Notas de Electrónica					
Título:	Pagos digitales: al cierre de 2025 se realizarán casi 2 mil millones de operaciones				
Encabezado:					
Fecha:	07/10/25	Fuente:	CONSUMOTIC	Por:	Juan Carlos Villarruel
Link:	https://consumotic.mx/ecommerce/medios_de_pago/pagos-digitales-al-cierre-de-2025-se-realizaran-casi-2-mil-millones-de-operaciones/#google_vignette				

Al finalizar el presente año, el número de operaciones de pago sin efectivo en todo el mundo podría llegar a mil 976 millones 900 mil, en tanto para finales del 2029 la proyección es que asciendan a 3 mil 540 millones 300 mil, adelantó Iván Uriza, director de Pagos de Capgemini para el Norte de América Latina.

Al presentar en conferencia de prensa el "Informe Mundial de Pagos 2026", explicó que "el campo de juego se está moviendo mucho; se está redefiniendo en todo el mundo y en particular en América Latina, donde los bancos, las fintechs y las paytechs (empresas especializadas en procesar transacciones en línea), lejos de competir, se complementan cada día más".

En su edición número 21, el reporte revela la difícil situación de los bancos que si bien gozan de 66 por ciento de confianza de los comercios para proveerles todos sus servicios financieros, los niveles de satisfacción indicados por los pequeños comercios sólo llega a 15 por ciento y entre los medianos comercios a 22 por ciento.

A partir de una encuesta levantada entre 2 mil 600 comercios a nivel mundial y 420 ejecutivos de pago (210 de bancos y 210 de jugadores de paytechs), de los cuales un tercio se ubican en América Latina, se conoció que los bancos están tratando de lidiar con los pagos digitales con enfoques distintos, desde desarrollar sus propias estructuras, hasta delegar el negocio en otros expertos.

El documento incluyó entrevistas a 267 pequeños comercios; 486 medianos y 122 grandes en América Latina, y encontró que 70 por ciento de los comercios valora las altas tasas de éxito en pagos al igual que la confiabilidad del entorno digital.

Una vez más, los bancos enfrentan una brecha porque sólo 19 por ciento de ellos confía en su propia capacidad para ofrecer estos servicios, en tanto 69 por ciento de los comercios demanda procesos de incorporación más rápidos y fluidos, es decir, que los pagos pasen rápido y los vean reflejados en su tesorería de manera ágil.

Es tan importante que los habilitadores de pagos digitales ya sean fintechs, paytechs o bancos ofrezcan a sus clientes que el pago se refleje pronto en su Tesorería, que los comercios incluso están dispuestos a asumir comisiones más altas, con tal de que el dinero fluya rápido, aunque también está creciendo la tendencia de soluciones que sólo cobran por transacción.

De acuerdo con Iván Uriza, esto significa que "los comercios buscan soluciones de cobro digital que sólo generen pagos cuando se haga una transacción y no por una especie de 'renta' durante el tiempo que se tenga la tecnología en el negocio, pues no quieren pagar por algo que no estén usando".

Para los comercios son relevantes las tasas de éxito en los pagos y la confiabilidad del entorno digital (70 por ciento) y sólo 19 por ciento de los bancos confía en su propia capacidad para ofrecer estos servicios, en tanto 13 por ciento de los ejecutivos bancarios considera que sus instituciones son completamente capaces de ofrecer este servicio.

El informe también destaca los principales retos que plantea la incorporación de comercios a los bancos, que puede llevar hasta siete días y tener un costo promedio de hasta 496 dólares en promedio mundial. Por el contrario, las paytech permiten a los comercios empezar a operar en menos de 60 minutos por tan solo 214 dólares en promedio.

En el mismo encuentro Walter Adriani, vicepresidente de Servicios Financieros de Capgemini para el Norte de América Latina, destacó que el informe se centra en la gestión de pagos en los comercios, donde el cliente llega y paga con su tarjeta, pero esa tarjeta entra en interacción con una terminal y luego el banco recibe el dinero, cosas que son importantes para el negocio de las empresas financieras.

“Este año tenemos el foco puesto ahí, porque los bancos parece que están perdiendo relevancia en ese lugar, porque otras soluciones de pago digital (entre ellos las llamadas paytech), son más ágiles y económicas, aunque los detalles del estudio cuentan una historia más completa”.

En ese sentido, Iván Uriza señaló que 70 por ciento de las paytech han implementado orquestación de pagos, un factor clave para el enrutamiento inteligente de las transacciones en comparación con sólo 47 por ciento de los bancos. Las instituciones financieras que no ofrecen directamente esos servicios, por lo general recurren a terceras empresas especializadas.

Respecto a la adopción de tecnologías, 41 por ciento por ciento de los bancos ha adoptado Inteligencia Artificial generativa para sus operaciones, contra 60 por ciento de los nuevos participantes, típicamente nativos digitales.

En este tema, Wagner Simao, Asociado de Banca de Capgemini para el Norte de América Latina, dijo que hay un conjunto de soluciones que se están implementando para facilitar los pagos digitales que van desde las APIs y la tokenización, hasta la identidad digital, a las cuales los bancos y las paytech les están dedicando inversiones importantes.

“Todos los jugadores del ecosistema están poniendo mucho énfasis en la ciberseguridad que es un tema muy importante para todos, en especial para la prevención del fraude, donde hay un área importante de mejora”.

Sólo 26 por ciento de los ejecutivos bancarios expresan confianza en ofrecer prevención avanzada de fraude y seguridad de datos. Los comercios sienten esta presión de manera significativa, reportando pérdidas de aproximadamente 2.0 por ciento de los ingresos totales por fraude en pagos, y hasta nueve horas de inactividad anual debido a sistemas poco confiables.

Notas de Electrónica					
Título:	Sector turismo enfrentaría pérdidas millonarias por rechazo de tarjetas de crédito				
Encabezado:					
Fecha:	07/10/25	Fuente:	CONSUMOTIC	Por:	Redacción

Link:	https://consumotic.mx/ecommerce/medios_de_pago/sector-turismo-enfrentaria-perdidas-millonarias-por-rechazo-de-tarjetas-de-credito/

El sector turismo y las aerolíneas en particular, podrían perder hasta 117 mil millones de dólares en 2025, debido al rechazo de pagos de sus usuarios con tarjeta de crédito, lo cual provocaría que 13 por ciento de los viajeros cambie de proveedor y 5.0 por ciento abandone definitivamente la compra.

El estudio “Los desafíos de la industria turística global en materia de pagos digitales” elaborado por Nuvei, empresa financiera de base tecnológica (Fintech), señala que 92 por ciento de los usuarios exige procesos de compra ágiles, en tanto 59 por ciento desea utilizar su método de pago preferido.

Según el documento, elaborado en conjunto con el despacho Edgar, Dunn & Company, destaca también la relevancia de este tema de cara al Mundial de Futbol 2026, que organizan conjuntamente Estados Unidos, Canadá y México, porque la madurez del sistema de pagos digitales en nuestro país, difiere respecto a otras naciones.

“En muchos mercados, los métodos de pago digitales y locales ya dominan las preferencias del consumidor. En Brasil, por ejemplo, 71 por ciento de los viajeros prefiere utilizar Pix, mientras en Hong Kong, 29 por ciento opta por AlipayHK”.

En la misma línea, 23 por ciento de los viajeros de España usa Bizum; en Reino Unido 40 por ciento usa PayPal y en Estados Unidos lo hace 41 por ciento de los paseantes, lo que “subraya la importancia de que México amplíe la aceptación de distintas soluciones”.

Sin embargo, en el caso de México la adopción no tiene los mismos niveles y se siguen presentando algunos retos para los pagos en línea desde la falta de conectividad, hasta la dificultad de los pequeños negocios a acceder a servicios financieros que les permitan recibir pagos digitales.

A su vez, según el Informe Mundial de Pagos 2026 de Capgemini, 66 por ciento de los pequeños negocios en América Latina se encuentran en el primer nivel –funcional operativo—de los pagos en línea y esperan que los sistemas que contratan para recibir pagos en línea les permitan hacerlo en todos sus canales, de manera ágil y con seguridad.

Por ejemplo, uno de los principales puntos de fricción identificados es la falta de opciones para dividir los pagos. Aunque 75 por ciento de los viajeros manifiesta interés en combinar distintos métodos de pago —como una tarjeta bancaria junto con millas o puntos de fidelidad— sólo 22 por ciento de las agencias de viaje en línea ofrece actualmente esta posibilidad.

Esta brecha entre la oferta y las expectativas del consumidor representa una oportunidad importante para mejorar la conversión de ventas y la retención de clientes.

También llama la atención que ocho de cada 10 usuarios (82 por ciento) que enfrentan a alguna falla al hacer su pago en línea, intentarán complementar su compra de otra forma, pero si no lo consiguen, el impacto es claro, ya sea por cambio de proveedor o abandono de la transacción.

En ese sentido, y debido a que México será anfitrión en 2026 de un evento de alcance mundial, es necesario trabajar para disminuir en lo posible las brechas tecnológicas y operativas, que dificultan los pagos digitales en el sector turismo.

De ahí que Nuvei señala la relevancia de la llamada orquestación inteligente de transacciones, es decir, aplicar un sistema que facilite a los comercios recibir todas las formas de pago.

Al implementar soluciones como soporte con métodos de pago locales, transferencias inmediatas y pagos con billeteras electrónicas, se puede incrementar la tasa de aceptación, lo que redunda en disminuir los abandonos en los intentos de pago y mejora la experiencia de los clientes.

El Informe Mundial de Pagos de Capgemini indica que el uso de billeteras digitales en el mundo alcanzó 53 por ciento de los usuarios el año pasado y podría llegar a 65 por ciento hacia el 2030.

Si se tiene en cuenta que muchos de los viajeros que vendrán para el Mundial de Futbol de 2026 provienen de mercados donde los pagos digitales son dinámicos y casi todos los negocios ofrecen distintas opciones, es muy relevante para las empresas del sector turismo que revisen sus sistemas y se actualicen con las tecnologías que permitan todo tipo de operaciones.

Notas de Electrónica					
Título:	Maestría en Dispositivos Semiconductores de BUAP, celebra 40 años de trabajo científico				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	ANGULO 7	Por:	Arely Sánchez Delgado
Link:	https://www.angulo7.com.mx/2025/educacion/maestria-en-dispositivos-semiconductores-celebra-40-anos/649650/?amp=1				

La Benemérita Universidad Autónoma de Puebla (BUAP) informó que los programas de maestría y doctorado que se imparten en el Centro de Investigaciones en Dispositivos Semiconductores (CIDS) del Instituto de Ciencias de la universidad (Icuap), cumplen 40 años de trabajo.

Ambas especializaciones son reconocidas por el Sistema Nacional de Posgrados de la Secretaría de Ciencia, Humanidades, Tecnología e Innovación (Secihti).

La maestría en Dispositivos Semiconductores inició actividades en mayo de 1986 y en 1988 se incorporó al Padrón de Excelencia del entonces Conacyt; mientras que, el doctorado entró en funciones en 2006, luego de que el Consejo Universitario lo aprobara el 19 de mayo de 2005.

El CIDS celebra sus cuatro décadas de labores, pues desde junio de 1985 ha egresado a 55 generaciones y titulado a 198 alumnos a través de los estudios de posgrado.

Logros de la maestría y doctorado en Dispositivos Semiconductores
A la par de la aprobación del doctorado en 2005, se puso en marcha el difractómetro de rayos X, equipo necesario para la caracterización de los materiales que potencialmente pueden actuar como semiconductores.

En 1987, un año después de la creación de la maestría en Dispositivos Semiconductores, se diseñó un prototipo electro-estimulador funcional para rehabilitación de personas hemipléjicas, un estimulador de campo magnético para el tratamiento de fracturas óseas y un oxigenador de sangre.

Luego, en 1988, el centro incursionó en el diseño, desarrollo, construcción y aplicación de equipo de hipertemia para pacientes oncológicos atendidos en el Departamento de Radioterapia del Hospital de Especialidades del IMSS en Puebla.

