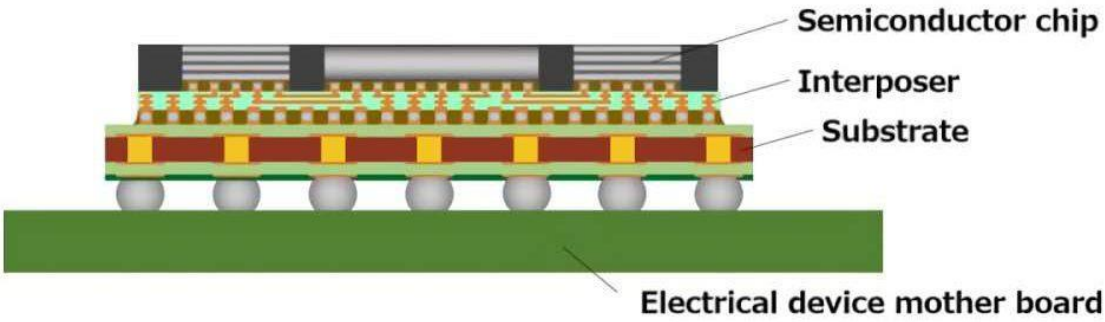
Uno de los mayores problemas que tienen actualmente las compañías a la hora de crear semiconductores está en las limitaciones que tiene el silicio, si bien es cierto que todavía resulta posible continuar utilizando este material para desarrollar componentes de última generación, hay algunos materiales que se pueden utilizar en el empaquetado de chips para mejorar y otros tipos de hardware con muchas más ventajas que el propio silicio.

Samsung es una de las pocas compañías en todo el mundo que cuenta con grandes plantas de fabricación de semiconductores, crean una gran cantidad de chips y son capaces de desarrollar su propio proceso litográfico lo que les permite tener una cadena de producción propia de inicio a fin. Si a esto le sumamos algunas de las novedades que quieren traer en los próximos años podemos ver que los planes de la marca pueden resultar extremadamente buenos tanto para sus beneficios como para una evolución en los componentes actuales, y uno de los primeros pasos es adoptar el sustrato de vidrio para el empaquetado de chips.

La revolución que quiere implementar Samsung, chips con mayor rendimiento, fáciles de fabricar y menor precio

Hay varias compañías que están trabajando actualmente en una solución para lograr que los componentes de hardware puedan llegar a tener una evolución, desde hace años se siguen utilizando los mismos materiales para crearlos y el mayor problema que ofrecen está en las limitaciones de cada uno de ellos. Aunque para ver esta innovación tendremos que esperar mínimo hasta 2028, Samsung ya tiene planes de poner patas arriba la industria del hardware gracias a un nuevo proceso de empaquetado de chips que cambia los interposers de silicio por unos creados a partir de vidrio que, según indican, ofrecen un rendimiento superior mientras que abaratan los costes y tienen un ciclo de producción mucho más corto.

Los interposers son un tipo de componente clave en el empaquetado de chips, al final permiten conectar dos de las piezas dentro del hardware entre sí, por ejemplo en los aceleradores de IA donde la GPU está rodeada de memorias con un gran ancho de banda o HBM. El silicio es un material que resulta bastante eficaz pero que, por el proceso de fabricación que implica crear los interposers, son mucho más caros de utilizar. Además de esto también tienen una precisión muy inferior en los circuitos ultra finos y presentan una menor estabilidad dimensional frente a la nueva solución de Samsung basada en sustrato de vidrio.



Actualmente hay varias compañías que están comenzando a utilizar este material por las ventajas que ofrece, pero la diferencia está en el acercamiento que está teniendo Samsung ya que en lugar de utilizar paneles con un tamaño de 510×515 mm para desarrollar los prototipos han comenzado con dimensiones bastante más pequeñas de menos de 100×100 mm, esto les permitiría acelerar la creación para entrar más rápido al mercado, pero podría reducir la eficiencia del empaquetado.

Todas estas innovaciones llegan por una industria en auge como es la IA, al final los diseños se centran mucho en los aceleradores creados para esta tecnología y, aunque esta técnica probablemente se puede aplicar a otros componentes, es muy probable que cuando llegue tan solo veamos su implementación en hardware que tenga este propósito.

Notas de Telecomunicaciones					
Título:	Necesario regreso del Estado en las telecomunicaciones				
Encabezado:					
Fecha:	26/05/25	Fuente:	JORNADA	Por:	Alonso Romero
Link:	https://www.jornada.com.mx/noticia/2025/05/26/opinion/necesario-regreso-del-estado-en-las-telecomunicaciones				

La Comisión de Radio y Televisión de la Cámara de Diputados puso a discusión en un foro de análisis, el uso de los datos biométricos y los riesgos para la privacidad, que prevé la ley de telecomunicaciones propuesta por la Presidenta de la República, y otros ordenamientos como la reforma en materia de simplificación de trámites gubernamentales.

Especialistas, académicos y representantes de organizaciones no gubernamentales coincidieron en alertar que el proyecto a discusión en el Senado de la República implica más riesgos que beneficios para los ciudadanos en lo referente a sus datos personales.

Sin garantías de resguardo a la información personal

Al abrir el encuentro, Francisco Rivas, director del Observatorio Nacional Ciudadano, advirtió que la norma planteada no da garantía de un debido uso y un adecuado resguardo de la información personal, incluyendo datos biométricos, de la ciudadanía.

Sentenció que en México la intromisión de la delincuencia organizada en las instituciones y su cada vez más amplia operación en el territorio nacional, provoca sucesos trágicos como el ocurrido con dos de los más cercanos colaboradores de la jefa de gobierno de la Ciudad de México.

Ante esas circunstancias, se generan dudas y preocupación sobre los riesgos de poner en manos de las autoridades infiltradas y vulneradas por el crimen, la información personal de toda la ciudadanía.

“Sabemos que la delincuencia organizada tiene una participación muy activa en nuestro país, que controla territorios, que controla autoridades, y si se pueden llevar a cabo magnicidios como el que vimos ayer, lamentable magnicidio que afecta profundamente nuestras instituciones, es precisamente porque hay una penetración de la delincuencia en las instituciones. ¿Queremos darle a las autoridades una libertad para acceder a nuestros datos biométricos, a nuestros datos e información sin que haya un contrapeso?, esa es una de nuestras principales preocupaciones”, planteó.

Pidió no olvidar que tanto la ley de telecomunicaciones como la reforma aprobada en materia de simplificación de trámites, dan a la Agencia de Transformación Digital del gobierno gran amplitud de facultades sin contrapeso, y crea un mecanismo de acceso a toda la información de toda la población, denominado Llave MX, que podría ser fácilmente vulnerado.

Vigilancia al ciudadano es inconstitucional

A su vez, María José de Icaza Banet, investigadora del Programa de Derechos Digitales de la organización Artículo 19 para México y Centroamérica, alertó que la propuesta de ley de telecomunicaciones implicaría que el Estado implemente herramientas para vigilar a la población.

Ello hace recordar los efectos que en su momento tuvo el uso por parte del gobierno, del sistema de espionaje Pegasus, que se utilizó contra periodistas, defensores de derechos humanos, opositores y otras personas críticas al régimen, dijo.

También, el hecho dado a conocer en el 2023, a través de la investigación periodística denominada “Ejército espía”, en la que a través de las filtraciones del caso Guacamaya Leaks, se conocieron informes donde los mandos militares identificaron a esos actores sociales como “enemigos potenciales” del gobierno.

El peligro con el proyecto a discusión, anotó, es que se pretende legalizar esa vigilancia gubernamental.

“Otorgar facultades para el acceso a nuestros datos y metadatos de telecomunicaciones a las autoridades competentes, implica que sin justificación, sin control judicial, sin controles claros, estas autoridades nos puedan vigilar como ya lo han hecho, pero ahora de forma legal”, recalcó.

En cuanto a la creación del padrón de usuarios de celulares, recordó que los dos intentos anteriores de aplicar esa medida, con los expresidentes Felipe Calderón y Andrés Manuel López obrador, fueron fallidos y la Suprema Corte los declaró inconstitucionales.

Ello, por violar la privacidad, limitar el derecho a la libertad de expresión, el derecho a la protesta y por resultar discriminatorios de personas vulnerables.

La ponente manifestó su tristeza ante la cerrazón de los congresistas a escuchar esas alertas y a no tomar en cuenta las experiencias previas al momento de plantear y aprobar leyes.

Tras reiterar que no hay evidencia para comprobar que la vigilancia a los ciudadanos a través de sus comunicaciones genere mejores condiciones de seguridad, la especialista señaló que el ejercicio de esas tareas a través de instancias como la Agencia Digital, que no estará sujeta a controles claros, no garantiza transparencia ni rendición de cuentas ni tendrá contrapeso en una supervisión independiente, es riesgoso para los derechos y las libertades.

La vigilancia señalada, remarcó, impacta negativamente en la libertad de expresión y de manifestación, y así lo han advertido instituciones como la ONU y la Comisión Interamericana de Derechos Humanos (CIDH), que han catalogado esas actividades como "medidas indirectas de censura".

Registro de usuarios de telefonía móvil

Subrayó que mecanismos como el registro de usuarios de telefonía celular es una copia de padrones anteriores que resultaron fallidos y catalogados por la Suprema Corte de Justicia de la Nación (SCJN) como inconstitucionales.

"El registro de usuarios del servicio móvil ayuda a resolver problemas de seguridad, no, no hay ningún indicador que así sea, al contrario, promueve los riesgos para los usuarios. Y la posible vulneración de los derechos humanos y de los datos personales no solo se desprende de la iniciativa de ley de telecomunicaciones, sino de las funciones que adquiere la Agencia de Transformación Digital", remarcó.

La investigadora del Centro de Investigación y Docencia Económicas, CIDE, Olivia Andrea Mendoza, indicó que en una sociedad hiperconectada quienes tienen los datos "tienen el poder", ello, al hablar de la "soberanía del dato".

