Notas de Electrónica					
Título:	Hereu invita a las empresas a concurrir a la tercera convocatoria del Perte Chip, dotada con 33 millones				
Encabezado:					
Fecha:	15/09/25	Fuente:	BOLSAMANIA	Por:	
Link:	https://www.bolsamania.com/noticias/empresas/economia--hereu-invita-a-las-empresas-a-concurrir-a-la-tercera-convocatoria-del-perte-chip-dotada-con-33-millones--20887770.html#google_vignette				

El ministro de Industria y Turismo, Jordi Hereu, ha invitado a las empresas de semiconductores a que concurran a la tercera convocatoria del Perte Chip, dotada con 33 millones de euros y lanzada el pasado 1 de septiembre, para "seguir llevando adelante proyectos de innovación".

Durante la inauguración de una nueva planta de la empresa Trace ID, Hereu ha destacado a la industria del chip como un sector "fundamental" para avanzar en proyectos "innovadores" que den "autonomía estratégica" a España.

Asimismo, el titular de Industria ha recordado que el Perte Chip --cuyo objetivo es reforzar las capacidades de diseño y producción de la industria de la microelectrónica y los semiconductores en España-- está dotado con más de 12.000 millones de euros en términos globales que gestionan varios ministerios (en lo que compete a su departamento, ya hay unos 330 millones de euros invertidos).

Jordi Hereu ha incidido en que la industria 4.0 es "una de las industrias más importantes" porque ayuda a ganar en tecnificación, aporta inteligencia y más competitividad a todos los sectores industriales.

El titular de Industria ha añadido durante la visita a la planta catalana que las etiquetas de identificación de radiofrecuencia son una de las tecnologías que ayudan a la logística, la automoción, el sector textil y "cualquier industria que mueve objetos y productos a través de la identificación".

Notas de Electrónica					
Título:	Taiwán y el Reino Unido firman un memorando de entendimiento sobre la capacitación de personal en semiconductores				
Encabezado:					
Fecha:	15/09/25	Fuente:	NOTICIAS NAT	Por:	
Link:	https://noticias.nat.gov.tw/Econom%C3%ADa/Noticias-de-Taiw%C3%A1n/274939/Taiw%C3%A1n-y-el-Reino-Unido-firman-un-memorando-de-entendimiento-sobre-la-capacitaci%C3%B3n-de-personal-en-semiconductores				

El Memorando de Entendimiento entre Taiwán y el Reino Unido sobre el Proyecto Conjunto de Habilidades en Semiconductores se firmó el 11 de septiembre por videoconferencia, lo que refleja el compromiso de ampliar el personal y otros intercambios en este sector clave.

El Ministerio de Relaciones Exteriores (MOFA, siglas en inglés) informó que el pacto fue firmado en Londres por el embajador Vincent Chin-hsiang Yao, de la Oficina de Representación de Taipéi en el Reino Unido; y su homóloga británica Ruth Bradley-Jones en Taipéi. El viceministro de Relaciones Exteriores, François Chih-chung Wu; y el asesor técnico nacional del Reino Unido, Dave Smith, estuvieron presentes en Taipéi para presenciar la firma.

Wu destacó la complementariedad de los sectores de semiconductores de ambas naciones y elogió el Memorando de Entendimiento como un hito. El viceministro señaló que el Departamento de Ciencia, Innovación y Tecnología del Reino Unido envió nuevamente una delegación a SEMICON Taiwán 2025, lo que refleja la estrecha interacción bilateral.

Yao afirmó que el memorando se sumó a los acuerdos de tres pilares firmados en junio en el marco de la Asociación Comercial Reforzada entre Taiwán y el Reino Unido. En virtud de dicho pacto, ambas partes acuerdan ampliar los intercambios estudiantiles para adquirir experiencia de primera mano en las industrias de semiconductores y los ecosistemas de investigación, indicó el viceministro, añadiendo que espera una mayor cooperación bilateral en sectores como la inteligencia artificial, la computación cuántica, los drones y las comunicaciones satelitales de próxima generación.

