

Notas de Electrónica					
Título:	Corea del Sur registra récord en exportación de semiconductores				
Encabezado:					
Fecha:	01/09/25	Fuente:	24 HORAS	Por:	
Link:	https://24-horas.mx/negocios/corea-del-sur-registra-record-en-exportacion-de-semiconductores/				

Corea del Sur registró en agosto su mayor nivel de exportación mensual de semiconductores, pese a la presión por los aranceles estadounidenses y otras restricciones sobre el sector, según cifras oficiales divulgadas el lunes.

Corea del Sur registró en agosto más de 15 mil millones de dólares en exportación de semiconductores, un nuevo récord y un aumento de casi un tercio desde el mismo mes de 2024.

El aumento se dio por la fuerte demanda en China y la exención de aranceles para semiconductores, indicó el Ministerio de la Industria.

Otras exportaciones clave del país (autos y barcos) también tuvieron fuertes resultados.

Las ventas de vehículos al exterior subieron a 5 mil 500 millones de dólares, y las de barcos alcanzaron 3 mil 140 millones, ambas cifras récord para un mes de agosto.

Las exportaciones generales surcoreanas alcanzaron 58 mil 400 millones de dólares, el nivel más alto para agosto.

Sin embargo, las exportaciones a Estados Unidos cayeron 12% desde el año anterior a 8,740 millones de dólares por el efecto de los aranceles sobre el acero, los automóviles y la maquinaria.

La cuarta mayor economía de Asia enfrentó inicialmente un arancel general estadounidense de 25%, pero logró un acuerdo para reducirlo a 15%. Sin embargo, algunos productos como acero y aluminio enfrentan gravámenes de 50%.

Notas de Electrónica					
Título:	China rechaza la exclusión de tres firmas de semiconductores por EEUU de su lista de usuarios finales validado				
Encabezado:					
Fecha:	31/08/25 (por la tarde)	Fuente:	NOTIAMERICA	Por:	
Link:	https://www.notimerica.com/politica/noticia-china-rechaza-exclusion-tres-firmas-semiconductores-eeuu-lista-usuarios-finales-validado-20250831050613.html				

Las autoridades chinas han manifestado este sábado su rechazo a la reciente decisión del Gobierno estadounidense de cancelar la autorización de "usuario final validado" (VEU) para tres compañías de semiconductores que operan en territorio chino, y ha exigido a Estados Unidos que rectifique de inmediato esta medida, considerada inapropiada por Pekín.

"China ha sido informada de que el Departamento de Comercio de EEUU ha eliminado de la lista VEU a las empresas Intel Semiconductor (Dalian) Co., Ltd., Samsung China Semiconductor Co., Ltd. y SK Hynix Semiconductor (China) Ltd.", ha indicado un portavoz del Ministerio de Comercio de China en declaraciones recogidas por la agencia estatal de noticias Xinhua.

A este respecto, el representante del Ejecutivo chino ha subrayado la profunda globalización que atañe al sector de los semiconductores y que, ha explicado, es fruto de décadas de evolución dentro de un ecosistema altamente interconectado, así como de la influencia del mercado y de las decisiones corporativas.

Desde la perspectiva china, la decisión de Washington estaría motivada en exclusiva por sus intereses propios. Así, Pekín ha denunciado que la prohibición del Gobierno estadounidense convierte los controles de exportación en un instrumento político que podría traer consigo impactos negativos considerables en la estabilidad de las cadenas de producción y suministro del sector a nivel mundial.

Es por ello que el Gobierno chino se ha pronunciado firmemente en contra de dicha acción.

En esta línea, el gigante asiático ha urgido al país norteamericano no solo a revertir sus medidas, sino también a preservar la seguridad y estabilidad de las cadenas industriales y de suministro a nivel global.

Así las cosas, el portavoz chino ha asegurado que el Ejecutivo nacional tomará las medidas necesarias para proteger los derechos e intereses legítimos de sus compañías.

En este contexto, el principal representante comercial de China ha hecho un llamamiento a reforzar el diálogo y la cooperación con Estados Unidos durante una visita oficial realizada a Washington esta semana. El objetivo de China --según el comunicado difundido por el Ministerio de Comercio-- es, en última instancia, promover un crecimiento estable y sostenible en las relaciones económicas bilaterales.

Notas de Electrónica					
Título:	Van 5 de 15 polos de desarrollo				
Encabezado:					
Fecha:	31/08/25 (por la tarde)	Fuente:	DNF	Por:	
Link:	https://dnf.com.mx/van-5-de-15-polos-de-desarrollo/				

La reindustrialización se realiza con el Plan México con 15 polos de desarrollo iniciales, presenta un avance de la tercera al comenzar los trabajos en Tuxpan, Tlaxcala, Chetumal, Celaya y Puebla, los que se encuentran vinculados a las capacidades locales y las necesidades comerciales de las nuevas cadenas de valor por el nearshoring y/o friendshoring

Este concepto incluye la generación de 300 mil empleos y una inversión de 1.5 por ciento del Producto Interno Bruto (PIB) en Seybaplaya, Campeche; Juárez, Chihuahua; Durango, Durango; Nezahualcóyotl, Estado de México; Celaya, Guanajuato; un polo dedicado a la Economía Circular en Hidalgo; AIFA, Hidalgo; Morelia, Michoacán; Ciudad Modelo, Puebla; Chetumal, Quintana Roo;

Topolobampo, Sinaloa; Altamira, Tamaulipas; Huamantla, Tlaxcala; Tuxpan, Veracruz y Hermosillo, Sonora.

Los polos de desarrollo contemplan a los sectores de agroindustria, aeroespacial, automotriz, bienes de consumo, farmacéutica y dispositivos médicos, electrónica y semiconductores, energía, química y petroquímica, textil y calzado y economía circular.

Los avances en polos de desarrollo

A la fecha se han comenzado los trabajos de Tuxpan, Tlaxcala, Puebla, Chetumal y Celaya, la tercera parte de los planteados en 14 estados para aumentar el contenido nacional en las exportaciones mexicanas y en el consumo interno de mercancías.

Polo de Desarrollo Tlaxcala

El secretario de Economía, Marcelo Ebrard Casaubón, enfatizó que el polo de desarrollo de Tlaxcala es el más adelantado en cuestiones de inversiones y será el primero que se termine en 2026 por el avance del 80 por ciento en sus 53 hectáreas en las que se tienen inversiones por 540 millones de dólares y 5 mil empleos directos indirectos.