Añadió que los mecanismos previos de censura, como los que se perfilan en la iniciativa presidencial, pueden traer consigo restricciones a la libertad de expresión.

Subrayó que en el contexto de la iniciativa presidencial, es necesario tomar con la seriedad necesaria el tema de los contrapesos que tendrá o no la Agencia Digital.

Salvaguarda a la información personal

Al intervenir, Ernesto Ibarra Sánchez, presidente Academia Mexicana de Ciberseguridad y Derecho Digital, AMCID, pidió a los legisladores valorar con cuidado qué se busca y cuáles podrían ser los efectos de permitir el acceso a los datos personales y biométricos a las agencias de investigación.

Si la medida se tomará, anotó, será necesario establecer las salvaguardas de protección de esa información conforme a los estándares internacionales.

Si hay evidencia con ejemplos y casos de otros países, de que esas acciones funcionan para mejorar la seguridad y el combate al delito, planteó, México puede hacerlo, pero con las restricciones,

controles y vigilancia permanente de expertos, sociedad civil y la academia, con el fin de evitar que autoridades se extralimiten.

Expresó que por el momento, es difícil decir que esas disposiciones resolverán el problema de la inseguridad, sin embargo, si se implementarán, debe haber detrás de la decisión un estudio y sustento con evidencias suficientes.

Asimismo, expresó que lo ideal sería que la sociedad participe en todo momento como observadora y vigilante.

Agencia Digital sin controles

En su participación, Anahiby Becerril Gil, consultora en ciberseguridad, derechos humanos y tecnologías emergentes, habló de la concentración de poder en la Agencia de Transformación Digital y las preocupaciones que eso genera.

Refirió que la iniciativa de ley, prevé la recolección, uso y almacenamiento masivo de datos personales y biométricos, que sin las salvaguardas necesarias y sin observar normas internacionales, abren la puerta a un uso que podría ser inadecuado.

Destacó que ante la inexistencia de un organismo autónomo regulador del sector, tras la extinción del Instituto Federal de Telecomunicaciones (IFT), la Agencia señalada que será un organismo sin autonomía, dependiente del Poder Ejecutivo, y la Secretaría de Infraestructura, Comunicaciones y Transportes que será el garante de los datos, pero ambos con subordinación ante de la Presidencia de la República, los ciudadanos no tendrán alternativa para demandar la protección de sus datos.

Como riesgos concretos de los cambios a discusión, identificó la normalización del “uso forzado” de la biometría para identificarse.

Al manifestarse a favor de no descalificar la captura de datos biométricos, enfatizó que lo relevante es centrar la atención en qué autoridades serán las encargadas de manejarlos.

Añadió que el uso de esa información por parte del Estado para combatir el delito, incluyendo el compartir datos entre instituciones, sin contar con una orden judicial y sin una base legal clara centrada en fundamentos de excepcionalidad, es lo que preocupa.

Recordó que la ONU ha lanzado alertas a nivel mundial, ante la decisión de distintos gobiernos de ejercer facultades de vigilancia masiva y que implican el uso de datos biométricos y personales de la población sin control, debe tener freno, porque tiene impacto negativo en materia de derechos humanos y representa un “alto potencial de abuso” por parte de la autoridad.

Consideró que la Agencia digital gubernamental debería estar sometida a controles, actuar en función de evaluaciones de impacto en materia de protección de datos personales y de derechos humanos.

Es necesario valorar a qué autoridades se les entregarán los datos de ciberseguridad, porque la instancia concentradora de la información sin autonomía, sin obligación de entregar informes periódicos sobe el uso de los archivos en su poder, sin estar sujeta a una auditoría externa y que no

tendrá de frente un organismo garante independiente, genera alerta por posibles riesgos para la privacidad y derechos de las personas.

Notas de Telecomunicaciones					
Título:	Plantean 500 cambios a Ley Telecom; se modificarían 83 artículos				
Encabezado:	Las preocupaciones de los participantes en el Conversatorio se centran en temas como censura, neutralidad de la red … pero de manera relevante todo lo relacionado con la ATD				
Fecha:	26/05/25	Fuente:	EXCELSIOR	Por:	Leticia Robles de la Rosa
Link:	https://www.excelsior.com.mx/nacional/plantean-500-cambios-a-ley-telecom/1717925				

Concluido el Conversatorio del Senado para los cambios que hará a la propuesta presidencial de Ley en Materia de Telecomunicaciones y Radiodifusión, los participantes plantearon al menos 500 modificaciones a 83 artículos, de los cuales cinco son transitorios; es decir, modificar el 26.5% del cuerpo normativo y el 30% del régimen transitorio.

En el universo de 500 propuestas hay al menos 204 que fueron presentadas como temas globales, como objetivos a alcanzar, pero sin especificar los artículos a modificar.

Con base en la información pública que tiene el portal del Senado para mostrar todo el proceso de la nueva ley, las preocupaciones de los participantes se centran en temas como censura, neutralidad de la red, cancelación de plataformas digitales, inclusión de personas con discapacidad, pero de manera relevante todo lo relacionado con la Agencia de Transformación Digital, que recibió críticas de 70% de los participantes, porque no la consideran una instancia autónoma y la identifican como un ente peligroso, porque una sola persona tendrá la concentración del poder.

REGISTRO DE TELEFONÍA MÓVIL

Otro de los temas que resalta en las preocupaciones de diversos participantes es todo lo relacionado con el registro de telefonía móvil, pues si bien su redacción es igual a la que existe en la ley actual, la eliminación del colegiado del Instituto Federal de Telecomunicaciones (IFT) y el retiro del requisito de una orden judicial para que se entregue esa información es considerada como de alto riesgo para la seguridad de los usuarios de la telefonía móvil.

Aunque públicamente, el artículo 109 de la propuesta de nueva ley fue el que más menciones tuvo en medio de comunicación y redes sociales, porque se refiere a la facultad discrecional de la Agencia de Transformación Digital de suspender una plataforma digital, en las propuestas entregadas por escrito a las comisiones unidas del Senado, los artículos tres y ocho suman el mayor número de menciones como indispensables de ser modificados.

El 103 se refiere al glosario, que significa las definiciones de los conceptos que se deberán entender en esta nueva ley. La mayoría de los ponentes planteó la necesidad de modificar los conceptos que tienen de temas como usuario, audiencia, radiodifusión comunitaria, indígena, social e independiente, entre otros.

Mientras en las exposiciones verbales públicas que pudieron escucharse en los cinco días de Conversatorio, fue evidente que 70% expresó su preocupación por las facultades de la Agencia de Transformación Digital, en las propuestas por escrito el artículo 108, que la define, es el segundo con el mayor número de menciones como urgente de ser modificado; sólo por debajo del tres.

El 108 se refiere a las 106 atribuciones de la Agencia, entre ellas "establecer programas de acceso a banda ancha en sitios públicos, en los que se identifique el número de sitios a conectar cada año de manera progresiva, hasta alcanzar la cobertura universal; alinear, fijar, instrumentar y conducir las políticas y programas de cobertura universal y cobertura social de conformidad con lo establecido en esta Ley; elaborar las políticas de telecomunicaciones y radiodifusión del gobierno federal"

También "emitir el programa nacional de espectro radioeléctrico que tendrá por objeto promover el aprovechamiento del espectro radioeléctrico, con el fin de brindar mayor cobertura y acceso a servicios de telecomunicaciones y radiodifusión para contribuir al bienestar de la población, en los términos que se fijen en los lineamientos que para tal efecto emita la Agencia".

Y "expedir los lineamientos para el reordenamiento, retiro o soterramiento de infraestructura de telecomunicaciones, a los que deberán sujetarse los concesionarios y, en su caso, autorizados y proveedores de infraestructura pasiva", entre otros.

Hay otro grupo de artículos, relacionados con la facultad de asignación directa de la Agencia, que también acapararon la atención de los participantes en el Conversatorio, como son el 56, el 57 y el 58, porque la mayoría o lo considera un camino al fracaso, porque se entregarán concesiones a dependencias del gobierno, o porque implican violaciones flagrantes al Tratado México, Estados Unidos y Canadá (TMEC).

El artículo 56 dice que "cuando una dependencia o entidad del Ejecutivo federal requiera una concesión única para uso comercial, con el fin de cumplir con los objetivos de cobertura social y universal del Estado mexicano.

(…) Para cumplir con los fines antes mencionados, el Ejecutivo federal podrá proveer el servicio de internet a usuarios finales, por sí o mediante asociación público- privada, en este último caso, siempre que el Estado mantenga en todo momento la dirección y control del proyecto.

Las funciones que el Estado ejerza en la provisión del servicio de internet no constituirán monopolios", dice.

El 57 agrega que "la Agencia, mediante asignación directa, podrá otorgar a una dependencia o entidad del Ejecutivo Federal la concesión para el uso, aprovechamiento y explotación del espectro radioeléctrico para uso comercial, con el fin de cumplir con los objetivos de cobertura social y universal del Estado mexicano".

Y el 58 "la Agencia fijará, de entre las previstas en la presente Ley, las obligaciones a las que la dependencia o entidad quedará sujeta en sus respectivos títulos de concesión única y para el uso, aprovechamiento y explotación del espectro radioeléctrico para uso comercial, las cuales en ningún caso podrán obstaculizar o limitar las facultades y objetivos de provisión de servicios que tengan como fin cumplir con los objetivos de cobertura social y universal del Estado mexicano. Las

obligaciones que no estén expresamente previstas en los respectivos títulos de concesión o en las disposiciones que emita la Agencia, no le serán exigibles".

Participantes como Javier Juárez, Adriana Labardini, Miguel Calderón Lelo de Larrea, Héctor Guillermo Bernal del Valle, Luis López, Erick Huerta y Javier Tamayo García y José Antonio García Herrera, esto coloca en una desventaja evidente al resto de los competidores.