En 1992, en los programas de maestría y doctorado, se fabricó el primer dispositivo laser semiconductor de arseniuro de galio; así como, tecnología para la elaboración de circuitos integrados en baja escala de integración y prototipos de mano electromecánica, de laringe electrónica y de marcapasos externo. Además, se crearon interfaces para el tratamiento y diagnóstico de alteraciones del lenguaje.

¿En qué trabaja el CIDS actualmente?
Para 2023, el CIDS se vinculó a una propuesta científica que involucra a varios laboratorios nacionales, titulada “Innovación y desarrollo de prototipos de módulos fotovoltaicos a partir de celdas solares experimentales”, proyecto perteneciente al Laboratorio Nacional de Innovación Fotovoltaica y Caracterización de Celdas Solares (Lifycs) del IER-UNAM.

Notas de Electrónica					
Título:	Panamá en SEMICOM West, cumbre de la innovación y de la industria de semiconductores en Arizona				
Encabezado:	La Comisión de Innovación en Microelectrónica y Semiconductores estará presente en este evento con la visión de presentar al país como «el nuevo centro para la innovación global en semiconductores»				
Fecha:	06/10/25 (por la tarde)	Fuente:	LA WEB DE LA SALUD	Por:	
Link:	https://lawebdelasalud.com/panama-en-semicom-west-cumbre-de-la-innovacion-y-de-la-industria-de-semiconductores-en-arizona/				

Panamá reforzará su proyección en la industria de semiconductores, con la participación en SEMICOM West, en el Centro de Convenciones de Phoenix, en Arizona (Estados Unidos), la principal exposición de microelectrónica en Norteamérica, del 7 al 9 de octubre.

La industria de los semiconductores es la columna vertebral de la innovación moderna. Líderes de la industria, startups e investigadores se reunirán en Phoenix, Arizona, fomentando la colaboración, el intercambio de conocimientos, el desarrollo de talento y la inversión a largo plazo, en el contexto de un estado reconocido como centro de fabricación avanzada.

La Comisión de Innovación en Microelectrónica y Semiconductores estará presente en este evento con la visión de presentar al país como «el nuevo centro para la innovación global en semiconductores».

Cuenta el país «con el respaldo de una estrategia nacional, alianzas internacionales y una conectividad inigualable, Panamá está construyendo la infraestructura, el talento y el ecosistema empresarial para albergar operaciones avanzadas de semiconductores, desde ensamblaje, prueba y empaque (ATP) hasta servicios de diseño y logística«.

Es un mensaje poderoso que se articula con las fortalezas históricas del país: posiciones de liderazgo en infraestructura logística, sólido sistema financiero y condiciones de estabilidad política y jurídica para operar negocios.

Nuevo comisionado de Microelectrónica y Semiconductores

Al respecto, ya fue nombrado el doctor Darío Solís Caballero como nuevo comisionado nacional de la Industria de Microelectrónica y Semiconductores de Panamá (adscrito a la Secretaría Nacional de Ciencia, Tecnología e Innovación), de acuerdo con el anuncio reciente del doctor Eduardo Ortega Barría, secretario nacional de la Senacyt.

El doctor Solís resultó electo de una terna propuesta al presidente de la República, José Raúl Mulino, por la Comisión de Innovación en Microelectrónica y Semiconductores, la cual es presidida por el ministro de Comercio e Industrias, Julio Moltó. El secretario nacional de Senacyt forma parte de dicha comisión.

El nuevo comisionado tiene una amplia combinación de credenciales académicas, competencias comerciales y experiencias con el desarrollo de la ciencia y la tecnología para apoyar la innovación. También, en el área de financiación competitiva y apoyo externo para investigación y desarrollo. Además, ha estado inmerso en la captación y desarrollo del talento de individuos y equipos científicos.

De igual forma, el doctor Solís tiene experiencia en forjar y fomentar asociaciones de investigación científica y desarrollo tecnológico (I+D) multisectoriales y multidisciplinarias, crear, conducir y dirigir proyectos de energía, transporte, logística, ingeniería, análisis, diseño y optimización.

Su hoja de vida destaca como director general del Centro de Innovación e Investigación Logística de Georgia Tech Panamá, así como asesor del rector de la Universidad Tecnológica de Panamá (UTP) en iniciativas estratégicas en investigación, innovación y desarrollo. Ha sido director de investigación, profesor de ingeniería mecánica y eléctrica en la UTP, entre otros.

Darío Solís Caballero se desarrolló como científico investigador senior del Simulador Nacional de Conducción Avanzada en la Universidad de Iowa. Fungió como jefe de la División de Modelado y Simulación.

En el sector privado fue presidente de Verde Power Corporation, S.A., consultor de Estrategia de Desarrollo de Negocios e Innovación, director de Austral Ingeniería y Software Inc., entre otros cargos.

El comisionado Solís realizó estudios de licenciatura en Ingeniería Electromecánica, como becario Fulbright. Tiene maestría en Ingeniería Mecánica. Es doctor en Ingeniería Mecánica. Fue el primer doctor de la rama de modelado y simulación del National Advanced Driving Simulator.

El Dr. Solís ha publicado en seis journals, ocho reportes técnicos, nueve publicaciones en conferencias; además, ha dictado y participado en conferencias científicas, semanarios y talleres a nivel nacional e internacional.

El nuevo Comisionado Nacional de la Industria de Microelectrónica y Semiconductores de Panamá deberá cumplir con importantes roles. Primero, de representación comercial y atracción de inversiones en el sector de semiconductores para Panamá; segundo, interactuar, coordinar y consensuar los esfuerzos e intereses de las entidades que integran la Comisión Nacional de Semiconductores y Microelectrónica; tercero, gestor de proyectos, dando seguimiento y asegurando el cumplimiento de todas y cada una de las acciones y compromisos que las dependencias y entidades de la Comisión asuman ; y cuarto, representación nacional e internacional del sector de semiconductores de Panamá.

Notas de Electrónica					
Título:	Taiwan Semiconductor alcanza récord por auge de IA y acuerdos con AMD y OpenAI				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	FINANZAS YAHOO	Por:	Anusuya Lahiri
Link:	https://es-us.finanzas.yahoo.com/noticias/taiwan-semiconductor-alcanza-r%C3%A9cord-auge-181334619.html				

Taiwan Semiconductor Manufacturing Co (NYSE:TSM) superó su máximo en 52 semanas de 196,72 dólares el lunes, ya que la continua fiebre de la inteligencia artificial fomentó el optimismo de los inversores.

El cliente clave Advanced Micro Devices (NASDAQ:AMD) anunció un acuerdo histórico con OpenAI para suministrar hasta 6 gigavatios de las GPU Instinct de AMD para impulsar la infraestructura de próxima generación del líder de la IA.

El despliegue está programado para comenzar en el segundo semestre de 2026 con un despliegue de 1 gigavatio de GPU MI450, seguido de expansiones en varias fases a lo largo de las futuras generaciones de chips de centros de datos de AMD.

El director financiero Jean Hu dijo que el acuerdo podría generar “decenas de miles de millones de dólares en ingresos” y ser “altamente acumulativo” para las ganancias.

Las acciones de AMD subieron un 33,6 % a 219,99 dólares, superando su máximo de 52 semanas de 186,65 dólares. El acuerdo sigue a la asociación de 100.000 millones de dólares de Nvidia (NASDAQ:NVDA) con OpenAI para desplegar al menos 10 gigavatios de sistemas Vera Rubin a partir de 2026. Nvidia es también un cliente clave de Taiwan Semiconductor.

El fabricante taiwanés de chips por encargo también encabezó un repunte récord en el mercado de valores de Taiwán el lunes, ya que el entusiasmo por el desarrollo de la IA llevó al TAIEX a nuevos máximos.

Los analistas dijeron que los inversores vieron a Taiwan Semiconductor con un valor atractivo en comparación con el fabricante de chips estadounidense Nvidia (NASDAQ:NVDA), cuyo stock se ha disparado debido a la creciente demanda de la IA.

El analista de Hua Nan Securities, Kevin Su, dijo al Taipei Times que el repunte de Taiwan Semiconductor reflejó la creencia de los inversores de que sigue siendo fundamental para la cadena de suministro mundial de IA como el mayor fabricante de chips por encargo del mundo que produce los avanzados procesadores de Nvidia.

La oleada de compras se extendió a otros nombres prominentes en el sector de los semiconductores.

Su señaló que los inversores están atentos a nuevas señales de Washington, ya que Estados Unidos se prepara para publicar los datos de nóminas no agrícolas de septiembre, que podrían influir en los próximos movimientos de la Reserva Federal en recortes de tasas de interés.

Rendimiento de las acciones de Taiwan Semiconductor
Las acciones de TSM cotizaban un 4,69 % más a 305,90 dólares en la última revisión del lunes.

Notas de Telecomunicaciones					
Título:	T-MEC y telecom, “la piedra en el zapato” de Sheinbaum				
Encabezado:					
Fecha:	07/10/25	Fuente:	CONSUMOTIC	Por:	Guadalupe Michaca
Link:	https://consumotic.mx/opinion/t-mec-y-telecom-la-piedra-en-el-zapato-de-sheinbaum/#google_vignette				

“No hace sentido pensar en extender el Tratado cuando los mexicanos ni siquiera están cumpliendo en partes importantes del mismo”, asestó recientemente Jamieson Greer, representante comercial de Estados Unidos, al tiempo que señaló al sector mexicano de las telecomunicaciones como uno de los puntos de mayor inconformidad, pero ¿qué de todo lo que por acción u omisión se ha hecho le preocupa a nuestro socio?

Con 27 artículos específicos para el sector telecom, el Capítulo 18 del Tratado entre México, Estados Unidos y Canadá (T-MEC), establece disposiciones que se han pasado por alto, pues hoy no se cuenta con un organismo regulador independiente, la competencia económica efectiva sigue siendo una quimera, de una u otra forma se abrió la puerta a un trato preferencial a empresas del Estado, y por si fuera poco, es clara la existencia de barreras no arancelarias para los exportadores estadounidenses, como por ejemplo los costos discriminatorios para el acceso al espectro radioeléctrico.

La preocupación de Estados Unidos en torno al sector telecom, no es un fenómeno de generación espontánea avivado por la cercanía de la negociación del tratado comercial con México, sino producto de una serie de decisiones que comenzaron a dibujarse con el ex presidente Andrés

Manuel López Obrador (2018-2024), pero que se están materializando peligrosamente en el actual gobierno de la presidenta Claudia Sheinbaum. a AMLO le tocó celebrar en julio de 2020 la entrada en vigor de un nuevo acuerdo, -resultado de una renegociación completa del Tratado de Libre Comercio de América del Norte (TLCAN) que estuvo vigente por más de dos décadas-, con un socio aún dispuesto a escuchar, pues la desaparición del Instituto Federal de Telecomunicaciones (IFT) no era más que un deseo arengado por el mandatario en sus conferencias.

Aunque el terreno de competencia en el sector telecom no ha logrado estar parejo, la existencia del IFT enviaba un mensaje tranquilizador a Estados Unidos, y es que aún con una amplia gama de áreas de mejora, el regulador tenía la batuta regulatoria: reglas asimétricas al Agente Económico Preponderante en Telecomunicaciones (AEP-T), revisiones bienales sobre la efectividad de la regulación, ajustes y procesos de interlocución con la industria.

Hoy, el IFT está conectado a un respirador artificial: La nueva Ley en Materia de Telecomunicaciones y Radiodifusión ató la extinción de este órgano a la conformación de la Comisión Reguladora de Telecomunicaciones (CRT), que lejos de contar con autonomía real, fue diseñada para operar como una entidad desconcentrada dependiente de la Agencia de Transformación Digital y Telecomunicaciones (ATDT).

En pocas palabras: el IFT no termina de morir y la CRT no termina de nacer. Hablar de incertidumbre no es exagerado y menos aún con el mensaje claro y contundente que envió el gobierno de Estados Unidos apenas en septiembre pasado a través de su informe “National Trade Estimate” (NTE) 2025, sobre otra “piedra en el zapato”: los impagables costos del espectro radioeléctrico.