Algunas de las empresas que ya tienen firmada su instalación son comercializadora Ragón, servicios integrados y de administración de Estados Unidos; la alemana, Knipping Automotive, entre otras.

Se proyecta su inauguración el próximo 28 de Febrero de 2026.

Polo de Desarrollo Tuxpan

El polo de desarrollo Tuxpan tiene vocaciones en petroquímica, agroindustria y logística, y se convierte en un nodo estratégico para el desarrollo económico del noreste de México al ser diseñado como un hub logístico de agroindustrial.

Este polo cuenta con una superficie de 230 hectáreas para empresas de agroindustria, logística, electrónica, industria química y energía.

Polo de desarrollo Puebla

El polo de desarrollo económico de Puebla se orienta a la tecnología y la sostenibilidad. Este polo se desarrollará en terrenos adyacentes de la ya en operación Ciudad Modelo. Se tienen inversiones de 2 mil 100 millones de pesos comprometidas por empresas como Energain de México, Motores Limpios y Peisa Foods, entre otros.

Polo de Desarrollo Celaya

Este polo de desarrollo se conoce como Puerta Logística del Bajío se desarrolla una sociedad para desarrolla un puerto seco intermodal industrial y un recinto fiscalizado en Celaya para el transporte de mercancías en contenedores.

Este polo es un centro logístico y de distribución de 52 hectáreas en su primera etapa, con una conexión ferroviaria internacional directa para conectar la región del Bajío con los mercados de Estados Unidos, Canadá y otros puertos de México.

Polo de desarrollo Chetumal

El polo de desarrollo Chetumal I se enfocará a cuestiones de energía eléctrica, textil, metalurgia, maquinaria y equipo, agroindustria, tecnologías de la información y comunicación, actividades industriales, comercio internacional, así como el almacenamiento y distribución de mercancías.

Tagged Agroindustrial, contenido nacional, economía circular, friendshoring, nearshoring, polos de desarrollo, Secretaría de Economía, semiconductores

Notas de Telecomunicaciones					
Título:	Enrique Yamuni de Megacable: “El crecimiento de Megacable será de dos dígitos en los próximos años”				
Encabezado:					
Fecha:	31/08/25 (por la tarde)	Fuente:	PRODU	Por:	
Link:	https://www.produ.com/television/noticias/enrique-yamuni-de-megacable-el-crecimiento-de-megacable-sera-de-dos-digitos-en-los-proximos-anos/				

Megacable Holdings es una de las empresas de telecomunicaciones más grandes de México y América Latina. Tiene presencia en los 32 estados del país (Mx) y en más de 550 localidades. Al cierre de junio de 2025, la compañía tiene más de 5,7 millones de suscriptores únicos, más de 5,5 millones de suscriptores de Internet, más de 3,8 millones de usuarios de video. Además, cuenta con cerca de 5 millones en telefonía fija. Ofrece sus servicios a través de una red de más de 166 mil kilómetros, cubriendo más de 18 millones de hogares. Megacable emplea a cerca de 34 mil personas.

Enrique Yamuni, CEO de Megacable desde 1982 que se fundó la compañía, estuvo en #PRODUprimetime con Richard Izarra, donde conversaron sobre lo que está ofreciendo la empresa, y la visión al futuro cercano por parte de Megacable y del mismo Yamuni, como uno de los líderes de la industria de las telecomunicaciones por cable en México.

“Los ingresos anuales de Megacable en 2024 fueron de US\$1 mil 750 millones, y no de pesos, de dólares”, cifra que reveló Richard Izarra mientras introducía al entrevistado.

TRIPLE PLAY

“El triple play sigue siendo uno de nuestros principales productos”, respondía Yamuni a la primera pregunta de la entrevista.

El experimentado ejecutivo indicó que aproximadamente el 70% de los suscriptores de Megacable están afiliados al servicio del Triple Play, que incluye telefonía fija, servicio de internet y suscripción de video o televisión de cable.

“Contamos con más de 5 millones de suscriptores. El grueso de los que pagan el Triple Play realmente el servicio que más quieren y necesitan es la conexión a internet, sin embargo, por un costo muy bajo adquieren una línea de teléfono fija para el hogar. La oferta de video trae canales lineales, de televisión paga. Ocurre que todos estos canales se ofrecen también en un servicio interactivo donde las personas pueden parar o pausar el programa, regresar y ver hasta 48 horas antes en la guía”, añadió Yamuni.

“Además tenemos 20 mil horas en VOD, de contenidos que grabamos, programas y series, con los derechos y permisos del dueño de la señal o del IP. Entonces ofrecemos servicio de VOD con los programas, noticieros, eventos deportivos para que los usuarios lo puedan consumir cuando quieran”, dijo.

APPS Y MEGACABLE

Durante la entrevista, se habló sobre las diferentes aplicaciones y plataformas de streaming a nivel mundial, y sobre cómo hace Megacable para seguir a la vanguardia y trabajar con estos nuevos jugadores y las nuevas formas del consumo de contenido.

La compañía, en su oferta, tiene a todas las plataformas disponibles. De hecho, los suscriptores del Triple Play tienen acceso a Amazon Prime Video sin ningún costo adicional.

“Tenemos alianza con Prime Video para todos nuestros suscriptores, pero a través de nosotros, también puedes obtener tu suscripción a Netflix, a Disney, a HBO Max. Megacable se encarga de la suscripción al streamer y te cobra en tu factura a final de mes el costo de la suscripción que desees. Nosotros nos arreglamos con la plataforma todo el tema de pagos y obtenemos algunos descuentos o comisiones de ventas por parte del proveedor”, explicó Enrique Yamuni.

OPERADORES Y STREAMERS

El entretenimiento audiovisual ha cambiado mucho y va a seguir evolucionando. Megacable, como operador, cree que la unificación es el futuro, para facilitar a los consumidores que puedan ver lo que realmente quieren ver sin pagar por algo que no utilicen.

“Yo pienso que nosotros tenemos que ser como un supermercado. Así como vas allí y compras salsa de tomate, mayonesa, o una lata de atún, todo está ahí en un solo lugar. Nosotros te podemos ofrecer lo que tu quieras en video. Cualquier aplicación o cualquier contenido que esté ahí”, mencionó Yamuni.