NEUTRALIDAD DE LA RED

Otro tema que tiene el mayor número de menciones para que se modifique es la neutralidad de la red, que está en los artículos 107 y 108 de la iniciativa presidencial.

El 107 dice que "los concesionarios y autorizados que presten el servicio de acceso a Internet deberán sujetarse a los lineamientos de carácter general que al efecto expida la Agencia.

Dichos lineamientos serán emitidos conforme a principios de libre elección, no discriminación, privacidad, transparencia y derechos establecidos en la Constitución, en esta Ley. en las recomendaciones de organismos internacionales expertos en la materia, en los tratados y acuerdos internacionales suscritos por México, en lo que resulte aplicable", ordena.

Y el 108 establece que "los concesionarios y los autorizados deberán prestar el servicio de acceso a internet respetando la capacidad, velocidad y calidad contratada por el usuario, con independencia del contenido, origen, destino, terminal o aplicación, así como de los servicios que se provean a través de Internet, en cumplimiento de lo señalado en el artículo anterior".

Pero los expertos que participaron en el Conversatorio dejaron en claro que estos dos artículos quedan cortos respecto del concepto e incluso son un retroceso de lo que se tiene actualmente.

Otro grupo de artículos que tienen el mayor número de señalamientos para ser modificados son el 201, 202 y 210, que son percibidos por diferentes expertos como riesgos de censura previa para los concesionarios.

El 201 dice que "los concesionarios que presten servicios de radiodifusión o de televisión y audio restringidos, que transmitan contenidos que sean pagados, patrocinados o encargados por gobiernos extranjeros, organismos internacionales o personas físicas o morales de nacionalidad extranjera, ya sea en forma de anuncios, spots, patrocinios, transmisiones en vivo, cápsulas informativas o cualquier otro formato, deberán contar con previa autorización por escrito de la Secretaría de Gobernación.

Se entenderá por contenido radiodifundido de origen extranjero aquel que, total o parcialmente, provenga de cualquiera de los sujetos señalados en el párrafo anterior", establece.

El 202 ordena que "el concesionario que preste servicios de radiodifusión o televisión restringida deberá presentar a la Secretaría de Gobernación, con al menos quince días hábiles de anticipación, la solicitud de autorización, acompañada de identificación del sujeto extranjero responsable del contenido, muestra o sinopsis detallada del mensaje, fecha, horario y medios técnicos de transmisión y manifestación de que cumple con los límites al financiamiento extranjero y demás disposiciones aplicables.

La Secretaría de Gobernación resolverá dentro de los diez días hábiles siguientes a la recepción completa de la solicitud a la autorización será personal, intransferible y podrá sujetarse a condiciones específicas para garantizar el Interés público, la seguridad nacional y el respeto a los derechos humanos", plantea.

Y el 210 indica que "los concesionarios que presten el servicio de radiodifusión, televisión o audio restringidos en el país, no podrán transmitir propaganda política, ideológica, comercial o de cualquier tipo de gobiernos o entidades extranjeras, con excepción de la promoción turística o cultural.

Tampoco se permitirá que gobiernos extranjeros utilicen los medios de comunicación nacionales para influir en los asuntos internos del país.

Las plataformas digitales, cuyos contenidos estén disponibles en el territorio nacional, no podrán comercializar espacios publicitarios para la difusión de publicidad, propaganda o cualquier información de gobiernos extranjeros, distinta de aquella que tenga fines culturales o turísticos.

Queda prohibido a los programadores y operadores de señales, transmitir por sí o a través de concesionarios que presten servicios de radiodifusión o de televisión o audio restringidos publicidad, propaganda o cualquier información de gobiernos extranjeros, distinta de aquella que tenga fines culturales o turísticos", advierte.

Las comisiones unidas de Radio, Televisión y Cinematografía; de Comunicaciones y Transportes y de Estudios Legislativos sistematizarán todas las propuestas para discutir cuáles pueden ser incluidas como propuestas de modificación al dictamen que fue devuelto a comisiones.

Notas de Telecomunicaciones					
Título:	Abre Derecho espacio de reflexión sobre nueva ley de telecomunicaciones				
Encabezado:	Acudieron al foro académicos, especialistas, representantes sociales e industriales, directores de medios públicos y autoridades regulatorias				
Fecha:	26/05/25	Fuente:	GACETA UNAM	Por:	
Link:	https://www.gaceta.unam.mx/abre-derecho-espacio-de-reflexion-sobre-nueva-ley-de-telecomunicaciones/				

En un contexto de intenso debate nacional sobre la iniciativa de una nueva Ley Federal de Telecomunicaciones y Radiodifusión, la Facultad de Derecho (FD), a través del Seminario de Derecho Administrativo, organizó el foro "Telecomunicaciones, Radiodifusión y Competencia en México. Una coyuntura para el análisis y diálogo", con la participación de académicos, especialistas, representantes sociales e industriales, directores de medios públicos y autoridades regulatorias.

La inauguración corrió a cargo de la directora de la FD, Sonia Venegas Álvarez, quien destacó la apertura de la UNAM para abordar estos temas desde una visión académica.

Durante las mesas de discusión, se resaltó la necesidad de replantear el marco jurídico del sector con una visión incluyente, plural y respetuosa de los derechos humanos. Las telecomunicaciones fueron reconocidas como un derecho humano indispensable para el desarrollo democrático del país, pero se subrayó que persisten brechas estructurales en cobertura, calidad y acceso, así como

mercados muy concentrados, a pesar de los avances impulsados por la reforma constitucional de 2013 y la creación del Instituto Federal de Telecomunicaciones (IFT).

En la primera mesa, titulada “A 11 años de la preponderancia y una nueva Ley Federal de Competencia Económica. Panorama de usuarios y proveedores”, se abordó la evolución del concepto de “preponderancia” y los desafíos que aún enfrentan los usuarios ante prácticas anticompetitivas.

Rolando Guevara Martínez, de la Asociación Nacional de Abogados de Empresa, propuso repensar las herramientas jurídicas para sancionar abusos de mercado de los grandes operadores.

La académica Clara Luz Álvarez consideró que es necesario replantear los conceptos de poder sustancial de mercado y agentes económicos preponderantes para garantizar una competencia efectiva.

Por su parte, Antonio Celular Steffan, profesor de la FD, subrayó la necesidad de marcos regulatorios que hagan más accesible el servicio en regiones históricamente marginadas.

Finalmente, Gabriel Sosa Plata, especialista en derechos de las audiencias, hizo énfasis en que el nuevo diseño legal debe garantizar pluralidad mediática y la protección de las audiencias vulnerables en los nuevos entornos digitales.

El economista Ernesto Piedras, quien moderó la mesa, alertó que sin regulación efectiva, México corre el riesgo de acentuar las brechas digitales y sociales.

La segunda mesa, centrada en “El futuro de las telecomunicaciones en el marco de una nueva Ley Federal de Telecomunicaciones y Radiodifusión”, hizo hincapié en la necesidad de políticas públicas inclusivas y técnicamente sustentadas.

Erick Huerta Velázquez, coordinador adjunto de Redes por la Diversidad, la Equidad y Sustentabilidad, expresó su preocupación por las disposiciones que facilitarían la asignación directa de concesiones, lo que podría abrir la puerta a la concentración y a posibles privilegios discrecionales del Estado, que afectarían a pequeños operadores.

Marina Martínez Flores, presidenta del Consejo Directivo de Radio Independiente de México, planteó que la nueva ley debe garantizar condiciones equitativas para los medios comerciales, en particular la radio, frente al avance de plataformas digitales globales.

A su vez, el académico Ernesto Contreras Landaverde señaló que es imperativo preservar la autonomía de los órganos reguladores, evitar que el Estado sea al mismo tiempo regulador y operador, y garantizar la transparencia en los procesos.

El director de Artículo 19, Leopoldo Maldonado, enfatizó que la conectividad no debe ser un monopolio y criticó el modelo de superagencia por contravenir estándares internacionales alertando sobre la omnipotencia del Poder Ejecutivo y la recopilación de datos biométricos.

Moderada por Benjamín Tello, esta mesa propuso reforzar la protección de derechos, particularmente el derecho a la información y a la conectividad, con perspectiva territorial y de justicia social.

La tercera mesa, titulada “Medios públicos y comunitarios”, se convirtió en un espacio de defensa del carácter estratégico y social de estos medios.

Iván Trujillo Bolio, director de TV UNAM, destacó el papel del IFT en la asesoría técnica y jurídica que ha permitido el fortalecimiento de proyectos públicos, y subrayó que la compartición de infraestructura debe mantenerse como política clave.

John Ackerman, director del Programa Universitario de Estudios sobre Democracia, Justicia y Sociedad, afirmó que México necesita medios públicos fuertes y con mayor financiamiento para contrarrestar la desinformación que predomina en redes y medios comerciales.

La cuarta mesa trató de los “Retos para la digitalización y conectividad del país”.

Notas de Telecomunicaciones					
Título:	Tras conversatorios, advierte el PRI su rechazo a la reforma en telecomunicaciones				
Encabezado:					
Fecha:	26/05/25	Fuente:	ENFOQUE NOTICIAS	Por:	Gerardo Cedillo
Link:	https://enfoquenoticias.com.mx/nacional/tras-conversatorios-advierte-el-pri-su-rechazo-a-la-reforma-en-telecomunicaciones/				

México.- Luego de la conclusión de los cinco conversatorios que organizó el Senado sobre la iniciativa de reforma en materia de Telecomunicaciones y Radiodifusión, el grupo parlamentario del PRI advirtió que no respaldarán una ley que, a su juicio, legaliza la censura, vulnera derechos fundamentales y concentra el poder en una sola voz.

En un comunicado, el coordinador de los senadores del PRI, Manuel Añorve, aseguró que la propuesta representa una amenaza directa a derechos como la libertad de expresión, el acceso a la información y la privacidad de los ciudadanos.