En ese documento, la Oficina del Representante Comercial de Estados Unidos (USTR, por sus siglas en inglés) refiere cómo el gobierno mexicano ha sido omiso ante la problemática que representan los derechos anuales por el uso del espectro radioeléctrico para los operadores de telecomunicaciones.

Y es que, pese a que cada año el Estado mexicano pierde más de 6 mil millones de pesos en recaudación por el uso del espectro, la propuesta de Ley Federal de Derechos 2026 que analiza el Congreso mexicano como parte del Paquete Económico (que debe quedar aprobado en noviembre próximo), repite la dosis de espectro caro aunque la narrativa busque verle el lado amable al hecho de que los operadores de telecomunicaciones deberán pagar las mismas cuotas a las que estuvieron expuestos en años anteriores, es decir, no habrá ajuste inflacionario.

En la práctica, la noticia no es tan buena si se observan los precios del espectro en México, contra las cuotas que se pagan en otros mercados, pues el precio total de este recurso, considerando el pago inicial o “guante” y los derechos anuales, supera 76 por ciento el “benchmark internacional, en todas las bandas ocupadas, con el mayor sobreprecio en las bandas AWS/PCS donde llega a 112 por ciento del estándar global (es decir, más del doble).

Más aún, en el caso de los derechos anuales, por sí solos, el sobreprecio en México en comparación con el mundo, es de 48 por ciento. En este escenario, como se ha escrito hasta el cansancio en este espacio, todos los involucrados pierden, incluyendo el propio Estado mexicano.

De cara a la revisión del T-MEC, el gobierno mexicano debe entender que el enredo regulatorio que armó en el sector telecom no sólo mantiene en vilo a una industria que no tiene condiciones para

invertir, sino que en el antes y durante el arranque formal del proceso de negociación en 2026, se estará sentando con un socio cuyo umbral de tolerancia es cada vez más reducido.

Y aunque "palo dado ni Dios lo quita", hay una luz al final del túnel: Dar un cambio de timón en materia de espectro colocando los precios de este recurso esencial para la economía digital al nivel de las referencias internacionales es algo que el Congreso puede analizar con seriedad y sin fobias, para responder con responsabilidad: ¿Vale la pena poner en riesgo un tratado comercial por un sector que bien podría ser el eslabón de oro para México?

Notas de Telecomunicaciones					
Título:	Conectividad, IA y data centers transformarán oportunidades de México ante revisión del T-MEC: Ciena				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	NOTICIAS YAHOO	Por:	Nicolás Lucas-Bartolo
Link:	https://es-us.noticias.yahoo.com/conectividad-ia-data-centers-transformar%C3%A1n-230350490.html				

El avance de la inteligencia artificial (IA) y otras nuevas tecnologías, como últimas innovaciones en conectividad de fibra óptica y 5G, prometen cambiar el panorama de los centros de datos y todo el ecosistema de infraestructura de conectividad tanto a nivel mundial como en México. En sus términos técnicos, la definición de estas tecnologías es seca, pero su significado, en cuanto economía y oportunidades de desarrollo para una empresa o un país, va mucho más allá.

Estas nuevas tecnologías que permitirán el desarrollo integral de la inteligencia artificial abrirán nuevas fronteras para varios sectores productivos de la economía, platicó el director de ventas regionales de Ciena para América Latina, Carlos Hernández.

El hecho de que México eleve a un siguiente nivel la automatización de sus parques industriales; que también haga más común la telemedicina o que las ciudades se vuelvan inteligentes por la gestión del tráfico y la eficiencia energética que posibilitará la aplicación de herramientas de IA con apoyo de otras tecnologías, como recientes desarrollos en conectividad de fibra óptica, es parte de lo que haría al país más atractivo a la inversión en los siguientes años.

Ciena es una empresa con especialidad en la conectividad de alta velocidad y automatización para redes de telecomunicaciones, y también para redes privadas de otras industrias. Ciena participó en el foro de telecomunicaciones Futurecom de São Paulo.

Un país como México podría robustecer todavía más sus procesos productivos, contó Carlos Hernández, con el respaldo de la inteligencia artificial, los centros de datos y la conectividad incrementada que le darán soporte, y otras innovaciones que están surgiendo en el mercado:

"Cuando hablamos de centros de datos, Brasil tiene prácticamente el 41% de los centros de datos en América Latina y México está en un segundo lugar, con el 39 por ciento. ¿Pero puede México hacer mucho más? Por supuesto que puede hacer más, definitivamente, por su propio contexto; y para todas sus industrias", dijo Hernández.

En México, las industrias representan aproximadamente el 28% del PIB nacional. El país ya es líder en subsectores como el automotriz, la electrónica, los textiles, la farmacéutica, la producción de alimentos y lo aeroespacial; también en la generación y distribución de energía; y en minería el nombre de México hace historia.

Pero aun con ello, el directivo de Ciena confía en que estas nuevas tecnologías pueden empujar todavía más hacia adelante el PIB de México, con una transformación digital de la economía.

Para Carlos Hernández, la inteligencia artificial, de la mano del desarrollo que se espera en términos de los centros de datos que prestarán la infraestructura tanto para su entrenamiento como para su utilización efectiva (inferencia) en aplicaciones tanto para usuarios como industriales, darán un "avance para recordar" en el sector industrial.

Además, con las bondades tecnológicas del cómputo al borde y el 5G, que significa una complementación de la alta velocidad con la baja latencia, la comunicación entre máquinas y el procesamiento inmediato de información, se posibilitará que más fácil que polos industriales del país sigan atractivos para la fabricación de productos.

Computación en el borde y centros de datos distribuidos

El empleo de equipos que permitan procesar los datos en el "borde" de la red, y por tanto, más cerca a los usuarios, tendrá un rol central, especialmente en aquellas aplicaciones que requieran muy baja latencia.

La propia naturaleza del cómputo al borde ahorra dinero a las entidades que valoren el uso de esa tecnología, explicó el directivo de Ciena.

De la misma manera, para atender los requerimientos de entrenamiento y empleo de aplicaciones de inteligencia artificial, se espera una mayor distribución geográfica de los centros de datos. Esta nueva arquitectura o distribución responderá a las nuevas necesidades tanto de consumo energético como de cercanía con los usuarios finales, entre otros aspectos. Y será clave conectar estos centros de datos distribuidos con redes de muy alta velocidad.

Esto también ocurre porque al reducirse la necesidad de que la información viaje desde y hacia una nube alojada en un centro de datos establecido en un territorio más lejano, también se reducen los costos operativos y los consumos de ancho de banda son menores para las empresas y gobiernos.

Así, "será crucial poner atención a que la capacidad de cómputo esté más cerca de los usuarios, cuando un país como México requiera de procesamiento de datos en tiempo real y de respuestas rápidas para mantenerse atractivo en la producción de bienes y servicios. Esto puede ser muy importante para las industrias tradicionales como la automotriz, pero también para los nuevos sectores que están creciendo rápidamente en México, como el de la salud o lo aeroespacial".

"México tiene un súper hub en centros de datos que es reconocido internacionalmente, que es Querétaro. ¿Por qué ha sido Querétaro? Por el hecho de que está cerca de la Ciudad de México y donde prácticamente están los centros de negocios, pero realmente en el futuro se van a tener que explotar otro tipo de aplicaciones. Entonces, será necesario la cercanía de los centros de datos para aprovechar todo el potencial de algunas aplicaciones que son sensibles a lo que es la latencia en industrias muy específicas como son la medicina o lo aeroespacial; muchas de ellas de valor

agregado. Esto puede ser muy relevante para un país como México en su contexto económico del corto plazo, ahora que parece que habrá cambios en sus relaciones comerciales con otros países", dijo Carlos Hernández.

"México, hoy en día, tiene un papel interesante en relación a telecomunicaciones, pero también la industria regional de América del Norte. Digo esto porque México, históricamente, en telecomunicaciones tenía un papel de conectividad a los Estados Unidos. Hoy en día, es la misma cosa, pero bastante más inversión en infraestructura dentro del país para data center, para la nube y para cómputo al borde y por eso hay bastante necesidad en desarrollar conectividad y no sólo por corredor de conectividad internacional (…) México sería una fuerza en las Américas, o más un apoyo a la fuerza económica de los Estados Unidos", acompañó Peter Wood, analista de investigación senior en TeleGeography.

Es por ello que el directivo de Ciena explicó que una tecnología con un nombre tan técnico y en su combinación con otras aplicaciones representa una oportunidad para asegurar la robustez de la infraestructura de telecomunicaciones y el avance de las economías hacia una nueva etapa.

El primer reto para comenzar a aprovechar el cómputo al borde con los centros de datos está en resolver los obstáculos sobre disponibilidad de abundante energía, un problema no único de México; y también hacia dónde comenzar a mirar como país para disponer de ese tipo de infraestructura:

"Ya está algo entendido que el cómputo al borde también mejora la seguridad de los datos, porque ahora los datos pueden procesarse así en sitios más cercanos, sin que tengan que recorrer mayores distancias. El obstáculo es la disponibilidad de energía y de terrenos, es lo que recomendamos a los distintos países. Hace poco hubo un panel donde hubo ese tipo de discusiones, sobre dónde deben ponerse. Es algo que México también debe valorar; es un asunto de diversificación, porque también están los cables submarinos que están empezando a tocar más al país".

Notas de Telecomunicaciones					
Título:	Ericsson se consolida como líder en infraestructura 5G RAN en el Cuadrante Mágico de Gartner 2025				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	PANAMA 24 HORAS	Por:	Redacción
Link:	https://www.panama24horas.com.pa/empresas/ericsson-lider-gartner-infraestructura-5g-ran-2025/				

Ericsson (NASDAQ: ERIC) fue reconocido por quinto año consecutivo como Líder en el Cuadrante Mágico™ de Gartner® 2025 para soluciones de infraestructura 5G RAN para proveedores de servicios de comunicaciones (CSP), logrando la posición más alta en Capacidad de Ejecución.

Gartner nombra a Ericsson líder en soluciones de infraestructura 5G RAN por quinto año consecutivo
• El informe de Gartner, publicado en septiembre de 2025, subraya la visión integral y la sólida ejecución de Ericsson en el despliegue de tecnología 5G a nivel global, un sector donde la compañía impulsa casi la mitad del tráfico móvil 5G fuera de China.

(06/Oct/2025 – web – Panama24Horas.com.pa) Ciudad de Panamá, Panamá.- Ericsson (NASDAQ: ERIC) ha sido oficialmente reconocido como Líder en el Cuadrante Mágico™ de Gartner® 2025 para soluciones de infraestructura 5G RAN para Proveedores de Servicios de Comunicaciones (CSP). Este es el quinto año consecutivo que la compañía sueca se posiciona en el cuadrante de Liderazgo, destacando por obtener la clasificación más alta en el eje de "Capacidad de ejecución" del informe.

Evaluación y Posicionamiento de Ericsson

El informe de Gartner, publicado el 10 de septiembre de 2025, proporciona una evaluación exhaustiva e independiente de las capacidades de infraestructura de la Red de Acceso de Radio (RAN) 5G, valorando a los proveedores en función de dos índices principales: la integridad de la visión y la capacidad de ejecución.

Per Narvinger, Vicepresidente Ejecutivo y Director de Redes de Ericsson, manifestó que el reconocimiento continuo es un reflejo de los esfuerzos de la compañía para evolucionar y apoyar las necesidades de sus clientes. "Creemos que este reconocimiento continuo no se trata solo de ampliar los límites de la tecnología, sino de ayudar a los proveedores de servicios a construir las redes del futuro," señaló Narvinger.

Liderazgo Global y Despliegue de Redes

El liderazgo de Ericsson en el mercado se traduce en cifras concretas, ya que aproximadamente la mitad del tráfico móvil 5G mundial, excluyendo a China, se canaliza a través de redes impulsadas por la compañía. En un contexto donde la GSA reporta alrededor de 300 redes 5G en servicio comercial a nivel mundial, Ericsson cuenta con 187 redes 5G en vivo en 78 países, de las cuales más de 40 son redes 5G independientes (SA).