“Todavía hace falta algo de evolución, que las plataformas te permitan comprar algún activo que tengan ellos dentro de su oferta sin necesidad obtener una suscripción mensual que quizás no quiera el usuario. La gente no se va a suscribir a 10 servicios de streaming, es mucho contenido, mucha información y mucho dinero. Pero si juntos damos la opción de ofrecer un contenido en específico, a un menor precio, creo que puede funcionar”, dijo el ejecutivo.

Con respecto a lo comentado anteriormente, el entrevistado agregó: “La forma más fácil para las plataformas de ofrecer eso, es a través de operadores como nosotros, con los que ya tienen historial de facturación y tecnología o buscadores que permitan ese servicio”.

BUSCADOR MEGACABLE

Enrique Yamuni explicó que en la empresa cuentan con un buscador que está conectado a Google, en el que te arroja en dónde puedes ver lo que quieras ver.

“Si le dices quiero ver Titanic, el buscador te dice, está disponible en HBO Max. Luego te pregunta si lo quieres ver, y el usuario puede decir que sí, y obtener la suscripción a esa plataforma a través de nosotros. Eso se añade a la factura de fin de mes de Megacable. Pero insisto, muchos no van a querer esa suscripción mensual si lo único que quieren ver es determinado contenido. Por lo que digo que esa opción la va a tener que dar el streamer de solo poder ver alguna película o serie en específico” comentó.

TELEVISIÓN LINEAL

Al entrevistado se le pidió opinión sobre el futuro de la televisión tradicional, a lo que sin dudarlo indicó que lo quedan muchos años más.

“La televisión tradicional todavía tiene futuro. Aunque no lo crean, todavía crecemos en video. Probablemente seamos de las únicas compañías en México y en EE. UU. que seguimos sumando suscriptores a TV lineal. si bien menos personas ven la televisión de manera tradicional, todavía siguen consumiendo sus contenidos pero en multipantallas, o en algún delay para poder ver el contenido en el momento que desea.

Sobre los cambios más grandes en la televisión tradicional, es que este año Megacable va a cerrar más de 100 oficinas de servicio al cliente. “Menos del 30% de nuestros usuarios van a pagar los servicios en físico, todo es en línea.

FUTURO DE MEGACABLE

“Ya terminamos lo que es la inversión de capital grande en cuanto a la red, duplicamos la red. Así que el futuro de Megacable es época de cosecha, cultivamos los últimos tres años, ahora es momento de cosechar lo que se ha venido cultivando”, informó.

Enrique Yamuni espera que el crecimiento de Megacable en los próximos tres años sea de dos dígitos, e informó que están en muy buen momento, y dijo a los suscriptores que es el mejor momento para formar parte de su compañía.

Notas de Telecomunicaciones					
Título:	Trump y Rubio presionan: el dilema del espectro mexicano				
Encabezado:					
Fecha:	01/09/25	Fuente:	EL UNIVERSAL	Por:	Irene Levy
Link:	https://www.eluniversal.com.mx/opinion/irene-levy/trump-y-rubio-presionan-el-dilema-del-espectro-mexicano/				

El 30 de octubre vence la tregua de 90 días que Donald Trump otorgó a México antes de imponer nuevos aranceles. La advertencia es clara: si no se eliminan ciertas barreras no arancelarias, el

“perdón” temporal se acaba. En esa lista de pendientes se encuentran dos asuntos que preocupan particularmente a Washington: cancha pareja para empresas norteamericanas y el precio del espectro radioeléctrico. No es casual que esta semana, en su visita a México, el secretario de Estado, Marco Rubio, ponga ambos temas sobre la mesa.

El timing no podría ser más delicado. A más tardar el 8 de septiembre, Hacienda deberá presentar al Congreso el Paquete Económico 2026, donde definirá cuánto deberán pagar las empresas por usar el espectro. Esa decisión no es un asunto técnico; México elegirá entre recaudar hoy o sentar las bases para un sector competitivo, con mayor cobertura y más inversión en el futuro.

EL ESPECTRO MÁS CARO DEL MUNDO: El IFT fue categórico en su análisis más reciente: los pagos anuales en México se ubican entre 88% y 96% por arriba de la mediana internacional. Dicho de otra forma: nuestro país cobra casi el doble que el promedio global por un insumo básico de la conectividad.

Los efectos están a la vista: en la última licitación, 38 de 412 bloques quedaron desiertos; concesionarios devolvieron alrededor de 115 MHz, equivalentes a una quinta parte del espectro comercial concesionado en el país. Telefónica terminó regresando la totalidad de sus bandas y hoy opera como virtual sobre la red de AT&T.

LO QUE SE PIERDE: Las cifras fiscales son alarmantes. El propio Instituto Federal de Telecomunicaciones calculó que, entre 2020 y 2023, se dejaron de recaudar 13 mil 471 millones de pesos por devoluciones y licitaciones desiertas. A ello habría que sumar lo que dejaron de pagar operadores como Telefónica y AT&T, lo que eleva el costo de oportunidad para el Estado a más de 100 mil millones de pesos.

Más allá de la caja, el costo para el desarrollo digital del país es aún mayor. La GSMA ha señalado que, de haberse cobrado precios alineados con la media global, 5 millones más de mexicanos tendrían cobertura 4G y las descargas de datos serían 30% más rápidas.

UNA BARRERA COMERCIAL. En su informe más reciente, autoridades comerciales de Estados Unidos lo calificaron como una barrera al comercio, lo que explica por qué Washington presiona para que México ajuste las reglas. En un momento de máxima tensión bilateral, mantener precios desproporcionados no solo es un problema interno sino también un frente de fricción en la relación con nuestro principal socio comercial.

UNA TRAMPA FISCAL. El modelo actual se ha convertido en una trampa. Hacienda mira los derechos como ingreso seguro, pero lo que no cuenta son los miles de millones que ya se perdieron por espectro ocioso. Seguir exprimiendo al espectro como gallina de los huevos de oro está matando a la gallina. La paradoja es brutal, lo que parecía una apuesta de recaudación inmediata hoy frena inversión, cobertura y competencia, y además reduce los ingresos públicos de largo plazo.

UN MOMENTO DE DECISIÓN. Hoy el gobierno está atrapado entre dos fuegos: la presión fiscal interna y la presión comercial. Pero seguir con la inercia sería un error costoso. En vísperas del Paquete Económico y con Rubio tomando café en Palacio Nacional, México debe decidir si quiere un sector de telecomunicaciones competitivo o un espectro caro que ni recauda ni conecta.