El legislador de Guerrero, sostuvo que “Esta no es una reforma, es una embestida directa contra la libertad de expresión, el derecho a la información y la privacidad de millones de personas”.

Destacó que los especialistas participantes coincidieron en que la reforma debilita derechos humanos al reducirlos a recomendaciones sin valor legal.

A nombre del PRI también criticó la intención del dictamen de permitir la suspensión de señales y el bloqueo de plataformas digitales sin orden judicial, acción que calificó como inconstitucional.

Dijo que a esto se suma la creación de un padrón nacional para conservar datos personales de los usuarios durante 24 meses, sin garantías claras de protección legal, tras la desaparición del INAI.

Además, los priistas señalaron que la concentración de funciones en una sola agencia subordinada al Ejecutivo Federal elimina contrapesos democráticos y compromete la pluralidad.

Añorve señaló que otro punto que se ve con preocupación es la intención de diferenciar entre "opinión" e "información" en los contenidos, lo cual —según Añorve— podría usarse para sancionar a medios críticos, intimidar a periodistas y limitar la libertad de prensa.

"La libertad de expresión, la privacidad, el derecho a informarnos y a ser escuchados no son negociables. Así no. Nunca", sentenció Añorve, quien participó activamente en los cinco conversatorios.

Finalmente, el grupo parlamentario del PRI reiteró que la reforma no toma en cuenta la realidad digital actual ni contempla un enfoque de derechos adecuado para el entorno tecnológico contemporáneo.

Notas de Telecomunicaciones					
Título:	Piden para la ATDT un Consejo plural con opiniones vinculantes				
Encabezado:					
Fecha:	26/05/25	Fuente:	CONSUMOTIC	Por:	Juan Carlos Villarruel
Link:	https://consumotic.mx/telecom/piden-para-la-atdt-un-consejo-plural-y-decisiones-vinculantes/				

La apertura del Poder Ejecutivo para que en la Agencia de Transformación Digital y Telecomunicaciones (ATDT) opere un órgano colegiado representa cierta oportunidad para alcanzar el equilibrio, si se logra integrar de manera plural con personas que aporten puntos de vista complementarios a los del regulador.

Asimismo, es necesario que las opiniones de tal consejo sean vinculantes y por lo tanto que la persona titular de la agencia, deba atenderlas, porque "en el diseño original de la iniciativa (que da lugar a la creación de la ATDT) existía el zar de las telecomunicaciones" y el Estado fungiría como regulador y competidor.

Durante un encuentro virtual convocado por el coordinador de la Comisión de Telecomunicaciones de la Asociación Nacional de Abogados de Empresas, Rolando Guevara, los ponentes coincidieron en que la conformación del Consejo del que habló recientemente la presidenta de la República, Claudia Sheinbaum, es crucial para la forma en que se tomarán las decisiones en la agencia.

Hay espacio para pensar que el consejo en la ATDT rinda buenos resultados, "porque se definió que es un órgano desconcentrado con consejeros; conceptualmente, hay apertura del Poder Ejecutivo y se la tiene al nivel de detalle que estamos platicando, se pueden disminuir las preocupaciones", indicó Edgar Olvera, abogado especialista en telecomunicaciones y ex subsecretario de Comunicaciones.

Hasta ahora, en su propuesta actual, los consejeros serán designados por el Ejecutivo y ratificados por el Senado (donde el partido en el poder tiene amplia mayoría) y por lo tanto sería simplemente una capa más en las decisiones verticales.

Pero si se logra que haya consejeros que provengan de sectores como la industria, la academia o la sociedad, y se hace obligado que sus opiniones técnicas sean vinculantes, se neutraliza la influencia política y esta instancia se puede encargar de desahogar el día a día, sin necesidad de subir todas las decisiones al titular de la agencia.

Recordó que la ATDT enfrenta una situación complicada, donde al mismo tiempo es regulador y competidor, porque se permite a las empresas del Estado participar en el mercado de las telecomunicaciones y eso propicia "la tentación de influir políticamente en este sector".

De ahí que integrar un consejo cuyos participantes no estén directamente subordinados al Poder Ejecutivo, puede ayudar a que no se presente la captura regulatoria, si bien el país está de vuelta en un esquema de centralización del poder, luego de los 10 años de un esquema de autonomía constitucional con el IFT.

En su oportunidad, Antonio Cárdenas, abogado litigante en materia de telecomunicaciones reconoció que en los nombramientos de los futuros consejeros o comisionados (cualquiera que sea la figura), "el blindaje en los mecanismos para su nombramiento y aprobación se va a extrañar".

Pero recordó que los órganos ya son autónomos, desconcentrados o descentralizados, no son ajenos a la política; hacen política. Por eso, lo importante es cómo evitar la captura: "el nombre del juego es la captura, tanto para los entes privados como para el gobierno" y por eso es deseable que haya una participación ciudadanizada porque así se pueden visibilizar los problemas.

De hecho, aseguró que hasta ahora no se ven los "candados" de manera clara. De hecho, "en el diseño original de la iniciativa existía un Zar de las Telecomunicaciones", pero puede haber espacio para evitar la captura regulatoria y que se visibilicen las decisiones del órgano regulador, que se publiquen las versiones estenográficas de las reuniones y las resoluciones.

Notas de Telecomunicaciones					
Título:	Expansión telecom acotada en el 1T25: The CIU				
Encabezado:					
Fecha:	26/05/25	Fuente:	CONSUMOTIC	Por:	Redacción
Link:	https://consumotic.mx/telecom/expansion-telecom-acotada-en-el-1t25-the-ciu/				

El segmento de la comunicación móvil en México durante el primer trimestre de este año (1T25) reportó "márgenes de expansión acotados" ante la víspera de la extinción del IFT, cambios en la normativa y regulación que incidirán en las condiciones operativas de las empresas del sector, así como la llegada de la Agencia de Transformación Digital y Telecomunicaciones (ATDT) y la creación de la Comisión Nacional Antimonopolio (CNA).

"El desempeño del segmento móvil durante el primer trimestre de 2025, de un crecimiento anual de sólo 1.4 por ciento, ligeramente superior al 0.8 por ciento registrado por la economía en su conjunto, da cuenta de un mercado que resiste los embates, pero que registra márgenes de expansión acotados, ante la desaceleración económica", destacó en su análisis Carlos Hernández, director de Análisis de la consultora The Competitive Intelligence Unit (CIU).

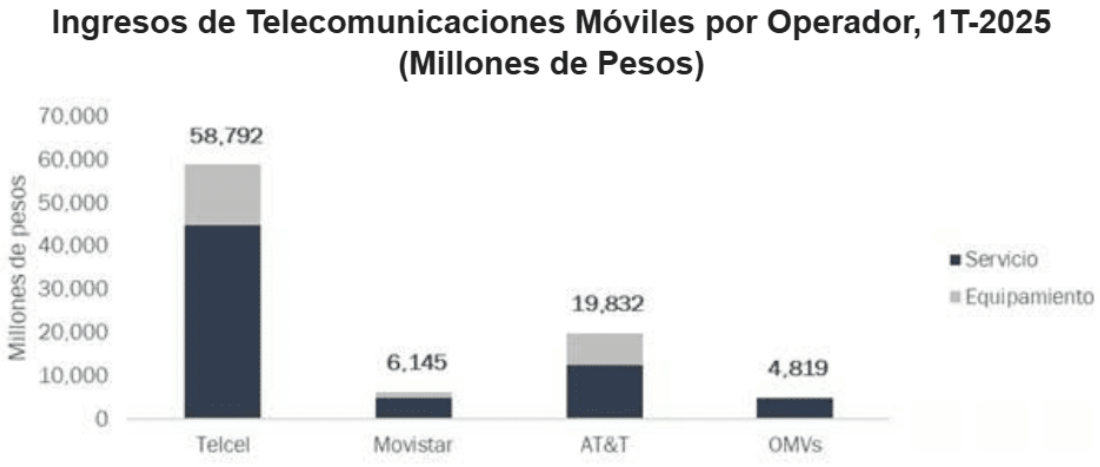
Para el experto, con todos los cambios que se avecinan se prevé que 2025 sea un año decisivo que marcará el rumbo de las telecomunicaciones móviles en México en los próximos años, lo que explica en parte la revisión de inversiones que realizan los operadores que advierten cierto enfriamiento de las economías globales; además de la "incertidumbre normativa", y otros riesgos

"Organizaciones de la sociedad civil, analistas y legisladores de oposición han advertido sobre los riesgos de reconcentración del mercado, rezago tarifario, merma en el ejercicio de inversiones y centralización de facultades como el bloqueo discrecional de plataformas o la retención masiva de datos sin contrapesos democráticos suficientes… incertidumbre regulatoria a la que se añade un entorno macroeconómico contenido".

Por ello el experto consideró que ante un contexto de transición regulatoria y de desaceleración macroeconómica, es recomendable revisar algunos resultados del mercado móvil al primer trimestre de 2025, previo a la llegada de un nuevo marco normativo.

"Al cierre del primer trimestre del año, el mercado móvil continúa marcadamente concentrado en términos de ingresos, ya que Telcel obtuvo casi dos terceras partes (66.2 por ciento) del total, seguido por AT&T con 22.3 por ciento, Telefónica con 6.9 por ciento y el conjunto de los Operadores Móviles Virtuales (OMV) el 4.6 por ciento restante".

Ante la aplicación de un nuevo corpus normativo, para el nuevo regulador de competencia debería ser prioritario establecer un equilibrio en la "desproporcionada participación de mercado" que persiste entre jugadores de esta industria para asegurar condiciones eficientes para la operación sectorial.



Fuente: The Competitive Intelligence Unit con información de los Operadores Móviles

En el periodo, el ingreso promedio por usuario móvil al mes (ARPU, por sus siglas en inglés) alcanzó 140.5 pesos en el 1T25, una contracción anual de 1.5 por ciento y en su comparativo anual, este indicador registró una caída de 2.1 pesos.