Adicionalmente, la tecnología de Ericsson permite la modernización de sitios 4G heredados a 5G, logrando una capacidad diez veces superior y hasta un 30 por ciento de ahorro de energía.

Innovación y Evolución de la Tecnología 5G

El liderazgo de Ericsson en la infraestructura 5G RAN ha sido consistentemente reconocido por la industria. Además de Gartner, la compañía fue nombrada líder en el informe Frost Radar: 5G Network Infrastructure, 2025 de Frost & Sullivan por quinto año consecutivo, y logró la clasificación más alta en el reciente informe Omdia Market Landscape RAN Vendors 2025.

La compañía evoluciona de manera continua sus carteras de productos, incluyendo 5G RAN con Ericsson Radio System, Cloud RAN y 5G Transport, además de sus servicios profesionales. Su hardware incorpora radios Massive MIMO y multibanda compactas y de bajo consumo, impulsadas por su silicio personalizado de última generación y preparadas para Open RAN.

En el ámbito del software, las soluciones avanzan con la automatización basada en la intención y funciones impulsadas por Inteligencia Artificial (IA). Su suite 5G Advanced incluye funciones de ahorro de energía automatizado y adaptación de enlaces nativa de IA, mejorando tanto el rendimiento como la eficiencia de la red.

Compromiso con la Sostenibilidad

Ericsson ha alcanzado sus objetivos de sostenibilidad para su portafolio de productos de 2025, logrando esta meta seis meses antes de lo programado. En un esfuerzo por asistir a los clientes con los costes crecientes y los objetivos de cero emisiones netas, la compañía ha reducido el consumo

de energía en sus nuevas estaciones base de radio en un 40% en comparación con los niveles de 2021. También disminuyó las emisiones de la cadena de suministro al reducir el peso del producto en un 45% respecto a los puntos de referencia de 2020.

Notas de Telecomunicaciones					
Título:	Nuevo campus de investigación de Huawei llegará a 35 mil trabajadores a fines de 2026				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	PORTAL INNOVA	Por:	
Link:	https://portalinnova.cl/nuevo-campus-de-investigacion-de-huawei-llegara-a-35-mil-trabajadores-a-fines-de-2026/				

Se trata del Centro de I+D LianQiu Lake, ubicado en las inmediaciones de Shanghái, que entró en operaciones a fines de 2024, posicionándose como el más grande de la empresa. Este, se suma a los de menor tamaño situados en Shenzhen, Beijing, Guangzhou y Wuhan.

6 de octubre. Santiago, Chile.-Su extensión equivale a unas 160 canchas centrales del Estadio Nacional de Chile: hablamos del Centro de Investigación y Desarrollo (I+D) LianQiu Lake del gigante tecnológico Huawei, ubicado en las afueras de Shanghái, que está operativo desde fines del año pasado y llegará a plena capacidad al cierre de 2026, con 35 mil trabajadores.

¿Por qué la empresa decidió construir esta nueva ciudadela dedicada por completo a la creación, desarrollo y pruebas de nuevas soluciones? La respuesta la entregó el fundador de Huawei, Ren Zhengfei, quien supervisó personalmente las obras: “Nuestro objetivo es crear un ambiente propicio para que los científicos extranjeros trabajen y vivan. Beneficios como 100 cafeterías y una mejor infraestructura atraerán aún más a jóvenes talentos del extranjero”.

El campus de 160 hectáreas, es decir más grande que la suma de los centros de operaciones Apple Park (71 hectáreas) y Microsoft Redmond Campus (74 hectáreas), se completó en solo 4 años, y cuenta con un tranvía con ocho estaciones para el traslado de los trabajadores entre los más de 180 edificios que componen LianQiu Lake.

Más allá del deseo de Ren Zhengfei de atraer profesionales foráneos, la millonaria inversión en dichas instalaciones -cerca de US$ 1.400 millones- está en línea con el crecimiento y diversificación de negocios de la tecnológica, que hoy es líder mundial en infraestructura de telecomunicaciones y soluciones digitales inteligentes. En los últimos 5 años, ha destinado más del 20% de sus ingresos anuales a Investigación y Desarrollo, equivalente a más de US$ 24 mil millones el año recién pasado y a sobre US$ 22 mil millones en 2023. En paralelo, a fines de 2024, Huawei tenía más de 150 mil patentes activas y se ha mantenido por 8 años consecutivos como el mayor solicitante de patentes a nivel global.

Ejes del nuevo campus

Las amplias instalaciones de LianQiu Lake -desplegadas en torno a una laguna y en medio de jardines y praderas- incluyen decenas de laboratorios, aulas, oficinas, cafeterías, salas de ensayos, auditorios, espacios de exhibición de tecnologías y numerosas zonas de ocio. Actualmente, se trabaja en los detalles finales de algunas de ellas, mientras que cerca de 28 mil investigadores ya

están laborando, al igual que las 3 mil personas destinadas exclusivamente al mantenimiento y atención de servicios.

Respecto a las actividades de investigación que ya se desarrollan en el lugar, desde la empresa han indicado que abarcan todo tipo de proyectos. Desde nuevos dispositivos inteligentes y chips a automóviles eléctricos, pasando por Data Centers, aplicaciones, infraestructura para 5G y 5G Avanzado, entrenamiento de Inteligencia Artificial, redes wireless y tecnologías para transformar energía fotovoltaica en eléctrica, por citar algunos.

Diferencias y similitudes con Dongguan
Hasta antes de la inauguración de LianQiu Lake, el corazón de las investigaciones de Huawei estaba situado en el campus de Ox Horn, en Dongguan, a algunos kilómetros de la casa matriz en Shenzhen. Sin embargo, dicho centro con sus 25 mil trabajadores queda en el segundo lugar en tamaño -tras las nuevas dependencias de Shanghai-, seguido por los polos de I+D en Beijing, Guangzhou, Nanjing y Wuhan.

No solo el tamaño diferencia a los distintos campus, sino también su estilo. Mientras el más nuevo tiene aires modernos mezclados con reminiscencias orientales y hasta japonesas (el arquitecto encargado es de dicha nacionalidad), en Dongguan conviven réplicas de universidades y centros culturales de Europa, con símiles perfectos de hitos ubicados en 12 ciudades como Oxford, Bologna, Heidelberg y París, entre ellas. El espacio físico es diferente, pero lo que no cambia es la premisa de trabajo de los investigadores de Huawei: contribuir con tecnología de vanguardia para un mundo más conectado, más inteligente y más verde.

Notas de Telecomunicaciones					
Título:	Límite de gasto, saldo que no expira y cancelación fácil: así es la nueva iniciativa para tu plan celular en México				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	XATAKA	Por:	Gonzalo Hernández
Link:	https://www.xataka.com.mx/telecomunicaciones/limite-gasto-saldo-que-no-expira-cancelacion-facil-asi-nueva-iniciativa-para-tu-plan-celular-mexico				

Un diputado de Movimiento Ciudadano propone reformar la manera en que funcionan los planes y servicios de telefonía móvil en México. Entre sus propuestas destacan establecer límites de gasto definidos por el usuario, cancelar un contrato sin penalización si el servicio es deficiente y retomar la premisa de que el saldo no utilizado se conserve.

Estas son algunas de las modificaciones que el diputado Pablo Vázquez Ahuet, del partido Movimiento Ciudadano, busca implementar en el artículo 185 de la Ley Federal de Telecomunicaciones y Radiodifusión, con el objetivo de fortalecer los derechos de los consumidores y usuarios de telefonía móvil.

La iniciativa, que ya fue turnada a la Comisión de Comunicaciones y Transportes para su discusión, busca como primer punto que el usuario pueda fijar un límite máximo de consumo. Este sería un derecho en los servicios móviles, independientemente de la modalidad del contrato, para evitar cobros adicionales a los planteados originalmente, sin que el ajuste represente un costo extra.

La propuesta también contempla que el usuario pueda cancelar su contrato sin ninguna sanción si considera que el servicio de telecomunicaciones no cumple con los índices de calidad establecidos en los lineamientos de la Comisión Reguladora de Telecomunicaciones. En dicho caso, únicamente deberá cubrir los adeudos pendientes.

Además, la propuesta establece que, una vez que termina el contrato o se liquida el costo de un equipo, el usuario podrá solicitar su desbloqueo de forma inmediata y por medios electrónicos, sin necesidad de acudir a una sucursal para realizar el procedimiento.

La iniciativa de Vázquez Ahuet también retoma una propuesta sugerida previamente por otros legisladores, que involucra que los saldos no consumidos, tanto del plan principal como de paquetes complementarios, se reintegren al cliente en el siguiente ciclo de facturación. En otras palabras, si a un usuario le sobran datos o saldo al final del mes, estos se podrían transferir al mes siguiente, siempre y cuando sea técnicamente posible.

Las quejas de los usuarios como motor del cambio
De acuerdo con el comunicado oficial de la Cámara de Diputados, uno de los principales motivos para estas modificaciones son los reportes del IFT, que señalan un gran número de inconformidades presentadas por los usuarios. Entre ellas destacan fallas en el servicio, problemas con cargos, cobros y bonificaciones.

Para la elaboración de la iniciativa también se consideró información sobre portabilidad, el incumplimiento de publicidad o promociones, las negativas de las compañías para desbloquear celulares, los cambios de planes o paquetes sin previo aviso, el incumplimiento de garantías sobre los equipos y las modificaciones de contrato sin consentimiento del usuario.

Notas de Telecomunicaciones					
Título:	Ley Kuri fue modificada por cambios a la Ley de Telecomunicaciones: Senadores del PAN				
Encabezado:	Los senadores queretanos Guadalupe Murguía y Agustín Dorantes destacaron que la iniciativa es respaldada por legisladores de distintos partidos y organismos internacionales				
Fecha:	06/10/25 (por la tarde)	Fuente:	PLAZA DE ARMAS	Por:	Francisco Segura
Link:	https://plazadearmas.com.mx/ley-kuri-fue-modificada-por-cambios-a-la-ley-de-telecomunicaciones-senadores-del-pan/				

Los senadores por Querétaro del Partido Acción Nacional (PAN), Guadalupe Murguía Gutiérrez y Agustín Dorantes Lámbarri informaron sobre los avances en la implementación y fortalecimiento de la llamada “Ley Kuri”, que busca regular el uso de dispositivos electrónicos y redes sociales por parte de menores de edad, con el objetivo de prevenir riesgos digitales como el grooming, el bullying y el sexting.

El senador Agustín Dorantes explicó que la iniciativa tuvo que adaptarse a las modificaciones aprobadas en el Congreso de la Unión sobre la Ley de Telecomunicaciones, sin embargo, destacó que estos cambios ayudaron a abonar la iniciativa impulsada por el gobernador Mauricio Kuri González.

“Con la nueva CURP y el registro obligatorio de celulares, se podrá detectar la edad del usuario. El padre será quien registre el dispositivo y autorice los niveles de control parental en redes sociales”, señaló.

Agregó que el propósito es homologar el uso responsable de las plataformas digitales para menores.

“La tecnología es una herramienta que puede potenciar habilidades, pero debemos evitar que los menores permanezcan en ecosistemas de riesgo”, puntualizó Dorantes. Además, informó que desde el Senado se impulsa un programa de alfabetización digital con apoyo de la Comisión de Inteligencia Artificial, META y desarrolladores de redes sociales, para sensibilizar a padres, maestros y estudiantes sobre el uso seguro de internet.

Por su parte, la senadora Guadalupe Murguía Gutiérrez recordó que la iniciativa fue presentada el 18 de febrero en el Senado, con el respaldo de legisladores de distintas bancadas.

“Se sumaron senadores de Morena, del PRI y del PAN, entre ellos el senador Cepeda, líder del SNTE, quien reconoció los beneficios que la medida trae para el trabajo docente y la protección de los estudiantes”, comentó.

Murguía Gutiérez subrayó que la iniciativa no pretende prohibir el acceso digital, sino establecer reglas claras para proteger a la niñez y adolescencia.