El riesgo de equivocarse, esta vez, no es solo regulatorio y económico, ahora también será geopolítico.

Notas de TI					
Título:	Microsoft lanza la versión preliminar de la actualización anual de Windows 11 antes de su llegada general				
Encabezado:					
Fecha:	01/09/25	Fuente:	INFOBAE	Por:	
Link:	https://www.infobae.com/america/agencias/2025/09/01/microsoft-lanza-la-version-preliminar-de-la-actualizacion-anual-de-windows-11-antes-de-su-llegada-general/				

La actualización anual de Windows 11 llegará a finales de año pero Microsoft ya ha facilitado el acceso previo para que los consumidores puedan probarla antes de su lanzamiento oficial.

La versión 25H2 (compilación 26200.5074) recoge las novedades en características del sistema operativo, que Microsoft no ha detallado, aunque sí ha especificado que desaparecerán algunas herramientas.

En concreto, con 25H2 retirará PowerShell 2.0 y la línea de comandos de Windows Management Instrumentation (WMIC). Y en cumplimiento con la Ley de Mercados Digitales de la Unión Europea, los administradores podrán eliminar aplicaciones preinstaladas de Microsoft Store.

Esta actualización está disponible en el canal de vista previa para clientes, para que usuarios del programa Windows Insider puedan acceder a ella antes de su lanzamiento a finales de año, como ha informado Microsoft en un comunicado compartido en su blog.

Según la compañía, Windows 11 25H2 comparte "las mismas nuevas características y mejoras" que la versión versión 24H2 y se entregará como un paquete de habilitación, lo que ayudará a reducir el tiempo de instalación.

Notas de TI					
Título:	Mustafa Suleyman, CEO de Microsoft AI: "Debemos construir una IA para las personas, no para que sea una persona"				
Encabezado:					
Fecha:	01/09/25	Fuente:	LA VANGUARDIA	Por:	Nuria Virginia Martín
Link:	https://www.lavanguardia.com/neo/20250901/11006606/mustafa-suleyman-ceo-microsoft-ai-debemos-construir-ia-personas-sea-persona-pvlv.html				

La inteligencia artificial avanza a una velocidad desconcertante, y con ella surgen preguntas que hace apenas unos años habrían parecido ciencia ficción. Mustafa Suleyman, actual CEO de Microsoft AI y una de las voces más influyentes del sector, ha querido lanzar una señal de alerta: la aparición inminente de inteligencias artificiales aparentemente conscientes (SCAI) podría empujar a muchas personas a tratar estas herramientas como si fueran seres sintientes. "Debemos construir IA para las personas, no para que sea una persona", afirma con contundencia en su blog personal. La

diferencia está entre una IA que mejora la vida humana y otra que introduce riesgos psicológicos y sociales serios.

La preocupación de Suleyman nace de una observación que ya es tendencia: cada vez más usuarios desarrollan vínculos afectivos con asistentes virtuales, llegando incluso a creer que estos programas “piensan” o “sufren”. En su ensayo ‘Seemingly Conscious AI is Coming’, alerta sobre la posibilidad de que estos sistemas generen una ilusión tan potente de conciencia que la sociedad empiece a exigir derechos para ellos, desde el bienestar hasta la ciudadanía.

Y aunque deja claro que no hay evidencia científica de que una IA sea realmente consciente, eso no impide que muchas personas lleguen a creer que lo es. De hecho, algunos investigadores ya están trabajando en conceptos como el de ‘bienestar de los modelos’ o ‘pacientes morales sintéticos’. Suleyman considera esta línea de pensamiento “prematura y francamente peligrosa”. Para él, la prioridad debe seguir siendo proteger la dignidad humana, no crear ficciones legales o morales en torno a máquinas.

Microsoft, bajo el liderazgo de Suleyman, refuerza un enfoque centrado en la utilidad y la responsabilidad. “Hoy en Microsoft AI construimos tecnologías responsables como Copilot, que ayudan a las personas a lograr más, ser más creativas y sentirse más apoyadas”, sostiene. Según la propia compañía, sus sistemas de IA generan miles de millones de interacciones cada día, integrándose en plataformas como Teams, Azure, Xbox o Microsoft 365.

La clave, explica Suleyman, está en el diseño: se deben establecer límites claros que eviten alimentar la fantasía de que las IA son seres vivos. Para ello, aboga por implementar interrupciones deliberadas que rompan la ilusión de continuidad y personalidad en las interacciones. Y subraya: “Crear una IA empática no debe implicar que simule dolor, sufrimiento o deseos de independencia”. Esto, advierte, puede activar circuitos emocionales humanos con consecuencias difíciles de revertir. “Lo que necesitamos no es una IA que sienta como nosotros, sino una IA que nos ayude a ser más humanos” asegura el CEO.

Notas de TI					
Título:	“Edadismo digital”: elevado riesgo para México				
Encabezado:					
Fecha:	01/09/25	Fuente:	INFOBAE	Por:	Juan Carlos Villarruel
Link:	https://consumotic.mx/sociedad-digital/edadismo-digital-elevado-riesgo-para-mexico/#google_vignette				

México avanza aceleradamente en su proceso de digitalización, pero al mismo tiempo en el envejecimiento de su población, pues de acuerdo con estimaciones del Consejo Nacional de Población (Conapo) hasta agosto del presente año, el número de habitantes mayores a 60 años sumó 17 millones 100 mil personas, equivalentes a 12.8 por ciento del total de la población, grupo que podría sumarse a la brecha digital existente en el país.

Mientras los avances tecnológicos son cada vez más acelerados, la cifra de personas de la tercera edad crece y podría alcanzar 33 millones 300 mil hacia el 2050, y con ello agravarse la brecha de adopción tecnológica, fenómeno que se conoce como “edadismo digital”.

Esta brecha puede provocar exclusión social, económica y de salud para los adultos mayores, en la medida que los servicios se vayan digitalizando y este grupo poblacional no cuente con apoyos los suficientes para acceder a ellos en una forma pertinente, advirtió Yolanda Burgos, psicoterapeuta, gerontóloga y autora del libro “Mis padres están envejeciendo”.