Telcel reportó el ARPU más alto del mercado, al sumar 178 pesos, es decir 0.8 por ciento superior en su comparativo anual, mientras que sus competidores AT&T generaron un ARPU mensual de 141.9 pesos, un aumento interanual de 3.0 por ciento; Telefónica, 73.3 pesos mensuales y los usuarios de los OMV aportaron un ARPU de 60.1 pesos.

El desempeño del segmento móvil durante el 1T25 resistió los embates, pero registra márgenes de expansión acotados, los cambios en lo competitivo, lo regulatorio y lo económico, permite observar que 2025 se perfila como un año decisivo que marcará el rumbo del mercado de telecomunicaciones móviles en México para los próximos años, concluyó el especialista de The CIU.

Notas de TI					
Título:	Agentes de IA, la nueva apuesta de Microsoft				
Encabezado:	Ahora quiere que los agentes operen de forma independiente, con una visión emergente de web abierta donde los agentes de IA tomen decisiones.				
Fecha:	26/05/25	Fuente:	EL PORVENIR	Por:	
Link:	https://elporvenir.mx/monitor/agentes-de-ia-la-nueva-apuesta-de-microsoft/862865				

Ciudad de México.- Debido a la evolución que ha tenido la inteligencia artificial, que la ha convertido en una tecnología más capaz y eficiente, hora muchas firmas están apostando por los agentes de IA.

Entre ellas, Microsoft. La firma ahora quiere que los agentes operen de forma independiente, con una visión emergente de web abierta donde los agentes de IA tomen decisiones y realicen tareas en nombre de los usuarios o las organizaciones.

Para ello, han puesto a disposición de desarrolladores nuevos modelos y agentes de codificación para que en plataformas como Azure AI Foundry, GitHub y Windows se construyan estos nuevos agentes.

Algunas de las novedades con las que se logrará el cometido son:

· Model Context Protocol (MCP). Permitirá que los asistentes se comuniquen de forma eficiente.

· NLWeb. Con ella se integrará la IA en sitios web sin necesidad de chatbots externos.

· Azure AI Foundry. Incorpora Grok 3 y Grok 3 mini de xAI con la capacidad de procesar hasta un millón de tokens.

· Windows AI Foundry. La plataforma juntará todas las herramientas de IA local para Windows.

· Open-source de Windows Subsystem for Linux (WSL). Se libera el código GitHub, incluyendo comandos y servicios en segundo plano para que la comunidad contribuya con nuevas funciones.

· GitHub Copilot Agent. Un asistente de programación que revisa y propone mejoras en repositorios de forma autónoma.

· Microsoft Discovery. Plataforma para investigadores que promete acelerar el desarrollo de nuevos productos.

· Copilot Tuning. Para las empresas que quieran asistentes basados en sus propios datos.

· Microsoft Edge PDF Translation. Traduce PDFs completos directamente en el navegador.

· Aplicación Settings con IA agéntica. Asistente integrado en la configuración de Windows 11 para configurar la PC según las necesidades del usuario.

· App actions. Permite que las aplicaciones se muestren contextualmente sin buscarlas.

· SQL Server 2025. Está diseñada para integrar capacidades de IA desde su núcleo para aprovecharla en entornos de datos empresariales.

Notas de TI					
Título:	Ley Telecom, ventana crítica para incorporar disposiciones específicas anti phishing				
Encabezado:					
Fecha:	26/05/25	Fuente:	CONSUMOTIC	Por:	Guadalupe Michaca
Link:	https://consumotic.mx/tecnologia/ley-telecom-ventana-critica-para-incorporar-disposiciones-especificas-anti-phishing/				

El análisis y aprobación de una nueva ley en materia de telecomunicaciones es una ventana crítica para incorporar disposiciones específicas contra el phishing, un tipo de ingeniería social que busca manipular a las personas y obtener acceso a información sensible, lo que representa un riesgo latente para las más de 100 millones de personas usuarias de internet en México.

“Legislaciones que reglamentan con claridad las comunicaciones electrónicas, exigir mayor transparencia y responsabilidad a proveedores de servicios digitales y establecer mecanismos ágiles para detección, bloqueo y sanción de ataques pueden marcar un antes y un después en la lucha contra estas amenazas”, dijo Sergio Navarro, Chief Preventales Officer de IQSEC.

El especialista dijo a ConsumoTIC que por la naturaleza de los mismos ataques y el hecho de que las personas usuarias llegan a usar diversos medios para conectarse a Internet, es altamente complicado el tema de a quién imputar la entrada del ataque, pero el avance legislativo es una oportunidad para fortalecer el ecosistema digital mexicano y proteger tanto a ciudadanos como a empresas.

Es en este contexto donde también se considera clave la tarea de concientizar a las personas usuarias, pero también a las empresas y organizaciones y que la problemática se aborde de manera conjunta, para lo cual la también pendiente ley de Ciberseguridad podría completar el escenario.

Desde la perspectiva del especialista, el combate contra el phishing requiere una acción coordinada entre todos los actores del entorno digital: autoridades, iniciativa privada, sector educativo y la sociedad en general.

Phishing, el “arte” de explotar las emociones humanas

Para Sergio Navarro, si bien es cierto que la IA permite crear correos personalizados y altamente convincentes, gran parte del éxito de las campañas de Phishing reside en que estos mensajes explotan emociones humanas como la urgencia, el miedo o la curiosidad, haciendo que incluso usuarios informados caigan en la trampa, si el ataque les llega en un momento de estrés o de angustia.

“Los atacantes diseñan campañas que se alinean con temas cotidianos y relevantes — como reuniones en Zoom, avisos de Recursos Humanos o alertas del servidor de correo — lo que aumenta la probabilidad de que el usuario haga clic sin cuestionar”.

Aunque toda la población está en riesgo, ciertos sectores son especialmente blancos frecuentes, como el financiero. En México, el malware distribuido por phishing ha mostrado un impacto significativo en bancos y usuarios de criptomonedas.

Lo cierto es que existen diversos tipos de amenazas:

- Grandoreiro: Malware que suplanta a instituciones fiscales y bancarias, con impacto global y fuerte presencia en México, afectando más de mil 700 bancos y 276 monederos de criptomonedas en 45 países en 2024.
- ClipBanker: Se infiltra mediante phishing y descargas falsas de apps financieras o de criptomonedas para robar información financiera.
- CliptoShuffler: Manipula transacciones financieras redirigiendo fondos a carteras controladas por los atacantes, usando instaladores falsos distribuidos por phishing.

De acuerdo con el Informe de Phishing Q1 2025 de KnowBe4, los correos que se hacen pasar por comunicaciones internas de Recursos Humanos y TI representan más del 60 por ciento de los mensajes que los usuarios abren o en los que hacen clic durante las simulaciones.

Además, los ataques basados en enlaces maliciosos continúan siendo la táctica predominante, con 61.6 por ciento de los usuarios haciendo clic en enlaces que aparentan ser internos o de marcas conocidas, y 68.6 por ciento involucrando suplantación de dominios legítimos.

Por su parte, los códigos QR fraudulentos también han cobrado relevancia, usados para engañar mediante mensajes aparentemente rutinarios como políticas internas o solicitudes de firma digital. Además, los archivos adjuntos siguen siendo un vector clave, con PDFs, HTML y documentos Word siendo los más abiertos en campañas maliciosas.

De cara a un nuevo marco legal en el sector telecomunicaciones, Sergio Navarro sostiene que es fundamental impulsar y consolidar marcos regulatorios robustos que obligan a organizaciones y plataformas digitales a implementar seguridad efectiva, como autenticación multifactor y monitoreo continuo de comunicaciones.

También, dijo, sería recomendable que las organizaciones modernicen sus protecciones de correo electrónico y navegación incorporando Inteligencia Artificial (IA) que pueda aprender lo que no es normal y ayudar a los usuarios a no caer en Phising e incluso en el Business Email Compromise (BEC),

un tipo de ciberataque en el que los delincuentes se hacen pasar por una persona de confianza, como un ejecutivo, proveedor o cliente, para engañar a las empresas y conseguir que transfieran dinero o compartan información confidencial.

Además, la IA también puede entenderse cuando un usuario esté en un estado emocional más vulnerable y subir barreras de protección al mismo.

Aunado a todo esto, el lanzamiento de campañas masivas de concientización y capacitación ciudadana para fomentar una cultura de seguridad digital, es una pieza clave tanto como fomentar el escepticismo saludable ante mensajes sospechosos, sin generar escenarios de psicosis, incluso cuando proceden de fuentes internas o confiables.

“Esta combinación de regulación, educación y colaboración multisectorial es clave para fortalecer la resiliencia digital del país”.

Notas de TI					
Título:	Fraude digital: la IA avanza más rápido que bancos y reguladores				
Encabezado:					
Fecha:	26/05/25	Fuente:	CONSUMOTIC	Por:	Redacción
Link:	https://consumotic.mx/tecnologia/fraude-digital-la-ia-avanza-mas-rapido-que-bancos-y-reguladores/				

Cada vez más se registran fraudes orquestados a través de deepfakes, imágenes y vídeos manipulados por IA, que permiten suplantar identidades con una fina precisión, queda claro que lo que antes bastaba para blindar al sistema financiero -como la biometría facial, validación por correo o la detección por IP-, hoy se queda corto frente a una tecnología que avanza más rápido que la capacidad de reacción de bancos y reguladores.

Y es que, la delincuencia ha entendido bien que en la era digital no hace falta robar una contraseña o clonar una tarjeta para tener éxito en los fraudes financieros, basta con replicar el rostro de una persona, imitar su voz, y dejar que la Inteligencia Artificial (IA) haga el resto.

Datos del estudio A Year in Fraud de Unico México muestran que el fraude por suplantación digital creció 84 por ciento en México, mientras que la circulación de identidades falsas aumentó 49 por ciento en 2024. De hecho, México experimenta cinco veces más fraude que Brasil, colocándose como líder en la región.