“No se trata de prohibir, sino de regular, de ordenar y de garantizar que nuestros niños vivan en condiciones de seguridad. El bullying digital afecta la autoestima y la salud emocional; necesitamos actuar antes de que cause más daño”, concluyó la senadora.

Notas de Telecomunicaciones					
Título:	Presentan reforma para proteger los derechos de los usuarios que contratan telefonía móvil				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	EL ARSENAL	Por:	
Link:	https://www.elarsenal.net/?p=1220635				

México.- El diputado Pablo Vázquez Ahued (MC), a través de una iniciativa, propone reformar el artículo 185 de la Ley en Materia de Telecomunicaciones y Radiodifusión, a fin de fortalecer los derechos de los consumidores y usuarios de telefonía móvil.

La reforma, turnada a la Comisión de Comunicaciones y Transportes, plantea establecer el derecho de los usuarios de servicios móviles, en cualquiera de las modalidades de su prestación, de fijar el límite máximo de consumo para evitar el cobro adicional por uso de los servicios originalmente contratados, sin que implique dicha solicitud una erogación adicional.

También, que se provean los servicios de telecomunicaciones conforme a los parámetros “e índices de calidad establecidos por los lineamientos que emita la Comisión Reguladora de Telecomunicaciones, debiendo establecerse de manera desglosada y sencilla en los contratos de adhesión las obligaciones que el concesionario o autorizado se haya comprometido a satisfacer”.

En caso de incumplimiento, la persona usuaria podrá rescindir el contrato sin sanción, quedando obligada únicamente a cubrir cualquier costo pendiente.

A que la entrega de equipos sea en los términos que establezca la Comisión Reguladora de Telecomunicaciones, así como a solicitar y obtener el desbloqueo de manera inmediata cuando concluya la vigencia del contrato, se liquide su costo o se pague de contado, a través de medios electrónicos, siempre que las funcionalidades técnicas del equipo lo permitan, sin necesidad de acudir a los Centros de Atención a Clientes del concesionario o autorizado.

Asimismo, a que en cualquiera de las modalidades de su prestación, los saldos remanentes de los servicios incluidos en el plan tarifario, así como los complementarios y disponibles contratados de manera expresa y que no hayan sido consumidos en su totalidad, le sean reintegrados al cliente o usuario en el mes siguiente de su facturación, siempre y cuando técnicamente sea posible, según determine la Comisión Reguladora de Telecomunicaciones en los lineamientos.

La Procuraduría Federal del Consumidor verificará al menos cada dieciocho meses si existen condiciones que deban observar los concesionarios o autorizados en los contratos de adhesión, en su caso, conforme a los lineamientos en materia de parámetros e índices de calidad de servicios móviles que emita el órgano regulador competente en materia de telecomunicaciones, por lo que podrá solicitar las modificaciones correspondientes para la mejora de la calidad de los servicios prestados a las personas usuarias.

El documento en su exposición de motivos indica que de acuerdo con la información del Instituto Federal de Telecomunicaciones (IFT) el mayor número de inconformidades corresponde a fallas en el servicio, siguiéndole los problemas relacionados con los cargos, saldos y bonificaciones.

Además, la portabilidad y contrataciones, incumplimiento en la publicidad o promociones, evasión para realizar el desbloqueo de celulares y, por último, el cambio de plan o paquete sin previo aviso y no hacer válida la garantía de equipos y cambio de modalidad.

Notas de Telecomunicaciones					
Título:	CURP Biométrica: ¿Se puede tramitar en línea?				
Encabezado:	Este documento tiene como objetivo facilitar gestiones administrativas y prevenir fraudes de identidad con tecnología avanzada				
Fecha:	06/10/25 (por la tarde)	Fuente:	INFOBAE	Por:	Abigail Gómez
Link:	https://www.infobae.com/mexico/2025/10/06/curp-biometrica-se-puede-tramitar-en-linea/?outputType=amp-type				

Como ya muchos saben la CURP biométrica es una versión de la Clave Única de Registro de Población (CURP) de México que incorpora datos biométricos como huellas dactilares, reconocimiento facial y firmas digitales.

Este sistema busca fortalecer la identidad de las personas y aumentar la seguridad en la verificación de datos personales.

La CURP tradicional contiene datos alfanuméricos basados en el nombre, fecha de nacimiento y lugar de nacimiento y la CURP biométrica añade al registro información recopilada mediante tecnología biométrica, lo que permite autenticar la identidad de manera más precisa durante trámites oficiales, acceso a servicios gubernamentales y procesos bancarios.

Sin embargo, aún existen diversas dudas sobre cómo trámitarla y el momento en que entrará en vigencia, por ejemplo, algunos se preguntan si este trámite podrá realizarse en línea, sobre lo cual te contamos a continuación.

CURP Biométrica: ¿Es posible tramitarla en línea?
Debido a que este trámite es muy nuevo por el momento solo puede realizarse de manera presencial en alguno de los módulos piloto que el gobierno ha implementado en la Ciudad de México y algunos estados del país.

Sin embargo, el plan de funcionamiento de este documento estima que sí sea posible realizar el trámite de manera remota para aquellos que ya hayan brindando sus datos biométricos en otras ocasiones, como por ejemplo quienes estén dados de alta en el SAT o ante la Secretaría de Relaciones Exteriores.

A pesar de ello, debido a que es un trámite que aún se encuentra en pruebas, por el momento solo puede realizarse de manera presencial y se desconoce cuándo estará disponible la opción en línea, aunque se espera que sea durante los primeros meses de 2026.

Cuando esta opción se encuentre disponible el trámite podrá realizarse de en línea a través de la plataforma Llave MX, habilitada por la Agencia de Transformación Digital y Telecomunicaciones, por lo que se recomienda tener lista tu Llave MX.

Cómo y dónde tramitar la CURP Biométrica de manera presencial
Por lo pronto, sí deseas adelantar tu trámite, puedes asistir a uno de los 145 módulos disponibles a lo largo del país.

Uno de los principales es el módulo que se encuentra ubicado en la calle Londres 102, colonia Juárez, alcaldía Cuauhtémoc, cerca de Glorieta de Insurgentes, a donde puedes acudir para trámitar este CURP.

Documentos:
-Acta de nacimiento reciente
-Identificación oficial vigente
-CURP impresa
-Comprobante de domicilio (no mayor a 3 meses)
-Correo electrónico
-Ir acompañado de un tutor legal en caso de ser menor de edad

Este punto de atención, que forma parte de un programa piloto, permitirá a los habitantes de la capital obtener el documento de manera gratuita y en un proceso que no superará los 30 minutos.

Durante la cita, los solicitantes deberán proporcionar sus datos biométricos, incluyendo las huellas dactilares, el escaneo del iris, una fotografía digital y la firma electrónica.

El objetivo es combatir fraudes de identidad, suplantaciones y agilizar procedimientos administrativos al contar con una identificación digital única y verificable.

Notas de TI					
Título:	México recibió 237,000 intentos de ataque de ransomware en el último año				
Encabezado:	México sufrió 237,000 intentos de ataque de ransomware entre agosto de 2024 y julio de 2025, consolidándose como el segundo país más atacado de América Latina, sólo por detrás de Brasil.				
Fecha:	06/10/25 (por la tarde)	Fuente:	EL ECONOMISTA	Por:	Rodrigo Riquelme
Link:	https://www.eleconomista.com.mx/tecnologia/mexico-recibio-237-000-intentos-ataque-ransomware-ultimo-ano-20251006-780231.html				

México registró 237,000 intentos de ataque de ransomware entre agosto de 2024 y julio de 2025, de acuerdo con la telemetría de Kaspersky para el país. La cifra corresponde a ataques bloqueados por las soluciones de la firma de ciberseguridad y sitúa a México como uno de los mercados más golpeados de la región en los últimos 12 meses.

El panorama latinoamericano ayuda a dimensionar ese dato. En el mismo periodo, América Latina acumuló más de 1.1 millones de intentos de ataques de ransomware, alrededor de 3,000 al día y un promedio de dos por minuto, con Brasil a la cabeza (549,000), seguido por México (237,000), Chile (43,000), Ecuador (37,000) y Colombia (35,000). En total, la región reportó una caída interanual de 7% frente al año previo.

La disminución se explica, en parte, por acciones policiales que interrumpieron la infraestructura criminal. Uno de los golpes más relevantes fue la detención de integrantes del grupo Phobos y el decomiso de más de 100 servidores usados para orquestar ataques, lo que desmanteló parte de su red. Phobos figuraba entre las familias más activas en la región y llegó a impactar a 4.44% de las organizaciones latinoamericanas.

Aunque hay un respiro estadístico, la lectura de fondo no permite complacencias. Como advierte Fabio Assolini, director del equipo global de investigación y análisis de Kaspersky para América Latina, el escenario sigue siendo “preocupante” por el ritmo, 3,000 al día, 2 por minuto, y el tipo de daño que provoca el ransomware, desde la interrupción de operaciones hasta pérdidas financieras y reputacionales.

En México, el mapa de familias detectadas apunta a una combinación de variantes clásicas y linajes más recientes. Las detecciones se concentran en Blocker (MSIL) con 39.72% y Blocker (Win32) con 29.11%, seguidas de Convagent (10.76 por ciento). Phobos, pese a los golpes policiales, aún aparece con 2.38% del total de familias observadas en el país.

El ransomware es un tipo de programa malicioso que bloquea o cifra los archivos de una computadora o red, impidiendo el acceso a ellos hasta que la víctima paga un rescate. Su objetivo es extorsionar a individuos, empresas o gobiernos, y puede paralizar operaciones enteras si no existen copias de seguridad o planes de respuesta adecuados.

Industria es la más afectada

El reparto sectorial de los ataques confirma que la industria es el principal blanco en México. La categoría de manufactura de procesos concentra 22.91% de los incidentes, por encima del gobierno (13.39%), retail y mayoreo (6.16%) y manufactura discreta (6.06%), entre otros sectores.

Este patrón coincide con la lectura regional de Kaspersky: en Brasil y México, el sector industrial figura como el más atacado, mientras que en países como Argentina, Chile o Perú predomina el foco sobre entidades gubernamentales.

En paralelo al ransomware, México registró 411,000 ataques móviles bloqueados en el último año y una presión creciente por fraudes de apps de préstamos. Solo estas aplicaciones maliciosas acumularon 363,000 bloqueos en el año más reciente.

El impacto del ransomware, advirtió la compañía, no distingue tamaño de organización. Ha forzado el cierre de empresas centenarias y provocado quiebras en el sector salud tras filtraciones masivas, con pérdidas de confianza del público y daño reputacional difícil de revertir. Bases de datos públicas, firmas de tecnología y empresas mixtas también han sido vulneradas.

Para contener el riesgo, Kaspersky sugiere una disciplina básica pero constante. Aplicar parches y actualizaciones en endpoints y servidores para cerrar fallas explotables; reforzar normas internas sobre el manejo de información sensible y el reporte inmediato de anomalías; y mantener copias de seguridad fuera de línea, cifradas y con control de accesos, de modo que la recuperación de datos sea posible incluso si una red es cifrada por atacantes.

Entre sus previsiones para 2025, la firma prevé la proliferación del ransomware como servicio (RaaS), junto con el auge de los stealers y nuevas amenazas basadas en blockchain. Dicho de otro modo, la oferta criminal seguirá profesionalizándose y abaratando la entrada a bandas de menor sofisticación técnica.

México se consolidó como segundo foco de ransomware en América Latina durante el último año y su tejido productivo, con la manufactura al frente, se mantiene en el centro de la diana para este tipo de ataques.

Notas de TI					
Título:	Lenovo revela el miedo oculto de los CIOs 65% de los líderes de TI no están preparados para enfrentar ciberataques impulsados por IA.				
Encabezado:	La compañía propone “combatir la IA con IA” mediante defensas inteligentes y adaptativas que refuercen el lugar de trabajo moderno.				
Fecha:	06/10/25 (por la tarde)	Fuente:	IT SITIO	Por:	Redacción
Link:	https://www.itsitio.com/mx/inteligencia-artificial/lenovo-revela-el-miedo-oculto-de-los-cios-65-de-los-lideres-de-ti-no-estan-preparados-para-enfrentar-ciberataques-impulsados-por-ia/				

La inteligencia artificial (IA) se convirtió en el mayor aliado y a la vez, en el nuevo enemigo de las empresas modernas. Un reciente estudio de Lenovo revela que el 65% de los líderes de TI reconocen que sus defensas actuales son incapaces de resistir los ataques cibernéticos habilitados por IA, y apenas el 31% asegura sentirse realmente preparado para enfrentarlos.