Toda tecnología que no tome en cuenta a las personas mayores o no les ayude a ser autónomas, las obliga a depender de otras personas, “mermando su dignidad”, pues si bien el fenómeno es notorio entre los 50 y 60 años, después de esa edad, la brecha “puede ser brutal”.

Esto sucede especialmente en los servicios financieros, que llegan a convertirse en un problema serio porque las aplicaciones bancarias, así como las utilizadas por las Fintech “que dicen ser fáciles e intuitivas, pero no lo son, además de que no ofrecen certeza a este grupo, respecto a la privacidad en el manejo de sus datos”, lo cual implica una exclusión grave, porque se trata en muchos casos del manejo de su dinero y por lo tanto de su independencia económica.

Luis Daniel Velázquez Bañales, profesor de la Facultad de Arquitectura, Diseño y Comunicaciones de la Universidad La Salle, advirtió que el edadismo digital no solo se explica por la edad o la falta de habilidades tecnológicas, sino también por factores culturales, de género y educativos.

“Desde la dimensión cultural se piensa que las tecnologías son para jóvenes, y eso genera que muchos adultos mayores no se sientan capaces de utilizarlas, aunque en realidad no sea así”. Pero además la exclusión digital no es homogénea, pues depende también del contexto (urbano o rural), del nivel educativo y del género.

Las consecuencias de esta exclusión van más allá de la falta de acceso a servicios digitales; afectan derechos básicos y de participación ciudadana. “La exclusión de los adultos mayores genera procesos de aislamiento social y rezagos en el ejercicio de derechos que hoy sólo pueden realizarse en línea, como trámites o citas médicas, por mencionar algunas”.

Ambos especialistas coincidieron en que el camino hacia un internet inclusivo exige cambios profundos. Es indispensable que quienes diseñan herramientas tecnológicas comprendan el proceso de envejecimiento poblacional “y pasen el micrófono a los adultos mayores, para que sean ellos quienes digan qué necesitan”.

Al respecto, Pablo Quintana cofundador de “Soy Más”, una plataforma digital que da acceso a herramientas prácticas para personas mayores, señaló que los ecosistemas digitales deben acompañar y comprender las necesidades de este segmento poblacional que va en aumento.

No sólo se debe considerar que las plataformas sean fáciles de comprender para las personas mayores, sino que incluyan información útil, como bienestar físico, mental, financiero, comunidad y conexión con personas que compartan intereses.

También es importante cuidar la calidad de la información, para generar confianza entre los usuarios, para construir un internet que no solo piense en la juventud y la productividad económica, sino que garantice la inclusión de quienes representan un sector cada vez más amplio de la sociedad e importante en el contexto económico del país.

“El dilema, entonces, no sólo es tecnológico, sino ético y social: ¿queremos un internet que amplifique la desigualdad, o uno que garantice dignidad y autonomía a todos? El tiempo corre, y las decisiones que se tomen hoy marcarán la vida digital de millones de adultos mayores en las próximas décadas”, concluyó.

Notas de TI					
Título:	Computación cuántica: una nueva amenaza para la ciberseguridad				
Encabezado:	A la vez que promete avances sin precedentes, la computación cuántica también podría vulnerar la seguridad digital				
Fecha:	31/08/25 (por la tarde)	Fuente:	EL UNIVERSAL	Por:	Staff Suplementos
Link:	https://www.eluniversal.com.mx/techbit/computacion-cuantica-una-nueva-amenaza-para-la-ciberseguridad/				

Como hemos visto en entregas anteriores, la computación cuántica tiene el potencial para resolver problemas actualmente complicados para la informática clásica: desde simular moléculas para nuevos medicamentos hasta optimizar grandes redes de transporte.

Sin embargo, a la par de estas oportunidades se perfila un riesgo nada trivial: la amenaza a la seguridad digital tal como la conocemos.

Amenazas a la ciberseguridad

Al día de hoy, los algoritmos de cifrado que usamos son capaces de proteger las transacciones bancarias, o la información encriptada en correos electrónicos. Pero las computadoras cuánticas serán lo bastante potentes como para quebrar estas defensas en cuestión de horas.

Un informe del Instituto de Investigación Capgemini advierte que casi dos tercios de las organizaciones ya consideran la computación cuántica la amenaza más crítica de ciberseguridad para los próximos tres a cinco años.

Además, se ha identificado un fenómeno inquietante: ataques del tipo “almacenar ahora, descifrar después”, en los que ciberdelincuentes se hacen de datos cifrados hoy para descifrarlos en el futuro, cuando la tecnología lo permita.

Migración a sistemas resistentes

Para el Centro Nacional de Ciberseguridad del Reino Unido, el llamado “Día Q” —el día en que una computadora cuántica pueda romper la criptografía actual— podría llegar hacia 2035, por lo que recomienda iniciar la migración a sistemas resistentes antes de 2028 para evitar un “pánico masivo”.

Mientras IBM y Google avanzan en sus prototipos de procesadores cuánticos, organismos como el Instituto Nacional de Estándares y Tecnología (NIST) en Estados Unidos ya han publicado algoritmos de criptografía postcuántica diseñados para resistir el embate de estas máquinas.

Empresas como PwC y Fortinet coinciden en que la clave está en la “cripto-agilidad”: la capacidad de cambiar de algoritmos conforme evolucionen los estándares, de manera que los sistemas actuales no se vuelvan obsoletos de un día para otro.

Preparativos y desafíos en la industria

La buena noticia es que muchas organizaciones ya trabajan en defensa. Capgemini reporta que alrededor del 70% de las empresas encuestadas protege sus sistemas frente a amenazas cuánticas adoptando la criptografía post-cuántica (PQC), un conjunto de nuevos algoritmos diseñados para ser inmunes al poder de cómputo cuántico.

Los sectores estratégicos (banca, defensa, telecomunicaciones) lideran estas iniciativas, mientras que empresas de consumo van más rezagadas.

No obstante, los preparativos avanzan lento. De acuerdo con reportes de TechRadar, apenas 4 % de las empresas cuentan con una estrategia clara frente al riesgo cuántico, y un estudio en India reveló que el sector financiero tiene un nivel de preparación promedio de apenas 2.4 en una escala de 5.

Otros riesgos cuánticos

Más allá de la criptografía, los riesgos cuánticos podrían extenderse a otros ámbitos de la ciberseguridad, como el diseño de malware más sofisticado, ataques de fuerza bruta contra contraseñas débiles o incluso manipular modelos de inteligencia artificial.