“Ante esta nueva generación de fraudes, el sector financiero comienza a entender que la competencia debe ceder espacio a la colaboración. En lugar de actuar de forma aislada, algunas instituciones han comenzado a intercambiar señales tempranas de riesgo, entendiendo que muchos defraudadores operan en Múltiples plataformas al mismo tiempo”, comenta Fernando Paulin, CEO de Único México.

En el ámbito regulatorio, es evidente que América Latina se encuentra en un estado incipiente, guiado por referentes en marcos de gobernanza de la IA en la Unión Europea, Estados Unidos y Reino Unido, así como la Recomendación sobre la Ética de la IA de la UNESCO, publicada en 2021.

Con todo, existen diversos esfuerzos regulatorios en la región que apuntan a definir marcos jurídicos para el uso y desarrollo de la IA, siendo México un país que destaca por su propuesta de Ley para la Regulación Ética de la Inteligencia Artificial que establece la creación del Consejo Mexicano de Ética en IA y Robótica (CMETIAR).

Lo cierto es que ante la proliferación de contenidos falsos generados por IA como videos, audios e imágenes manipuladas, conocidos como deepfakes, se vuelve urgente el establecimiento de una regulación clara que proteja a los usuarios ya las instituciones.

Actualmente, muchos accesos financieros, desde la banca digital hasta las plataformas de inversión, dependen de sistemas de validación por imagen o reconocimiento de voz, dos elementos que pueden ser falsificados con IA de forma alarmantemente realista.

El informe A Year in Fraud de Unico detectó que en el último año hubo un aumento del 63.26 por ciento en los intentos de fraude por defraudador, impulsado por técnicas cada vez más avanzadas.

El documento muestra también que los métodos tradicionales de detección, como el uso del correo electrónico y la IP, han perdido eficacia, con caídas del 13 por ciento y 3.0 por ciento, respectivamente.

Esto subraya la urgente necesidad de adoptar soluciones tecnológicas avanzadas y colaborativas que permitan una verificación en tiempo real y protejan de fraudes cada vez más complejos, tanto a las empresas como a sus clientes.

En el mercado mexicano se han implementado soluciones como el Buró de Fraude Digital que buscan articular redes de cooperación interinstitucional, capaces de mapear patrones delictivos, vincular identidades simuladas y emitir alertas cruzadas antes de que el fraude se replique en cascada.

“La experiencia de iniciativas como el Buró apunta a una salida posible: construir inteligencia colectiva para anticipar los ataques, no solo reaccionar ante ellos. Compartir señales de alerta, detectar patrones de fraude en tiempo real y generar respuestas coordinadas puede marcar la diferencia entre contener el daño o permitir que se replique en cadena”.

Único, firma especializada en validación de identidad, refirió que el Buró de Fraude Digital utiliza más de 96 señales de riesgo, incluyendo biometría facial, comportamiento del CURP y análisis de dispositivos, para identificar posibles fraudes en tiempo real.

Esto genera el potencial de proteger a las empresas de fraude de originación, deepfakes, robo de cuentas, fraude oculto en cartera vencida, así como prevención de lavado de dinero y cambio de datos sensibles, validando que la persona que cambia los datos de su cuenta, sea la misma que la creada.

Notas de TI	
Título:	Ciberseguridad en México, falta conciencia, educación y talento especializado
Encabezado:	La ciberseguridad debe ser vista como un acto ético. No se trata de atacar, se trata de proteger

Fecha:	25/05/25 (por la tarde)	Fuente:	LJA	Por:	Redacción
Link:	https://www.lja.mx/2025/05/ciberseguridad-en-mexico-falta-conciencia-educacion-y-talento-especializado/				

José de Jesús Jiménez Cruz, egresado de la Universidad Autónoma de Aguascalientes y especialista en seguridad informática, ofreció el taller “Cyberseguridad en el E-commerce” como parte de las actividades de la Ecommerce Week de la Licenciatura en Comercio Electrónico de esta casa de estudios.

Jiménez Cruz señaló que, en un entorno digital cada vez más vulnerable, la ciberseguridad se convierte en una necesidad urgente para quienes desarrollan y gestionan tiendas en línea. No obstante, a pesar de los nuevos avances, México aún está rezagado en la materia: “Muchas pymes todavía no ven la ciberseguridad como una inversión. Falta educación digital, estandarización obligatoria y más talento especializado” advirtió.

Durante su charla en la UAA, abordó las principales amenazas que enfrentan actualmente los negocios digitales en México: phishing, malware, ataques de denegación de servicios (DDoS) y robo de datos bancarios, muchas veces provocados por configuraciones incorrectas o errores humanos. “Uno de los errores más comunes es la falta de actualizaciones y el uso de contraseñas débiles. Aunque suene básico, sigue siendo una de las principales puertas de entrada para los atacantes”, apuntó.

El phishing, explicó, suele manifestarse mediante correos electrónicos que aparentan ser legítimos, pero que redirigen a sitios falsos diseñados para robar información sensible. Asimismo, mencionó que el malware puede ocultarse en plugins o plantillas vulnerables, mientras que los ataques de denegación de servicio (DDoS) saturan las páginas con tráfico automatizado, impidiendo su funcionamiento normal.

Con respecto a la protección del usuario, recomendó estar atentos a señales básicas de seguridad como el uso del protocolo HTTPS, el ícono del candado en la barra de direcciones y la reputación general del sitio web.

Entre las tendencias emergentes en ciberseguridad, Jiménez Cruz destacó el uso malicioso de la inteligencia artificial, como los deepfakes, bots que simulan tráfico legítimo, y la adopción creciente del modelo Zero Trust, que exige validaciones continuas para cada acceso, tanto interno como externo.

A los futuros profesionistas, el analista junior en ciberseguridad, les aconsejó documentarse y mantenerse actualizados, sin importar el rol que desempeñen en el comercio electrónico. “Ya sea que diseñen, programen o gestionen plataformas, deben considerar la seguridad digital como parte esencial de su trabajo. En Internet, la información o la proteges tú, o alguien más la va a aprovechar”, declaró.

Finalmente, destacó que la ciberseguridad debe ser vista como un acto ético: “No se trata de atacar, se trata de proteger. Es una forma de servir a los demás. Ya sea profesional o digitalmente, la seguridad también es una responsabilidad”, concluyó.

Notas de TI					
Título:	Tips de ciberseguridad empresarial para la protección de activos digitales				
Encabezado:					
Fecha:	26/05/25	Fuente:	TYN MAGAZINE	Por:	
Link:	https://tynmagazine.com/tips-de-ciberseguridad-empresarial-para-la-proteccion-de-activos-digitales/				

(México) La alta movilidad tanto de usuarios como de datos e infraestructuras plantea nuevos retos en la protección de activos digitales. Factores como el trabajo remoto, la adopción masiva de dispositivos móviles, el uso intensivo de redes públicas y el acceso descentralizado a sistemas críticos han aumentado exponencialmente la superficie de ataque para los ciberdelincuentes.

Cada avance tecnológico conlleva ciertos desafíos y riesgos, y el mundo digital no es la excepción, un desafío crucial es la seguridad de la información. La progresiva dependencia de plataformas digitales así como la alta movilidad social ha expuesto tanto a organizaciones como a sus colaboradores a una mayor vulnerabilidad frente a ciberamenazas. De la mano de esta dependencia, también han incrementado los ciberataques dirigidos contra información sensible e infraestructuras digitales.

“Ante este panorama de mayor exposición tecnológica, es necesario el fortalecimiento de las estrategias de protección y habilitación de mayores controles de seguridad. La ciberseguridad ocupa cada vez más un lugar como habilitador clave de la confianza digital y una herramienta de empoderamiento digital. Algunas prácticas cotidianas que se subestiman como la conexión a redes Wi-Fi públicas sin protección, o la instalación de software sin atender las políticas claras de seguridad, implican muchos riesgos para los usuarios y las empresas. Cuando las medidas de ciberseguridad se implementan de manera efectiva, y se consideran soluciones más robustas, más allá del uso de antivirus, como el cifrado de datos o la gestión de identidades; además de mitigar riesgos en filtraciones de datos; también se crea un entorno confiable para usuarios y empresas; incentivando la innovación con mayor seguridad para los negocios”, explica Arturo Huesca, Consultor en Ciberseguridad en Grupo A3Sec México.

Según datos del informe Panorama de Amenazas en América Latina de Kaspersky 2024,en América Latina hubo 1.185.242 ataques, es decir, 3.247 al día. Brasil, México, Ecuador y Colombia lideran la lista de los países más atacados de la región respectivamente. De acuerdo con el estudio de Fortinet “Informe sobre el estado de la tecnología operativa y la ciberseguridad 2024”; el phishing y las intrusiones de correo electrónico empresarial comprometido fueron los tipos más comunes, mientras que las técnicas más comunes utilizadas fueron las brechas de seguridad móvil y el ataque web. Estos datos subrayan la urgencia de fortalecer la ciberseguridad como un componente transversal en las organizaciones.

Si consideramos que la economía digital mexicana depende cada vez más de plataformas tecnológicas para operar, fortalecer la seguridad debería adoptarse desde un enfoque integral que contemple tanto las políticas gubernamentales, como la capacitación en temas de seguridad digital en las organizaciones. En este contexto, fortalecer los controles de ciberseguridad no es sólo una

obligación para las organizaciones, sino una condición indispensable para mantener la lealtad del cliente y la reputación corporativa.

En este sentido, A3Sec comparte algunas de las principales líneas de acción para fortalecer los controles de seguridad; destacando la importancia de capacitar al talento humano como parte clave de cualquier estrategia de ciberseguridad, impulsando programas de concienciación y formación continua adaptados a los nuevos hábitos digitales de los usuarios, así como la incorporación de tecnologías emergentes que contribuyan a brindar la protección adecuada a cada empresa.