Estos hallazgos forman parte del tercer informe Work Reborn de Lenovo, titulado “Reforzando el lugar de trabajo moderno”, que analiza cómo la IA, mientras impulsa la eficiencia y la innovación, también está transformando el panorama de la ciberseguridad. El documento advierte que las amenazas de hoy en día aprenden, se adaptan y evolucionan con velocidad lo que exige un replanteamiento de las estrategias de defensa empresarial.

“La IA transforma el equilibrio de poder en ciberseguridad. Para mantenerse al día, las organizaciones necesitan inteligencia que se adapte a la velocidad de las amenazas. Esto significa combatir la IA con IA”, afirmó Rakshit Ghura, vicepresidente y director general de Soluciones Digitales para el Lugar de Trabajo de Lenovo.

De acuerdo con Lenovo, los cibercriminales utilizan algoritmos avanzados para lanzar ataques hiperágiles capaces de imitar comportamientos legítimos, mutar para evadir detecciones y operar simultáneamente en distintos frentes: desde la nube hasta los endpoints, pasando por las aplicaciones y los almacenes de datos.

Amenazas cada vez más sofisticadas

Asimismo, el informe identifica tres grandes focos de preocupación para los líderes de TI.

El primero son las amenazas externas impulsadas por IA, que incluyen malware polimórfico, campañas de phishing automatizadas y suplantaciones de identidad mediante deepfakes. Estos ataques son cada vez más convincentes y difíciles de detectar.

El segundo punto es el riesgo interno. Un 70% de los encuestados considera que el mal uso de herramientas de IA por parte de los empleados representa un peligro significativo, mientras que más del 60% teme que los agentes de IA generen una nueva categoría de amenazas internas para las cuales las empresas aún no están preparadas.

Finalmente, el informe advierte sobre la vulnerabilidad de la propia IA. Los modelos de entrenamiento, los datos y las indicaciones que alimentan los sistemas inteligentes se han convertido en objetivos de alto valor, susceptibles de ser manipulados o comprometidos.

Estas tendencias dejan en evidencia que las defensas convencionales han quedado atrás. Frente a ello, Lenovo propone una estrategia nativa de IA, capaz de detectar amenazas antes de que se materialicen, adaptarse en tiempo real y escalar conforme evolucionan los entornos de trabajo.

Del enfoque reactivo a la ciberresiliencia

Datos de Gartner apuntan que para 2027 el 90% de las implementaciones exitosas de IA en ciberseguridad estarán enfocadas en la automatización de tareas y la ampliación de procesos, más que en la sustitución de roles humanos. McKinsey, por su parte, advierte que las empresas que continúen dependiendo de defensas tradicionales quedarán rezagadas frente al rápido avance de las amenazas basadas en IA.

Actualmente Lenovo está ampliando la protección inteligente hasta el nivel del dispositivo. Con la nueva generación de PC con IA, la compañía está integrando capacidades de defensa autónoma en los endpoints, que ahora pueden actuar como activos autoprotectores. Estas funciones se enlazan directamente con la plataforma de ciberresiliencia de Lenovo, que ofrece una cobertura integral desde el borde hasta la nube.

“Con defensas inteligentes y adaptables, los líderes de TI pueden proteger a su personal, sus activos y sus datos, a la vez que aprovechan todo el potencial de la IA para impulsar el negocio”, añadió Ghura.

Para atender estos retos, Lenovo propone una visión integral mediante Digital Workplace Solutions, impulsada por la plataforma Care of One con tecnología Gen-AI.

Esta propuesta integra Lenovo Security Services con ThinkShield, una suite que protege endpoints, aplicaciones, datos y empleados a escala empresarial, fortaleciendo así la ciberresiliencia en todo el entorno digital.

Empresas como Meta ya utilizan las herramientas de Lenovo para validar la autenticidad de su hardware. “ThinkShield Supply Chain Assurance refuerza significativamente nuestra confianza en la autenticidad e integridad de nuestro hardware”, destacó la compañía en el informe.

“Con las herramientas de IA proliferando más allá de la visibilidad de TI y los atacantes explotando brechas que los sistemas tradicionales no pueden reconocer, Lenovo está brindando las defensas impulsadas por IA que las empresas necesitan para cerrar la brecha, convirtiendo el riesgo en resiliencia y habilitando lugares de trabajo protegidos, productivos y preparados para el futuro”, concluyó Ghura.

Notas de TI					
Título:	Ciberseguridad en la banca privada				
Encabezado:					
Fecha:	07/10/25	Fuente:	OEM	Por:	Elizabeth Pastor Jácome
Link:	https://oem.com.mx/elsoldemexico/analisis/ciberseguridad-en-la-banca-privada-26154953				

En un mundo cada vez más interconectado, la ciberseguridad en la banca privada ha dejado de ser un tema técnico para convertirse en un asunto de seguridad internacional. Las vulnerabilidades en los proveedores de servicios digitales no sólo ponen en riesgo a una institución aislada, sino que pueden desencadenar efectos en cadena capaces de desestabilizar mercados financieros completos.

La banca privada gestiona patrimonios millonarios, fideicomisos y operaciones transfronterizas de individuos y corporaciones con alto poder económico. Esta naturaleza la convierte en un actor estratégico dentro de la arquitectura financiera internacional y, al mismo tiempo, en un blanco prioritario para el cibercrimen.

Una brecha de seguridad en este sector no se limita a pérdidas económicas; sus consecuencias pueden extenderse a ámbitos diplomáticos, fiscales y políticos, dado que la información que se maneja suele estar vinculada con estructuras empresariales y capitales de alcance global.

Los ciberataques no reconocen fronteras. Un incidente en un banco privado europeo puede tener repercusiones inmediatas en América Latina y viceversa. Los casos recientes de ataques a cadenas

de suministro digital muestran cómo una vulnerabilidad en un solo proveedor puede convertirse en una amenaza sistémica con impacto en múltiples jurisdicciones al mismo tiempo.

Esta realidad plantea un desafío para la gobernanza internacional: ningún Estado, banco o proveedor puede enfrentar en solitario un fenómeno que trasciende fronteras y que evoluciona con rapidez.

Aunque existen marcos normativos como el Reglamento General de Protección de Datos GDPR en Europa o la regulación de la Comisión Nacional Bancaria y de Valores en México, la velocidad con la que avanzan los ciberdelincuentes supera la capacidad de adaptación de las leyes. La falta de armonización regulatoria a nivel global genera vacíos que pueden ser explotados y obliga a las instituciones a cumplir con normas divergentes en distintas regiones.

Ante ello, se vuelve indispensable la cooperación multinivel. A nivel nacional, reforzar la supervisión y las alianzas público-privadas. A nivel regional, homogenizar estándares de seguridad digital y a nivel internacional, se debería avanzar hacia un marco común de gobernanza que permita compartir inteligencia, coordinar respuestas y fortalecer la resiliencia del sistema financiero global.

La ciberseguridad en la banca privada también refleja tensiones propias de las relaciones internacionales: disputas por la soberanía digital, competencia geopolítica en el ciberespacio y el papel de la banca como custodio de la confianza internacional.

Además, la dimensión humana no puede ignorarse. Errores internos, negligencias o la manipulación psicológica mediante ingeniería social siguen siendo puertas de entrada que ponen en juego incluso a los sistemas más sofisticados.

Blindar la banca privada es proteger algo más que capitales: es salvaguardar la confianza que sostiene los flujos financieros internacionales. Una vulnerabilidad no atendida puede convertirse en un riesgo sistémico capaz de afectar inversiones, mercados bursátiles y la credibilidad de los Estados.

La ciberseguridad, por tanto, no es solo una cuestión tecnológica, sino un eje estratégico de la seguridad económica internacional. Su gestión requiere cooperación, marcos regulatorios sólidos y una visión de gobernanza global que reconozca que los riesgos digitales, como los capitales, no conocen fronteras.

Notas de TI					
Título:	La IA generativa ‘weaponizada’ amenaza las infraestructuras críticas				
Encabezado:					
Fecha:	07/10/25	Fuente:	SEGURILATAM	Por:	
Link:	https://www.segurilatam.com/ciberilatam/ciberseguridad-ciberilatam/la-ia-generativa-weaponizada-amenaza-las-infraestructuras-criticas_20251007.html				

La inteligencia artificial (IA) generativa representa un cambio paradigmático en ciberseguridad. La Cybersecurity and Infrastructure Security Agency (CISA) documentó cerca de 1.300 alertas de

defensa cibernética durante 2024, reflejando un incremento sustancial en la actividad maliciosa dirigida a infraestructuras críticas.

Esta evolución ha democratizado capacidades ofensivas sofisticadas. Herramientas que requerían equipos especializados y meses de desarrollo ahora se generan automáticamente. El impacto es evidente: el 54 por ciento de los CISO de instalaciones críticas reportaron ataques de ransomware, afectando a sistemas de tecnología operativa (OT).

La convergencia entre IA generativa y ciberataques reformula fundamentalmente cómo los adversarios operan y escalan operaciones. Los sistemas críticos, diseñados con criterios de seguridad de generaciones anteriores, enfrentan amenazas que evolucionan en tiempo real.

La proliferación en mercados clandestinos es documentada por la inteligencia de amenazas. Las búsquedas de software de clonación de voz aumentaron un 120 por ciento entre julio 2023 y 2024, mientras que herramientas deepfake en foros de la Dark Web se incrementaron un 223 por ciento durante el mismo período.

Transformación de vectores de ataque con la IA

Los sistemas OT representan el núcleo operacional de las infraestructuras críticas. El 26 por ciento de las organizaciones utiliza ahora tecnologías cloud para aplicaciones ICS/OT, marcando un aumento del 15 por ciento respecto a períodos anteriores.

Esta conectividad expandida coincide con herramientas de IA capaces de mapear automáticamente topologías de red complejas. Los algoritmos pueden analizar patrones de tráfico, identificar sistemas críticos y desarrollar estrategias de ataque adaptativas sin intervención humana.

No en vano, los deepfakes han evolucionado hacia aplicaciones maliciosas. Casos documentados incluyen el uso de deepfake para defraudar 25 millones de dólares, donde criminales se hicieron pasar por ejecutivos durante videoconferencias corporativas.

La automatización de ingeniería social representa otra frontera crítica. Los sistemas de IA generan contenido híperpersonalizado basándose en análisis de perfiles públicos, creando campañas de phishing con tasas de éxito superiores a las de métodos tradicionales.

Los mercados de cibercrimen también han respondido rápidamente. Servicios de «IA-as-a-Service» maliciosa proliferan en plataformas clandestinas, permitiendo que actores con recursos limitados accedan a capacidades avanzadas de generación de malware y orquestación de ataques multivectoriales.

Casos documentados

El panorama de 2024 está caracterizado por un incremento en la sofisticación y la automatización. CISA documentó 68 ciberataques con consecuencias físicas contra sistemas de control industrial durante 2023, con proyecciones que indican cifras considerablemente más altas para 2024.

El grupo CyberArmyofRussia_Reborn ejemplifica esta nueva generación. Sus operaciones contra instalaciones industriales estadounidenses durante 2024 demuestran el uso integrado de la IA para automatizar el descubrimiento y la explotación de vulnerabilidades en sistemas OT.

El caso Volt Typhoon ilustra la persistencia y sofisticación de actores estatales. Este grupo se infiltró en redes de infraestructura crítica, permaneciendo latente mientras desarrollaba capacidades disruptivas. La campaña Salt Typhoon comprometió sistemas de telecomunicaciones críticas en noviembre de 2024.