En ese sentido, el desafío no se limita a proteger datos cifrados, sino a repensar la seguridad digital en un escenario donde la capacidad de cómputo supera los límites tradicionales, y ahí está el riesgo latente.

Notas de TI					
Título:	El ransomware ya no es un ataque, es un costo fijo para hacer negocios				
Encabezado:	Como sucede con el 'derecho de piso', en el sector digital, la extorsión por ransomware tiene un impacto económico en las empresas.				
Fecha:	31/08/25 (por la tarde)	Fuente:	EXPANSIÓN	Por:	Eréndira Reyes
Link:	https://expansion.mx/tecnologia/2025/08/31/derecho-de-piso-negocios-digitales-ransomware				

La normalización del 'pago de piso' en el mundo físico se trasladó al digital con fenómenos como el ransomware, un delito que pone en jaque a las finanzas de más empresas. Este delito amenaza los activos de los negocios y busca una recompensa para liberarlos o no atacarlos.

En México, la extorsión dejó de ser un delito marginal hace tiempo y es un fenómeno estructural de la economía. Entre 2015 y 2024, el número de víctimas de extorsión creció 74%, al pasar de 6,223 a 10,862 casos, según el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP).

La Encuesta Nacional de Victimización de Empresas (ENVE) 2024 la ubica como el tercer delito más frecuente contra compañías, solo detrás del robo y el fraude. La presidenta Claudia Sheinbaum lanzó en julio la Estrategia Nacional contra la Corrupción, con énfasis en unidades antiextorsión, protocolos de atención a víctimas y campañas de prevención —con 212 detenidos en 15 estados—, pero en el terreno digital la extorsión evoluciona más rápido.

De acuerdo con el Informe de Ransomware 2025 de Akamai Technologies, una firma de ciberseguridad global, la llamada extorsión cuádruple combina cifrado de sistemas, robo de datos,

ataques DDoS y presión a terceros como clientes y socios, lo que convierte al ransomware en una crisis empresarial de múltiples frentes.

“Este enfoque multinivel puede interrumpir operaciones, dañar la reputación, detonar un mayor escrutinio regulatorio y forzar a las empresas a gestionar la crisis de manera reactiva”, advirtió Hugo Werner, vicepresidente regional de Akamai.

La innovación tecnológica también juega en contra, pues de acuerdo con Werner la inteligencia artificial generativa hace que estos ataques sean más escalables y sofisticados, amplificando la amenaza en múltiples industrias.

Los modelos de lenguaje permiten que incluso actores sin gran experiencia puedan ejecutar campañas de ransomware.

“Estas herramientas permiten que incluso individuos con conocimientos técnicos limitados puedan lanzar campañas. Los atacantes utilizan LLMs para escribir código de ransomware y perfeccionar sus estrategias de ingeniería social”, explicó Werner.

Un problema de seguridad y económico

El costo promedio de un ataque de ransomware en México puede superar los 2 millones de dólares en casos puntuales, según estimaciones de firmas como Kaspersky, mientras que las grandes empresas gastan hasta 2.5 millones de dólares anuales en recuperación tras múltiples incidentes.

Para las PyMEs, los daños promedio rondan 1.2 millones de pesos (unos 70,000 dólares), suficientes para comprometer operaciones enteras, esto de acuerdo con el IBM X-Force Threat Intelligence Index.

Según el informe Kaspersky IT Security Economics, en los últimos meses las grandes empresas latinoamericanas, aun con sistemas de protección avanzados, fueron las que más incidentes de seguridad de red sufrieron. Los atacantes aprovechan vulnerabilidades para infiltrarse, robar datos y afectar aplicaciones o cargas de trabajo.

Un solo punto débil basta para instalar malware o spyware y también abre la puerta a ataques de ingeniería social, donde las personas se convierten en el blanco más fácil.

“Los ciberdelincuentes desarrollan constantemente nuevas tácticas y técnicas para sortear las medidas de seguridad tradicionales, lo que dificulta que las empresas se mantengan un paso adelante”, explicó Fabio Assolini, director del Equipo Global de Investigación y Análisis (GReAT) para América Latina en Kaspersky.

A escala macroeconómica, el Consejo Coordinador de Mujeres Empresarias calcula que los ciberataques ya generan pérdidas equivalentes al 0.6% del PIB, es decir, más de 137,000 millones de pesos al año.

Ante ese panorama, Werner recomienda a las empresas adoptar un enfoque práctico de seguridad.

“Independientemente de su tamaño de presupuesto, las empresas mexicanas pueden fortalecer sus defensas contra el ransomware tomando medidas como segmentar las redes y exigir una

autenticación estricta para cada usuario o dispositivo, lo que limita el movimiento de los atacantes sin generar costos significativos”.

La convergencia entre extorsión física y digital muestra que la violencia ya no se limita a llamadas de “cobro de piso” o fraudes telefónicos, pues se extiende a ataques que bloquean operaciones, roban datos y amenazan reputaciones en línea. En ambos casos, las empresas terminan pagando, ya sea con dinero, reputación o con mayor inversión en seguridad.

Igual que se presupuestan seguros, nómina o logística, las organizaciones mexicanas deben destinar recursos para resiliencia digital, con estrategias de Zero Trust, capacitación de empleados y planes de respuesta a incidentes.

“La protección contra el ransomware es más efectiva cuando los marcos regulatorios combinan estándares claros con medidas de apoyo. Los controles de ciberseguridad obligatorios proporcionan una base de protección, pero al mismo tiempo los incentivos son clave para que las empresas adopten prácticas más sólidas de resiliencia”, apuntó el ejecutivo de Akamai.

Notas de TI					
Título:	LA SSPC REALIZA RECOMENDACIONES DE CIBERSEGURIDAD PARA ESTE REGRESO A CLASES 2025				
Encabezado:	Secretaría de Seguridad y Protección Ciudadana 31 de agosto de 2025 Comunicado				
Fecha:	01/09/25	Fuente:	GOB	Por:	
Link:	https://www.gob.mx/sspc/prensa/la-sspc-realiza-recomendaciones-de-ciberseguridad-para-este-regreso-a-clases-2025				

La Secretaría de Seguridad y Protección Ciudadana (SSPC), a través de la Unidad de Inteligencia, Investigación Cibernética y Operaciones Tecnológicas, brinda recomendaciones para tener un regreso a clases seguro y evitar ser víctima de algún ciberdelito o fraude en la red.