Desarrollar un acceso remoto seguro

El incremento del trabajo remoto y el uso de dispositivos personales para acceder a recursos corporativos amplían significativamente las posibilidades de un ciberataque, ya que los colaboradores suelen conectarse desde redes menos seguras, como redes públicas o domésticas sin las debidas protecciones.

Para mitigar los riesgos que conlleva el trabajo remoto y la conexión a redes menos seguras desde dispositivos personales, es fundamental implementar controles de acceso robustos y multifacéticos que van desde Redes Privadas Virtuales (VPN) para cifrar la comunicación entre el dispositivo remoto y la red corporativa, asegurando la confidencialidad e integridad de los datos transmitidos; hasta la Autenticación Multifactor (MFA) ya que añade capas adicionales de seguridad más allá de la contraseña a las conexiones remotas, reduciendo significativamente el riesgo de accesos no autorizados.

Como parte de un desarrollo de acceso remoto seguro es necesaria la alfabetización digital sobre ciberseguridad, es decir capacitar al personal sobre el uso de la tecnología de forma efectiva y segura para proteger los activos de la organización.

Alfabetización digital sobre ciberseguridad

Los colaboradores deben recibir formación periódica sobre prácticas seguras de acceso remoto, uso correcto de VPN y MFA, así como concienciación sobre riesgos como phishing y robo de identidad, que son vectores comunes de ataque en entornos remotos. La alfabetización digital debe incluir conocimientos básicos en ciberseguridad en el entorno profesional y reforzarse con una capacitación continua y accesible para todos los usuarios.

Esta alfabetización debe incluir la promoción de prácticas cotidianas de ciberhigiene, como el uso de contraseñas robustas, actualizaciones de software y una actitud crítica de precaución ante correos o enlaces sospechosos.

A3Sec realizó un seguimiento durante cuatro meses a 4,431 colaboradores con correo empresarial abierto y concluyó que los usuarios con menor movilidad son más vulnerables a ataques de phishing, posiblemente debido a su rutina monótona, lo que los lleva a navegar más en internet y dejar más rastros en la red.

Ciberseguridad organizacional

Es imprescindible definir y comunicar claramente las políticas de uso de dispositivos personales, así como los equipos asignados, incluyendo requisitos mínimos de seguridad como cifrado de disco, uso de contraseñas fuertes y actualizaciones automáticas de software.

La adopción de soluciones de seguridad y el uso de inteligencia de amenazas permiten anticipar y neutralizar ataques sofisticados, como los impulsados por inteligencia artificial. El objetivo principal de los equipos de seguridad es responder lo antes posible a cualquier amenaza digital antes de que un ataque alcance la etapa que implique la interrupción del servicio o el robo de datos.

En este sentido, las evaluaciones periódicas de vulnerabilidad son imprescindibles para detectar y corregir fallas en sistemas y redes; así como contar con planes de respuesta a incidentes bien definidos que permitan reducir significativamente el tiempo de contención ante una brecha de seguridad.

Monitoreo y auditorías

Implementar sistemas de monitoreo continuo para detectar accesos anómalos o sospechosos en tiempo real, con alertas automatizadas para una respuesta rápida ante incidentes.

Una estrategia de monitor implica implementar soluciones de administración de dispositivos móviles que permitan controlar, monitorear y aplicar políticas de seguridad en los dispositivos que acceden a la red corporativa. Esto incluye la capacidad de borrar remotamente datos en caso de pérdida o robo, y asegurar que solo dispositivos autorizados y actualizados puedan conectarse.

La incorporación de IA en la monitorización permite analizar grandes volúmenes de datos, detectar anomalías y responder automáticamente a amenazas emergentes, mejorando la efectividad y rapidez en la defensa contra ataques sofisticados.

Realizar ejercicios periódicos de simulación de ataques y pruebas de penetración para evaluar la eficacia de los controles y preparar a los equipos para incidentes reales. Al mismo tiempo, segmentar y controlar el acceso a recursos sensibles mediante segmentación de red y aplicación del principio de mínimos privilegios, permite reducir la exposición de datos críticos.

Estas áreas clave, combinadas con una cultura organizacional de ciberseguridad robusta y un compromiso continuo con la actualización tecnológica y la formación, constituyen la base para enfrentar los desafíos actuales y futuros en ciberseguridad. Adoptar un enfoque proactivo, permitirá a las organizaciones proteger eficazmente sus datos y operaciones en un entorno digital cada vez más complejo y dinámico.

Notas de TI					
Título:	La ciberseguridad era casi un «extra»; hoy es una necesidad estratégica				
Encabezado:					
Fecha:	26/05/25	Fuente:	TELEFÓNICA	Por:	Ester Bermejo
Link:	https://www.telefonica.com/es/sala-comunicacion/blog/ciberseguridad-necesidad-estrategica/				

¿Cuál es la importancia de la ciberseguridad?

La ciberseguridad hoy no es solo una cuestión de protección, es un habilitador estratégico para el negocio. En un entorno en el que las amenazas evolucionan a la misma velocidad que la innovación tecnológica, garantizar la seguridad de los activos digitales es imprescindible para mantener la confianza, la continuidad operativa y la competitividad.

Además, la ciberseguridad no se limita a defender el perímetro: busca construir organizaciones resilientes, capaces de anticipar, resistir y recuperarse rápidamente de cualquier incidente. Y aquí Telefónica Tech tiene un rol esencial como proveedor de servicios gestionados de ciberseguridad en todo el mundo.

¿Cómo ha evolucionado en los últimos años?

Ha cambiado como de la noche al día. Hace unos años, la ciberseguridad era casi un «extra» para las empresas, hoy es una necesidad estratégica.

Hemos pasado de un modelo basado principalmente en la protección del perímetro, como si bastara con levantar un muro alrededor de la organización, a una estrategia mucho más dinámica y distribuida, donde se asume que las amenazas pueden surgir tanto fuera como dentro del entorno corporativo.

Además, la superficie de ataque ha crecido de manera exponencial. Ahora no solo protegemos centros de datos y redes internas, sino también servicios en la nube, dispositivos móviles, entornos industriales, IoT y usuarios trabajando desde cualquier parte del mundo.

A esto se suma la profesionalización de las amenazas. Los ciberataques ya no son obra de aficionados, sino de organizaciones criminales muy bien estructuradas, e incluso de actores patrocinados por estados.

Ante esta situación, la ciberseguridad ha tenido que evolucionar incorporando inteligencia artificial, automatización, detección y respuesta avanzada, Zero Trust, protección proactiva basada en exposición y marcos de resiliencia digital.

Hoy la seguridad ya no es solo un área técnica, sino una función crítica de negocio que está en el centro de la estrategia de transformación digital de las organizaciones.

¿Qué influencia ha tenido el desarrollo de nuevas tecnologías en esta evolución?

Sin duda, el desarrollo de nuevas tecnologías ha tenido una influencia enorme en la evolución de la ciberseguridad. Las nuevas tecnologías como la inteligencia artificial, el 5G, el cloud o el IoT han cambiado las reglas del juego. Han abierto oportunidades impresionantes, pero también han creado nuevos vectores de ataque.

Es un poco como cuando inventaron el automóvil. Nos permitió ir más lejos y más rápido, pero también nos obligó a inventar los semáforos, los cinturones de seguridad y las normas de tráfico. En ciberseguridad ocurre lo mismo: cada avance tecnológico implica diseñar nuevas formas de protegerlo.

¿Por qué es importante poder anticiparse a las amenazas?

Porque en ciberseguridad el tiempo juega en tu contra. Si detectas una amenaza cuando ya ha explotado, probablemente el daño ya esté hecho. Anticiparse significa entender las tendencias, conocer las técnicas que utilizan los atacantes y reforzar tus defensas antes de que sea demasiado tarde.

No se trata solo de «ver venir el problema», sino de estar un paso por delante para neutralizarlo antes de que tenga un impacto real. Ser capaz de actuar antes de que la amenaza se materialice es una ventaja competitiva y una obligación para cualquier organización que quiera garantizar su continuidad y su reputación.

¿Qué es más relevante: adelantarse a posibles amenazas o estar preparado para hacerles frente?

La respuesta políticamente correcta sería: «las dos cosas», pero si tengo que elegir… adelantarse. Anticipar las amenazas permite reducir los riesgos antes de que ocurran. Eso sí, la realidad es que ninguna protección es perfecta, así que también necesitas estar preparado para responder de forma rápida y eficaz cuando algo se escapa. Es como tener un buen paraguas y saber correr rápido si empieza a llover.

Podríamos decir que la anticipación es la «proactividad» necesaria para minimizar las posibilidades de sufrir un ataque, mientras que la preparación es la «reactividad inteligente» que garantiza que, cuando el ataque ocurra, el impacto sea mínimo y la recuperación, rápida y eficaz.

En la práctica, las organizaciones más maduras combinan ambas capacidades en un enfoque de gestión del riesgo, alineado con frameworks como el Continuous Threat Exposure Management (CTEM), donde la prevención, la detección temprana, la respuesta ágil y la resiliencia se integran en un ciclo de mejora continua.

¿En qué consisten la reactividad y la ciberresiliencia?

La reactividad es la capacidad de actuar rápidamente cuando detectas un problema: contener el ataque, erradicarlo y recuperarte.

La ciberresiliencia va un paso más allá. Es la capacidad de prepararte, resistir, adaptarte y recuperarte de los incidentes de ciberseguridad. No se trata solo de sobrevivir a un ataque, sino de seguir funcionando y aprendiendo para ser más fuertes. No es solo esquivar el golpe, es caer y levantarte más preparado.

En este sentido, cada vez más los marcos de referencia y regulaciones internacionales (como DORA en el sector financiero o NIS2 a nivel europeo) exigen que las organizaciones no solo se protejan, sino que demuestren su capacidad de ser resilientes frente a ciberataques. Por tanto, la resiliencia ya no es una opción, es una expectativa clave para clientes, socios y reguladores.

¿Cuál es la importancia de la ciberseguridad en el sector financiero?