Por su parte, Reino Unido reportó un incremento del 300 por ciento en ataques clasificados como más serios durante 2024. Esta escalación coincide con el desarrollo de herramientas de IA que generan malware polimórfico, capaz de modificar su código automáticamente para evadir sistemas de detección tradicionales.

Finalmente, el sector energético experimentó ataques particularmente sofisticados. Análisis revelan el uso de IA para mapear redes eléctricas, identificar puntos de falla críticos y desarrollar escenarios de ataque coordinados diseñados para causar interrupciones en cascada. Incluso algunos malware permanecieron indetectables durante períodos superiores a 180 días en sistemas SCADA.

El panorama de 2024 está caracterizado por un incremento en la sofisticación y la automatización

Estrategias defensivas emergentes

La respuesta requiere una reformulación de estrategias defensivas. La segmentación debe evolucionar hacia una microsegmentación inteligente que utilice análisis comportamental en tiempo real. Los sistemas zero trust requieren verificación continua incorporando análisis biométrico conductual para detectar anomalías sutiles.

De hecho, CISA lanzó 21 avisos de sistemas de control industrial el 10 de octubre de 2024. La gestión efectiva requiere sistemas de análisis predictivo que utilicen IA defensiva para anticipar vectores de ataque y priorizar remediciones basándose en la probabilidad de explotación y el impacto potencial.

Por todo ello, los sistemas de respuesta tradicionales resultan insuficientes contra adversarios adaptativos. Las organizaciones implementan capacidades de respuesta automatizada capaces de aislar amenazas, reconfigurar redes y restaurar servicios sin intervención humana, reduciendo tiempos de respuesta de horas a segundos.

Por otro lado, la inteligencia de amenazas incorporó machine learning para análisis predictivo. Estos sistemas identifican patrones emergentes, correlacionan indicadores across múltiples fuentes y generan alertas tempranas sobre campañas en desarrollo.

Finalmente, los marcos regulatorios evolucionan para abordar estos desafíos. La Ley de IA de la Unión Europea, vigente desde agosto de 2024, establece obligaciones de transparencia para contenido generado por IA. Estados Unidos introdujo también múltiples propuestas legislativas dirigidas a regular uso de la IA en contextos de seguridad crítica.

IA y ciberseguridad: Proyecciones para 2026

Las tendencias proyectan hacia 2026 un escenario de confrontación directa entre IA ofensiva y defensiva. Los sistemas de defensa deberán incorporar capacidades evolutivas automáticas, aprendiendo de cada ataque y adaptando defensas sin intervención humana.

Los «ataques de envenenamiento de modelo» emergerán como vector crítico, dirigidos a corromper sistemas de IA defensivos mediante la introducción de datos maliciosos en algoritmos de detección. Esta técnica podría crear puntos ciegos sistemáticos explotables por adversarios sofisticados.

Asimismo, la velocidad de adaptación se convertirá en el factor determinante. Arquitecturas de «defensa evolutiva» capaces de reconfigurar automáticamente topologías, actualizar reglas de detección y desplegar contramedidas adaptativas sin interrumpir operaciones representarán el estándar mínimo para la protección crítica.

El equilibrio estratégico dependerá de cuál lado innova más rápidamente en el desarrollo de IA más adaptable, resiliente y eficiente. Esta carrera tecnológica determinará el futuro de la seguridad en infraestructuras críticas durante la próxima década.

Notas de TI					
Título:	Digitalización | el nuevo motor de la competitividad empresarial en México				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	LIDERES MEXICANOS	Por:	Santiago Ortíz
Link:	https://lideresmexicanos.com/tendencias/tecnologia/digitalizacion-el-nuevo-motor-de-la-competitividad-empresarial-en-mexico				

Durante años, la digitalización fue vista en México como una meta a mediano plazo, presente en los consejos de administración pero aún en debate. Sin embargo, los recientes eventos globales aceleraron esa transición: lo que era una aspiración se convirtió en una prioridad urgente para garantizar continuidad operativa y competitividad.

Hoy, la conversación empresarial ya no se centra en si digitalizarse, sino en cómo liderar esta transformación para fortalecer la resiliencia en un entorno marcado por la volatilidad.

Eficiencia y resiliencia en tiempos de cambio
La digitalización encuentra su mayor valor en la eficiencia. La automatización de procesos, el uso de sensores y el análisis de datos en tiempo real están revolucionando industrias que antes dependían de verificaciones manuales.

Un ejemplo claro es la monitorización remota, que permite a equipos pequeños supervisar múltiples instalaciones, comparar rendimientos y actuar de forma proactiva ante cualquier alerta. Esta capacidad no solo mejora la operación diaria, sino que otorga mayor agilidad y robustez en momentos de crisis, ya sea una interrupción en la cadena de suministro o una contingencia local.

En este sentido, una empresa digitalizada no solo es más eficiente, sino también más resiliente.

Sostenibilidad: el nuevo pilar de la rentabilidad
La digitalización también está redefiniendo la sostenibilidad como motor de competitividad. La presión de los consumidores y la necesidad de optimizar costos energéticos han alineado los objetivos ecológicos con los financieros.

Con herramientas digitales, las empresas pueden monitorear activos, analizar consumos y detectar ineficiencias energéticas con precisión. Un caso emblemático es el de Schneider Electric en su planta de Le Vaudreuil, Francia, donde la digitalización permitió una mejora del 10% en la efectividad operativa y una reducción del 15% en el consumo energético.

Estos resultados confirman que la digitalización no solo contribuye al cuidado ambiental, sino que también genera ahorros directos que fortalecen la rentabilidad.

Talento: el verdadero motor de la transformación
Si bien la tecnología es clave, la digitalización depende en última instancia del factor humano. La automatización genera interrogantes sobre el futuro del empleo, pero más que eliminar puestos, está provocando una evolución del talento.

Las tareas repetitivas tienden a desaparecer, pero en su lugar surgen nuevas funciones que exigen habilidades más especializadas, desde la supervisión de sistemas digitales hasta el análisis avanzado de datos.

El desafío radica en capacitar y reconvertir al personal, además de fomentar una cultura organizacional que impulse la agilidad y la toma de decisiones informada. En muchos casos, el obstáculo no es la tecnología, sino la preparación de las personas y el liderazgo para aprovecharla.

Un camino de evolución continua
La digitalización no es un destino fijo, sino un proceso constante de transformación. Su adopción marca una diferencia clara entre empresas que apuestan por modelos más ágiles e inteligentes y aquellas que permanecen en esquemas tradicionales.

Para los líderes empresariales en México, este es un momento de reflexión estratégica: no basta con adquirir tecnología, es necesario integrarla de manera que fortalezca la cadena de valor, mejore la sostenibilidad y ponga al cliente en el centro.

La invitación es clara: liderar la transformación digital para construir organizaciones más competitivas, resilientes y preparadas para los retos y oportunidades del futuro.

Notas de TI					
Título:	Mes de la Concienciación sobre la Ciberseguridad: La seguridad empieza con ustedes				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	MICROSOFT	Por:	Vasu Jakkal
Link:	https://news.microsoft.com/source/latam/noticias-de-microsoft/mes-de-la-concienciacion-sobre-la-ciberseguridad-la-seguridad-empieza-con-ustedes/				

En Microsoft, la seguridad es nuestra prioridad número uno, y creemos que la ciberseguridad tiene que ver tanto con las personas como con la tecnología. A medida que avanzamos hacia octubre y comenzamos el Mes de Concientización sobre la Ciberseguridad, esta época del año en verdad me hace pensar en lo importante que es la seguridad en línea, no solo en el trabajo, sino también para mi familia y amigos. A menudo comparto consejos con mis seres queridos sobre cómo mantenerse

seguros en línea, porque desarrollar hábitos de seguridad sólidos y mantenerlos en mente se ha convertido en una parte clave de cómo me protejo a mí misma y a quienes me rodean.

Como parte de Microsoft Secure Future Initiative (SFI), nos hemos comprometido a integrar la seguridad en cada capa de nuestra tecnología, cultura y gobernanza, al colocar la seguridad por encima de todo. Desde su lanzamiento en noviembre de 2023, SFI ha movilizado el equivalente a más de 34 mil ingenieros para reducir el riesgo de forma proactiva y reforzar la seguridad en Microsoft y en los productos y servicios que ofrecemos a nuestros clientes. Un gran ejemplo de esto es la mitigación de los ataques avanzados de autenticación multifactor, donde la autenticación multifactor resistente al phishing ahora protege el 100% de las cuentas del sistema de producción y el 92% de las cuentas de productividad de los empleados. Además, continuamos con la reducción del riesgo de compromiso durante la configuración de nuevos empleados al aplicar la verificación basada en video, ahora al 99%.1

Habilitación de su enfoque donde la seguridad es primero
Este año, también hemos desarrollado nuevos recursos y herramientas para ayudar a los profesionales de la seguridad a mantener seguras a sus organizaciones, en particular a medida que entramos en esta próxima era de IA. Sobre la base de nuestros aprendizajes con SFI, hemos creado patrones y prácticas de SFI, que es una nueva biblioteca de orientación práctica diseñada para ayudar a las organizaciones a implementar la seguridad a escala.

Además de las mejores prácticas para los profesionales de la seguridad, continuamos con la adición de artículos a nuestro Kit Be Cybersmart, que es un excelente punto de partida para los profesionales de la seguridad que necesitan educar a sus organizaciones sobre cómo estar seguros. El kit Be Cybersmart contiene artículos sobre seguridad de IA, seguridad de dispositivos, suplantación de dominio, fraude, inicio de sesión seguro y phishing. El kit es solo uno de los muchos recursos disponibles en el sitio de concientización sobre ciberseguridad de Microsoft.

Aquellos que buscan recursos más detallados pueden acceder a rutas de aprendizaje, certificaciones y documentación técnica de nivel experto para continuar su educación en ciberseguridad. Y para los estudiantes que buscan el campo de la ciberseguridad, el Programa de Becas de Ciberseguridad de Microsoft y las oportunidades educativas como Microsoft Elevate están aquí para ayudar. El objetivo de todos estos programas es ayudar a fomentar una cultura que priorice la seguridad y el aprendizaje continuo tanto para estudiantes como para profesionales.

La seguridad es lo primero en acción: Franciscan Alliance
Un gran ejemplo de una cultura de seguridad primero, en especial en torno a la educación y la capacitación de concientización, es Franciscan Alliance, una organización católica de atención médica sin fines de lucro con sede en Indiana. Esta organización emplea una estrategia proactiva e interactiva para la concientización sobre ciberseguridad y la educación de los empleados.

«Creemos que la educación en ciberseguridad debe ser continua, atractiva y empoderadora, porque los empleados informados son nuestra defensa más fuerte». — Jay Bhat, director de seguridad de la información (CISO), Franciscan Alliance

La organización realiza simulaciones mensuales de phishing y evaluaciones trimestrales para exponer al personal a escenarios realistas de manera consistente. Los empleados que no aprueban las evaluaciones trimestrales reciben capacitación adicional en lugar de ser penalizados, lo que

respalda una cultura centrada en el aprendizaje y el desarrollo. Los programas de capacitación incorporan elementos de gamificación para mejorar la accesibilidad y la retención. Además, los empleados reciben un boletín mensual que cubre temas de seguridad relevantes que respaldan las prácticas seguras tanto profesional como personalmente.

Durante el Mes de Concientización sobre Ciberseguridad, se distribuyen ediciones semanales, junto con actualizaciones oportunas sobre amenazas emergentes, incluidas infracciones y ataques. Franciscan Alliance también organiza sesiones informativas sobre amenazas en asociación con socios externos y utiliza recursos como los materiales de concientización sobre ciberseguridad de Microsoft para informar sus iniciativas de capacitación.

Desarrollo de competencias de seguridad en la era de la IA
A medida que las organizaciones adoptan de manera rápida la IA, hacer de la seguridad la primera prioridad no es solo una mejor práctica, es una necesidad. Los sistemas de IA son herramientas poderosas que pueden transformar la productividad empresarial, pero sin medidas sólidas de gobernanza y seguridad, también pueden presentar riesgos significativos. Para abordar estos desafíos y potenciar el liderazgo que prioriza la seguridad, invitamos a los ejecutivos de nivel C a registrarse en el próximo seminario web de Microsoft «Confianza en la IA: Aceleren el crecimiento empresarial con confianza«, que contará con discusiones críticas sobre cómo generar confianza en la IA para su organización.