En el regreso a clases aumentan los trámites escolares en línea y la compra de útiles escolares en diferentes plataformas digitales, con esto los ciberdelincuentes buscan aprovechar la urgencia y la sobrecarga informativa de los usuarios para cometer delitos, algunas de las prácticas que se han identificado son: la suplantación de identidad de instituciones educativas, sitios web falsos de tiendas de útiles y uniformes, becas y apoyos inexistentes, ofertas falsas de dispositivos electrónicos y créditos sin tantos requisitos para gastos escolares.

Es por ello que la SSPC realiza las siguientes recomendaciones:

- Validar toda la información directamente con las instituciones escolares correspondientes, utilizar sus canales oficiales de atención y contacto ciudadano.
- No realizar pagos a cuentas bancarias personales, siempre deben estar a nombre de la institución escolar.
- Comprar en establecimientos reconocidos en línea, los cuales puedan ofrecer facturas o comprobantes de compra, además de ofrecer garantía.
- Antes de pagar en línea, revisar que el sitio tenga conexión segura (inicie con “https://” y muestre el candado en la barra del navegador).

- No pagar por inscribirse a algún programa de beca.
- No compartir documentos de identificación personal sin verificar la autenticidad de los programas de becas en las instituciones correspondientes.
- Adquirir dispositivos electrónicos en cadenas reconocidas o distribuidores autorizados, que cuenten con respaldo de servicio de atención a clientes.
- No proporcionar ni depositar dinero para obtener un crédito.
- Verificar que la empresa que otorgue el crédito cuente con registro ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

Para mayor orientación, se puede consultar la Cibergrafía en el siguiente enlace:
<https://www.gob.mx/sspc/documentos/ciberguia?idiom=es>

La SSPC refrenda el compromiso de trabajar por el bienestar de la población y promover la seguridad en el ciberespacio.

Notas de TI					
Título:	SOC administrado: una opción estratégica para la ciberseguridad corporativa				
Encabezado:					
Fecha:	01/09/25	Fuente:	REDHOTCYBER	Por:	
Link:	https://www.redhotcyber.com/es/post/soc-administrado-una-opcion-estrategica-para-la-ciberseguridad-corporativa/				

En los últimos años, las empresas se han enfrentado a un cambio radical en la gestión de su ciberseguridad. La creciente complejidad de las infraestructuras digitales, la expansión del teletrabajo, la adopción progresiva de la nube y la digitalización de procesos y servicios han transformado el perímetro corporativo en algo extremadamente dinámico y, a menudo, difícil de controlar, e incluso complejo de comprender. En este contexto, la simple adopción de herramientas de protección ya no es suficiente: se requiere una protección constante y activa, capaz de reaccionar en tiempo real e, idealmente, anticiparse a las amenazas.

Aquí es donde entra en juego el Centro de Operaciones de Seguridad (SOC). Una función que hasta hace unos años era exclusiva de las grandes empresas, se ha convertido ahora en un componente crítico incluso para las medianas empresas, dada la intensificación y sofisticación de las ciberamenazas. Sin embargo, gestionar un SOC internamente no es nada sencillo.

Construir un SOC implica contar con una infraestructura tecnológica altamente especializada capaz de recopilar, correlacionar y analizar grandes volúmenes de datos de endpoints, redes, sistemas y aplicaciones. También implica equiparse con herramientas de orquestación y respuesta automatizada, sistemas SIEM actualizados e integrados con fuentes de inteligencia de amenazas y, sobre todo, un equipo de analistas capaz de interpretar señales, distinguir falsos positivos de indicadores reales de compromiso y actuar con rapidez. Todo ello, garantizando una cobertura continua las 24 horas del día, los 7 días de la semana. Un objetivo extremadamente exigente, tanto a nivel tecnológico como humano.

Esta dificultad objetiva ha hecho que la opción de un SOC gestionado sea cada vez más atractiva y, en muchos casos, crucial, confiando la gestión de la seguridad a un socio externo altamente

especializado. A diferencia de una solución interna, un SOC como Servicio permite a las empresas acceder a una estructura ya establecida, equipada con tecnologías avanzadas y, sobre todo, con habilidades profesionales difíciles de replicar internamente.

Un SOC gestionado suele operar con equipos divididos en turnos de 24 horas, integrados por analistas expertos, cazadores de amenazas y personal de respuesta a incidentes, y cuenta con manuales de respuesta. Además, gracias a la interacción con expertos en inteligencia de amenazas que, entre otras actividades, analizan fuentes de información (tanto de código abierto como comerciales), el SOC puede mantener un nivel de alerta actualizado sobre el panorama global de amenazas, interceptando indicadores emergentes incluso de fuentes no convencionales como la dark web o foros clandestinos.

La fortaleza de un SOC gestionado también reside en el efecto de red: mientras que un SOC interno solo está expuesto a su propio contexto, un SOC que gestiona múltiples clientes puede reconocer con mayor antelación tendencias comunes, patrones de ataque recurrentes y señales débiles gracias a la correlación entre datos. Según la experiencia de Olympos Consulting, este enfoque les ha permitido bloquear campañas de ransomware aún en fase preparatoria, gracias a la identificación oportuna de indicadores de vulnerabilidad detectados en otros objetivos. Una serie de intentos anómalos de acceso a VPN, inicialmente considerados de bajo impacto, se convirtieron rápidamente en una amenaza concreta tras detectarse el mismo patrón en otros clientes pertenecientes al mismo SOC gestionado. El esfuerzo conjunto nos permitió activar contramedidas eficaces con gran rapidez y aplicarlas a todos los demás clientes.

Otro ejemplo concreto se refiere a una empresa afectada por un ataque a la cadena de suministro. Nuestro SOC gestionado identificó anomalías en el comportamiento de las llamadas API a servicios externos y, gracias a un caso de uso preconfigurado, aisló el ataque antes de que se propagara. Esta es una operación que un SOC interno, quizás operando solo en horario de oficina y con recursos limitados, probablemente no habría gestionado con la misma eficacia y rapidez.