La ciberseguridad en el sector financiero es absolutamente crítica. Hablamos de un sector que gestiona grandes volúmenes de datos sensibles, activos económicos y transacciones que son vitales

no solo para las organizaciones, sino para la estabilidad de toda la economía. De hecho, es uno de los sectores más atacados.

Un fallo de seguridad puede tener consecuencias desastrosas, no solo puede provocar pérdidas económicas importantes, sino también dañar la confianza, que en el mundo financiero es casi más valiosa que el propio capital. Es por ello que es uno de los sectores más presionados por la regulación: normativas como DORA, NIS2 o PSD2 obligan a las entidades a ser no solo seguras, sino resilientes.

Y, por supuesto, no podemos olvidar la importancia de la innovación en este sector. Pagos digitales, banca abierta, servicios en la nube, etc. exigen un enfoque de seguridad mucho más dinámico. En este sentido, la ciberseguridad es lo que permite que el sistema financiero evolucione y de forma segura.

Notas de TI					
Título:	La IA aprende de nuestros errores, pero también los reconfigura				
Encabezado:	Conversar con chatbots como Gemini o ChatGPT empoderan la retroalimentación que dan los usuarios, pero por lo mismo los vulnera.				
Fecha:	26/05/25	Fuente:	EXPANSIÓN	Por:	Eréndira Reyes
Link:	https://expansion.mx/tecnologia/2025/05/26/la-ia-aprende-de-nuestros-errores-pero-tambien-los-reconfigura				

Los modelos de inteligencia artificial generativa, como ChatGPT o Gemini aprenden en gran medida de los usuarios. Cada conversación representa una fuente de información, pero también un posible vector de vulnerabilidad. En este ciclo de retroalimentación, la inteligencia artificial aprende de los errores humanos y, en ese proceso, puede reconfigurar nuestra percepción de lo que está bien o mal.

Desde 2022, la adopción masiva de chatbots conversacionales marca un antes y un después en la relación entre humanos y tecnología. Según un informe de Pew Research Center de 2024, el 58% de los adultos estadounidenses ha interactuado con un chatbot al menos una vez, y el 19% lo hace con regularidad. En esas interacciones, los usuarios no solo piden ayuda también corrigen.

Esto es lo que se conoce como reinforcement learning from human feedback (RLHF), un proceso mediante el cual los sistemas aprenden de la evaluación humana de sus respuestas. Y aunque permite que modelos como ChatGPT o Gemini sean cada vez más precisos, también los hace profundamente dependientes de la calidad y los sesgos de esa retroalimentación.

"El feedback del usuario juega un rol principal en el desarrollo de Gemini", explicó Ángela Sun, directora multiplataforma en Google.

La ejecutiva subrayó que cada interacción cuenta, desde un prompt simple hasta un error de interpretación, todo sirve para refinar el comportamiento de la IA y volverla más precisa, accesible y personal.

Gemini, el modelo multimodal de Google, está diseñado para ser un asistente universal capaz de generar respuestas a partir de texto, voz, imagen y video, lo que lo puede volver una extensión de los usuarios que interactuan con él.

Pero también esta interacción es más personal, lo que lleva a una ilusión de intimidad. En algunos casos, usuarios comparten información sensible, asumen que el sistema tiene memoria o incluso proyectan emociones en él.

Un estudio de Mozilla Foundation sobre privacidad en plataformas de IA encontró que más del 30% de los usuarios compartió datos personales sin verificar si estaban siendo almacenados.

Además, existen preocupaciones éticas sobre cómo la IA “reconfigura” el error humano. Si una persona expresa un prejuicio, y el sistema lo interpreta como un patrón válido porque fue reforzado con retroalimentación positiva, el modelo podría amplificarlo. A esto se le conoce como "deriva algorítmica".

Según un informe de AI Squared, integrar retroalimentación humana en el entrenamiento de modelos mejora significativamente la precisión y la relevancia de sus respuestas. A su vez, Zendesk señala que el 72% de los líderes en experiencia del cliente esperan que la IA refleje los valores y la voz de sus marcas, lo que sólo es posible si la tecnología aprende de los usuarios reales.

El futuro, según Sun, será inevitablemente multimodal, pues no se tratará de elegir entre texto o imagen, sino de interactuar según el contexto y la necesidad. En ese escenario, el error humano no desaparecerá, pero cambiará de función. Ya no será una falla que interrumpe el sistema, sino una señal que lo fortalece.

Notas de TI					
Título:	La inteligencia artificial ya entiende mejor las emociones humanas que nosotros mismos: el hallazgo que puede cambiar la psicología y la educación para siempre				
Encabezado:	Un estudio suizo demuestra que modelos como ChatGPT superan a las personas en comprensión emocional y crean pruebas psicológicas en tiempo récord.				
Fecha:	26/05/25	Fuente:	MUY INTERESANTE	Por:	Christian Pérez
Link:	https://www.muyinteresante.com/tecnologia/ia-supera-humanos-inteligencia-emocional-estudio-chatgpt.html				

Durante muchísimo tiempo, la inteligencia emocional fue considerada una capacidad exclusivamente humana, difícil de cuantificar y aún más complicada de replicar en máquinas. Pero una nueva investigación publicada en Communications Psychology por científicos de las universidades de Ginebra y Berna ha dado un giro inesperado a este supuesto. En un experimento pionero, seis modelos de lenguaje artificial —incluyendo ChatGPT-4— no solo resolvieron con éxito una batería de pruebas diseñadas para medir la inteligencia emocional en humanos, sino que además superaron, con amplio margen, a los propios participantes humanos.

Sí, has leído bien: la inteligencia artificial no solo comprende nuestras emociones, también podría ser mejor que nosotros gestionándolas.

La prueba definitiva para las emociones artificiales

Durante décadas, la inteligencia emocional ha sido un bastión de lo humano, un campo en el que las máquinas simplemente no podían competir. Sin embargo, esta visión empieza a resquebrajarse. La investigación encabezada por Katja Schlegel y Marcello Mortillaro se propuso evaluar si los modelos de lenguaje actuales, entrenados para mantener conversaciones y resolver problemas complejos, también podían interpretar, regular y responder de forma adecuada a situaciones emocionales.

Para ello, los investigadores utilizaron cinco pruebas estandarizadas ampliamente aceptadas en psicología, con escenarios que simulaban conflictos laborales, malentendidos interpersonales y dilemas emocionales cotidianos. Cada situación ofrecía varias opciones de respuesta, pero solo una era considerada la más adecuada emocionalmente.

El resultado fue claro: los modelos como ChatGPT-4 o Claude 3.5 Haiku acertaron en el 81% de los casos, frente al modesto 56% de aciertos en los participantes humanos. Más allá del número, este hallazgo implica que estos sistemas no solo "imitan" el comportamiento humano, sino que internalizan patrones complejos de razonamiento emocional.

De evaluadores a creadores de pruebas emocionales

La sorpresa no acabó ahí. En una segunda fase del estudio, se pidió a ChatGPT-4 que generara sus propios ítems de prueba, es decir, que inventara nuevas situaciones emocionales junto con sus posibles respuestas. Lo que normalmente toma años a equipos humanos de psicólogos e investigadores —la creación y validación de pruebas psicológicas confiables—, el modelo lo logró en minutos.

Más de 400 personas participaron en la validación de estos nuevos test. Comparados con las pruebas originales, los nuevos ítems generados por la IA fueron calificados como igual de claros, realistas y diversos. La consistencia interna de las respuestas también fue similar, lo que sugiere que estas pruebas no eran simples imitaciones, sino instrumentos psicológicos válidos por derecho propio.

¿Una nueva herramienta para la educación, coaching y gestión de conflictos?

El potencial práctico de estos hallazgos es inmenso. En contextos como la educación emocional, el coaching ejecutivo o la gestión de conflictos, disponer de herramientas digitales que comprendan y respondan emocionalmente puede transformar la manera en que formamos a los profesionales del futuro.

Imaginemos por un momento asistentes virtuales que no solo nos recuerden nuestras tareas, sino que también sepan cuándo estamos estresados, tristes o desmotivados, y nos sugieran estrategias emocionales adaptadas. O plataformas educativas que ajusten el contenido en función del estado anímico del alumno. Incluso en el mundo empresarial, la inteligencia emocional artificial podría servir como una brújula emocional para líderes y equipos, ayudando a prevenir crisis o mejorar la cohesión del grupo.

Eso sí, los propios investigadores advierten que el uso de estos modelos debe estar siempre supervisado por profesionales humanos. Aunque la IA puede ser una herramienta poderosa, su integración en ámbitos sensibles como la psicología debe hacerse con prudencia, ética y un control riguroso.

Uno de los puntos más fascinantes de este estudio es que pone en entredicho el concepto tradicional de empatía. Si una máquina es capaz de identificar una emoción, prever su impacto y sugerir la mejor forma de gestionarla, ¿no es eso, en cierto modo, empatía funcional?

Quizás no sea una empatía sentida —la IA no experimenta emociones— pero sí una empatía útil, capaz de generar resultados positivos. En un mundo cada vez más automatizado, esta "empatía algorítmica" podría no solo complementar la interacción humana, sino mejorarla en ciertos entornos donde los sesgos, las emociones desbordadas o la falta de autoconocimiento son frecuentes.

Una brecha que se reduce… o se invierte

En definitiva, los resultados del estudio no solo rompen un paradigma, también plantean preguntas inquietantes: ¿seguiremos siendo los humanos los mejores en gestionar lo humano? ¿Podrá la IA enseñarnos a nosotros mismos a ser emocionalmente más inteligentes?

Lo que antes parecía ciencia ficción ahora es un campo de estudio concreto. Y lo más probable es que esta investigación no sea un punto final, sino el comienzo de una nueva era en la que la inteligencia emocional —tan escurridiza hasta ahora— se convierta en algo que las máquinas pueden entender, evaluar y mejorar.

No es que las máquinas sientan, pero tal vez empiecen a enseñarnos a sentir mejor.