Además, la directora de productos de IA responsable de Microsoft, Sarah Bird, moderará el panel, «Ciberseguridad e IA, riesgo estratégico y ventaja competitiva«, en la Cumbre NASDAQ el 21 de octubre de 2025 en la Bolsa de Valores de Nueva York, donde expertos de la industria brindarán orientación sobre gobernanza y seguridad para la IA. En esta sesión, los expertos discutirán casos de uso del mundo real, desarrollos regulatorios y las implicaciones estratégicas de la integración de la IA en entornos empresariales. Eventos como estos son oportunidades increíbles para que los ejecutivos profundicen su comprensión y lideren con confianza en la era de la IA.

Aprovechen al máximo el Mes de la Concientización sobre Ciberseguridad
Esperamos que estos recursos les brinden el aprendizaje, la capacitación y la confianza para prepararlos a ustedes y a sus organizaciones para el éxito, tanto este mes como más allá. Ahora es el momento de construir una cultura con una mentalidad donde la seguridad es primero, al hacer que la seguridad sea parte de sus hábitos diarios en el trabajo, el hogar y en cualquier otro lugar. Una mentalidad donde la seguridad es primero significa mantenerse informados, proteger de manera proactiva los activos digitales y alentar a otros a hacer lo mismo. La seguridad es un deporte de equipo. Al promover la vigilancia y la responsabilidad compartida, podemos crear un mundo más seguro para todos.

Para obtener más información sobre las soluciones de seguridad de Microsoft, visiten nuestro sitio web. Agreguen a Favoritos el blog de Seguridad para mantenerse al día con nuestra cobertura experta en asuntos de seguridad. Además, síganos en LinkedIn (Microsoft Security) y X (@MSFTSecurity) para conocer las últimas noticias y actualizaciones sobre ciberseguridad.

Notas de TI	
Título:	Lidera Quintana Roo la digitalización catastral en Iberoamérica
Encabezado:	

Fecha:	06/10/25 (por la tarde)	Fuente:	QUINTANA ROO QUADRATIN	Por:	Melody Ortiz
Link:	https://quintanaroo.quadratin.com.mx/lidera-quintana-roo-la-digitalizacion-catastral-en-iberoamerica/				

CANCÚN, QRoo, 6 de octubre de 2025.- Quintana Roo se consolidó como líder iberoamericano en modernización catastral durante el XVI Simposio del Comité Permanente sobre el Catastro en Iberoamérica (CPCI), presidido por el Instituto Geográfico y Catastral del Estado (IGECE).

Con la participación de más de 100 representantes de 13 países, el encuentro abordó los avances tecnológicos y el papel de la inteligencia artificial (IA) en la gestión del territorio.Encabeza la entidad por tercer año el Simposio Iberoamericano y destaca por el uso de inteligencia artificial en gestión territorial.

El titular del IGECE, Ricardo López Rivera, subrayó que la IA impulsa una gestión más transparente y eficiente, marcando una nueva era en los procesos catastrales.

Gracias al impulso de la gobernadora Mara Lezama Espinosa, el estado ha digitalizado los catastros de Lázaro Cárdenas, Felipe Carrillo Puerto, Puerto Morelos y Bacalar, con planes de incorporar próximamente a Tulum, José María Morelos y Benito Juárez.

El Nuevo Acuerdo por el Bienestar y Desarrollo de Quintana Roo ha permitido integrar herramientas geoespaciales que fortalecen la transparencia y combaten la corrupción.

Con ello, el estado se posiciona como modelo de innovación y gestión territorial sostenible, reconocido por toda Iberoamérica.

Notas de TI					
Título:	El modelo chino para dominar la IA: una estrategia de 40 años en marcha				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	DPL NEWS	Por:	Sharon Durán
Link:	https://dplnews.com/el-modelo-chino-para-dominar-la-ia-una-estrategia-de-40-anos-en-marcha/				

Planeación, inversión y ejecución es la fórmula estratégica de China para posicionarse y mantenerse como un epicentro de innovación y transformación digital. Desde hace más de cuatro décadas, el gigante asiático se trazó una ruta ascendente que combina políticas estatales de largo plazo, financiamiento masivo en infraestructura tecnológica y una coordinación estrecha entre gobierno, academia y sector privado.

Esta estrategia no sólo le ha permitido escalar en sectores como telecomunicaciones, manufactura y minería avanzada, sino también consolidar a la Inteligencia Artificial (IA) como un eje central de desarrollo económico, social y geopolítico, con metas claras hacia 2030 para liderar la feroz carrera en IA. Esta competencia para el gigante asiático ya es del tejido urbano, desde consultas frecuentes a Deepseek por parte de la ciudadanía, hasta centros de investigación y desarrollo como el Lianqiu

Lake, de Huawei, son parte de la realidad para acelerar el desarrollo en la materia y en el fortalecimiento de su industria de chips.

La estrategia de China por liderar la IA no es actual, de hecho, se remonta a los años 80. Bajo el liderazgo de Deng Xiaoping, el país abrazó la reforma y apertura bajo cuatro pilares de desarrollo nacional: agricultura, industria, ciencia y tecnología, y defensa nacional.

Con la implementación de las modernizaciones, el gigante asiático marcó la dirección estatal con metas medibles, provisión de incentivos para apoyar los cuatro sectores estratégicos y dejar que empresas privadas traduzcan la visión estatal en soluciones tecnológicas de escala al servicio de la ciudadanía.

Con el paso de los años, la estrategia de China se transformó en cifras de conectividad que alcanzan el 79.7% de penetración de Internet en junio de 2025, según el informe del China Internet Network Information Center (CNNIC). Pero ahí no se detiene la estrategia: empresas como Huawei han dejado claro que la prioridad ya no es únicamente el desarrollo de IA, sino hacerlo desde sus propios GPUs (Unidad de Procesamiento Gráfico). Esta decisión responde a las tensiones geopolíticas que atraviesa el sector tecnológico en el mundo, pero también es parte de la planeación propia de China.

En el marco del Huawei Connect 2025, la compañía presentó su hoja de ruta con los chips Ascend hasta 2028, que refuerza la apuesta por un ecosistema robusto y localmente diseñado. Su plan contempla la evolución de procesadores cada vez más potentes y eficientes, acompañados de la construcción de SuperPods, clusters masivos que conectan miles de unidades de procesamiento a través de interconexiones ópticas de alta velocidad.

Con los chips en desarrollo de Huawei, como el Ascend 950 para 2026, el Ascend 960 en 2027 y el Ascend 970 planeado para 2028, la compañía demuestra que entiende la competencia en IA como una carrera tanto de infraestructura como de algoritmos, y ofrece soluciones de modelo avanzados para sostener aplicaciones de nueva generación en sectores diversos como finanzas, energía, transporte o salud.

Pero la apuesta de China, de nuevo, es integral y trasciende las soluciones de hardware: “El diseño de Centros de Datos desde cero, la provisión de conectividad, el suministro energético y los servicios en la Nube que alimenten a un ecosistema propio”, detalló César Funes, líder de Industrial de política y desarrollo del ecosistema de IA para Huawei Latinoamérica y el Caribe.

A esto se suma la presencia de China en diferentes países que, por ahora no, tienen un rol protagónico en la carrera por la IA, como América Latina y África, y las empresas comparten no sólo la experiencia que 4 décadas pueden ofrecer, sino alternativas para fortalecer la transformación digital desde sus propios territorios. Parece como si China, a través de sus empresas, buscara que cada país se convierta en nodo de esta red global, capaz de sostener su propia transformación digital.

Sin embargo, la ruta no está exenta de retos. En el terreno persisten tres grandes desafíos en una carrera global que no se detiene. A pesar de la capacidad de movilización de recursos, las barreras técnicas y las tensiones políticas siguen siendo variables críticas que por ahora no presentan una conclusión.

Por el momento, China sí tiene un potencial enorme de liderar la carrera por la IA. La razón es que mientras otros actores globales concentran sus esfuerzos en chips o modelos específicos, China impulsa un modelo sistémico e integral que incorpora hardware, redes, Centros de Datos, aplicaciones industriales y, sobre todo, la capacidad de escalar masivamente. En esa fórmula se apoya su ambición de convertirse en el principal centro de innovación en IA hacia 2030.

Ese diseño estratégico toma forma concreta precisamente en el Plan de Desarrollo de la Nueva Generación de Inteligencia Artificial promulgado en 2017, que se convirtió en la hoja de ruta nacional que articula objetivos, etapas y métodos hacia 2030. En ese plan, China define tres etapas sucesivas. Para 2020, lograr avances significativos en métodos y aplicaciones, para 2025, convertirse en un competidor global con innovación reconocible; y para 2030, transformarse en el líder mundial en teorías, tecnologías, aplicaciones y normas de IA. Etapas que hasta ahora ha cumplido.

Además, el plan propone el liderazgo en tecnología, diseño sistémico, orientación al mercado y apertura colaborativa como los cuatro principios rectores para lograr sus objetivos.

El plan también subraya cómo China ve la IA y es que no se trata de un campo aislado, sino como un ecosistema tecnosocial que debe integrarse con la industria, la gobernanza, la educación y la ética. En ese sentido, la ambición no es sólo técnica, sino normativa: el plan también busca que China juegue un papel determinante en la definición de estándares internacionales, regulaciones de IA segura y directrices para gobernanza algorítmica.

No se trata de una carrera improvisada, sino de una estrategia sostenida que busca ganar en términos de tecnología, pero también en influencia normativa y política.

En China, la IA es vista tanto como un motor económico como un pilar de poder nacional que seguirá impactando sus industrias nacionales y la proyección global de un país que no mide su alcance en años, sino en décadas, y que hasta ahora ha funcionado.

Notas de CANIETI Regional					
Título:	Ciberataques a empresas de Guanajuato aumentan 22% en el último año				
Encabezado:					
Fecha:	06/10/25 (por la tarde)	Fuente:	PUERTO INTERIOR GUANAJUATO	Por:	
Link:	https://puertointerior.guanajuato.gob.mx/blog/2025/10/06/ciberataques-a-empresas-de-guanajuato-aumentan-22-en-el-ultimo-ano/				

Guanajuato. En el último año, la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) en el estado, reportó un incremento del 22 por ciento en los ciberataques a empresas de la entidad.

Luz Adriana Valdivia, directora de la cámara, explicó que los métodos de hackeo se han vuelto más sofisticados y que los delincuentes ahora utilizan inteligencia artificial para clonar datos y suplantar identidades.

Además de las tradicionales estrategias de phishing a través de redes sociales o WhatsApp, estos canales se han convertido en los más frecuentes para cometer estafas.

El año pasado, en México se registraron más de 42.4 millones de intentos de ataques de malware contra empresas, lo que representa cerca de 116 mil intentos diarios, es decir, unos 80 ataques por minuto.

La directora de la CANIETI advirtió que muchas empresas carecen de protocolos de seguridad integrales o de suficiente capacitación para su personal, lo que las hace vulnerables a ataques derivados de errores humanos.

“Ya hacen uso de la voz, toman nuestra voz para editar y hacer llamadas a nuestros conocidos. Hackean la información del teléfono y piden apoyos económicos”, detalló.

De enero a octubre, la cámara ha asistido al menos a 15 empresas víctimas de hackeos de alto impacto, con exigencias de rescate económico que van desde 20 mil pesos a personas físicas hasta un millón de pesos en casos de secuestro de datos corporativos.

Valdivia subrayó que la prevención es la mejor herramienta para reducir riesgos, aunque aún es una práctica poco explorada por empresas y personas.

La CANIETI ha impulsado charlas y capacitaciones para enseñar a los empresarios a proteger su información y dispositivos mediante prácticas básicas y software especializado.

“Cada aplicación móvil tiene herramientas que nos pueden ayudar a reducir los riesgos; la clave es utilizarlas y estar atentos”, concluyó.