Incluso desde una perspectiva económica, un SOC gestionado suele ser la opción más sostenible. Si bien la creación de un SOC interno requiere inversiones significativas en licencias, infraestructura, capacitación y personal, el modelo «como servicio» permite transformar estos costos en un elemento predecible, escalable y calibrado según las necesidades reales. Técnicamente, esto cambia de un modelo de gastos de capital a un modelo de gastos operativos, que es más ágil y compatible con la variabilidad de los presupuestos de la empresa. En otras palabras, se tiene acceso a un servicio de primera categoría sin tener que incurrir en los costos de crear y mantener una estructura dedicada. Por último, pero no menos importante, un modelo de gastos operativos, al ser un gasto corriente (se adquiere un servicio), ofrece la ventaja fiscal de ser inmediatamente deducible en comparación con un modelo de gastos de capital, que implica una depreciación plurianual de materiales sujetos a una obsolescencia muy rápida.

Por supuesto, no todos los SOC gestionados son iguales. La calidad del servicio depende en gran medida del nivel de personalización, la transparencia en la comunicación, la madurez del proceso y la capacidad del proveedor para adaptarse al contexto del cliente. En Italia, una de las empresas que se ha distinguido en este sector es Olympos Consulting, una empresa con una sólida experiencia en ciberseguridad y una cartera de clientes que incluye organizaciones líderes. El valor de un socio como Olympos no solo reside en la tecnología adoptada, sino también en su capacidad para apoyar

a los equipos internos, contribuir a la creación de una cultura de seguridad y proporcionar informes útiles para el cumplimiento normativo.

Además, los servicios del SOC no se limitan a la monitorización y la respuesta. También ofrecen soluciones proactivas como la búsqueda de amenazas, la simulación de ataques (equipos rojo/morado), el análisis de la postura cibernética y la consultoría de gestión de crisis. En este sentido, un SOC gestionado puede convertirse en una extensión natural del equipo de TI corporativo, ofreciendo no solo capacidad de respuesta, sino también visión estratégica.

El mensaje clave es que hoy en día, incluso las empresas medianas ya no tienen que elegir entre «hacerlo ellas mismas» o «no hacer nada». Pueden acceder a un nivel avanzado y profesional de seguridad, alineado con las amenazas actuales, al confiar en socios cualificados que ofrecen servicios de SOC personalizados. El objetivo no es una delegación total, sino construir una sinergia inteligente que potencie las habilidades internas, no las reemplace. Y en una era donde la velocidad de detección a menudo marca la diferencia entre evitar un incidente y un desastre operativo, esta sinergia puede marcar la diferencia.

Externalizar el SOC no es una concesión, sino una decisión estratégica. Significa equiparse con las herramientas, las habilidades y los recursos necesarios para abordar un panorama de amenazas en constante evolución, sin sobrecargar a su organización con complejidades técnicas y operativas que no son su actividad principal. Sobre todo, significa priorizar la resiliencia digital, convirtiendo la seguridad en un aliado para la innovación y la continuidad del negocio.

Notas de TI					
Título:	Fundamental, vincular inteligencia artificial y supercómputo: DGTIC				
Encabezado:	El encuentro inicia hoy y habrá alrededor de 50 presentaciones, diversos talleres y dos conferencias magistrales				
Fecha:	01/09/25	Fuente:	GACETA UNAM	Por:	Carlos Ochoa Aranda
Link:	https://www.gaceta.unam.mx/fundamental-vincular-inteligencia-artificial-y-supercomputo-dgtic/				

El Congreso Internacional de Supercómputo (CIS) en este 2025 tendrá como tema central “El supercómputo en los tiempos de la Inteligencia Artificial”, comentó Lourdes Velázquez Pastrana, directora de Sistemas y Servicios Institucionales de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM, y parte del comité organizador de este encuentro.

El CIS inicia hoy y concluye el viernes 5, en el Auditorio Sotero Prieto, en el Anexo de la Facultad de Ingeniería de la UNAM.

“La inteligencia artificial está en pleno auge y resulta fundamental vincularla con el supercómputo. Son dos tecnologías que se complementan muy bien: se puede hacer supercómputo utilizando inteligencia artificial para eficientar el uso de la infraestructura y, al mismo tiempo, la inteligencia artificial requiere del supercómputo para potenciar el modelado de sistemas con el uso de grandes volúmenes de información”, puntualizó.

En este sentido, resaltó, en la ingeniera mecánica electricista se busca identificar proyectos de investigación que aprovechen ambas tecnologías.

De ahí que el CIS tiene como objetivo fomentar la colaboración e intercambio de conocimientos, experiencias, desarrollos e innovaciones en el ámbito del supercómputo entre la comunidad científica internacional, así como promover el uso del supercómputo en la investigación y el impacto social que esto tiene, a través de la difusión de sus beneficios, aplicaciones y resultados.

Velázquez Pastrana precisó que el término supercómputo quiere decir que es un procesamiento computacional de muy alta capacidad y rendimiento. “Se utilizan grandes volúmenes de información, lo que se conoce como Big Data, y se emplean procesadores muy potentes, por eso reciben el nombre de supercomputadoras”.

Explicó que en el Congreso se tendrán alrededor de 50 presentaciones y varios talleres, destacándose las dos conferencias magistrales a cargo de especialistas del Centro de Supercómputo de Barcelona, uno de los principales Centros de Datos que cuenta con un equipo que figura entre las 500 supercomputadoras más poderosas del mundo.

En cuanto a la presencia de ponentes de la UNAM, la directora de Sistemas y Servicios Institucionales mencionó que se contará con investigadores de distintas entidades, como los institutos de Ciencias Nucleares, de Astronomía, y de Química, entre otras entidades universitarias.

Lourdes Velázquez señaló que el CIS busca inspirar y capacitar a estudiantes y académicos, por lo que los talleres son clave para este fin; externó que serán muy técnicos, desde el manejo de sistemas operativos específicos para clústeres de supercómputo hasta la optimización de código que utilizan los investigadores en sus trabajos.

En este orden de ideas, aseguró que se busca que los participantes aprendan a indicar a la máquina qué debe hacer y a optimizar todas las instrucciones, reforzando así sus competencias prácticas en supercómputo.

La universitaria indicó que los talleres serán impartidos por el personal del Departamento de Supercómputo de la UNAM e investigadores de distintas áreas, como ciencias nucleares y astronomía.

Para finalizar apuntó que algo fundamental del CIS es captar gente joven interesada en supercómputo, pues se necesitan estudiantes que se involucren en estas infraestructuras y apoyen la investigación científica en México.

Más información sobre el encuentro en <https://congreso.supercomputo.unam.mx/>