Bradley-Jones afirmó que este memorando es el primero de este tipo entre Taiwán y un país socio europeo. Asimismo, la representante británica explicó que el pacto beneficiará a los estudiantes y a las industrias de ambas partes, y allanará el camino para una mayor cooperación bilateral.

Smith celebró el pacto para fortalecer la cooperación en la capacitación de personal, especialmente en medio de la escasez mundial en el sector de alta tecnología. El funcionario británico expresó su interés en ampliar la cooperación en sectores avanzados como los semiconductores compuestos, la fotónica de silicio y la tecnología cuántica.

El MOFA afirmó que el memorando de entendimiento subraya la política de diplomacia integrada del Gobierno y añadió que contribuirá a construir una cadena de suministro de alta tecnología resiliente y basada en valores, en consonancia con la visión del presidente Lai Ching-te de promover alianzas globales en la cadena de suministro de semiconductores democrática.

Notas de Electrónica					
Título:	México en el radar logístico global				
Encabezado:					
Fecha:	15/09/25	Fuente:	THE LOGISTICS WORLD	Por:	Mildred Ramo
Link:	https://thelogisticsworld.com/comercio-internacional/mexico-en-el-radar-logistico-global/				

Cuando la Secretaría de Economía anunció que México había captado 21,373 millones de dólares (mdd) en inversión extranjera directa (IED) durante el primer trimestre de 2025, marcando un récord histórico, no solo se trató de una cifra impresionante: fue una señal clara de que algo profundo está ocurriendo en las decisiones estratégicas de las empresas globales, de una reconfiguración acelerada de las cadenas de suministro, donde México se posiciona como protagonista clave

Este fenómeno no es casual. Según el informe Global Business Optimism Insights, de Dun & Bradstreet —firma de información financiera y de riesgo sobre empresas— basado en una encuesta a más de 10,000 ejecutivos en 32 economías, la confianza empresarial global está en caída libre. Las tensiones geopolíticas, la volatilidad comercial y las vulnerabilidades logísticas han llevado a las empresas a repensar sus prioridades de inversión y a buscar resiliencia en sus operaciones

Y ahí es donde México entra en juego.

Estrategias de supervivencia

Nearshoring, friendshoring y multisourcing: más que tendencias o palabras de moda, son pilares de la estrategia empresarial. México, por su cercanía con Estados Unidos, su red de tratados comerciales y su creciente infraestructura logística, se ha convertido en un destino natural para la relocalización industrial. De hecho, el 43.2% de la IED registrada en el primer trimestre se concentró en el sector manufacturero, destacando industrias como la automotriz, química, electrónica y alimentaria.

No obstante, el entusiasmo inicial por el nearshoring enfrenta ahora un entorno más complejo: amenazas arancelarias, revisión del T-MEC y presiones regulatorias desde Estados Unidos están obligando a las empresas a ajustar sus expectativas y a blindar sus operaciones ante posibles cambios abruptos.

La logística mexicana: entre la oportunidad y el desafío

El impacto del nearshoring en la logística mexicana es profundo. Estados como Nuevo León, Jalisco, Guanajuato y Querétaro han visto un auge en la demanda de parques industriales y centros de distribución. La necesidad de servicios 3PL y 4PL se ha disparado, y el transporte terrestre y transfronterizo ha cobrado un protagonismo inédito. Sin embargo, también persisten retos: saturación en aduanas, brechas en infraestructura y desigualdad logística entre regiones.

Un análisis de la estadounidense The Nearshore Company, señala que para que México mantenga su ventaja competitiva, es clave fortalecer las cadenas de suministro locales, invertir en capacitación del talento y avanzar en automatización, sin perder el componente humano.

Además, la sostenibilidad se vuelve un imperativo: las empresas buscan socios que cumplan con estándares ESG, y México tiene la oportunidad de posicionarse como un hub logístico responsable y trazable.

Según el Pulsómetro Logístico 2025, presentado por ConaLog y otras asociaciones líderes del sector, la logística mexicana está en un punto de inflexión. Las empresas que apuesten por la modernización, la sostenibilidad y la toma de decisiones basadas en datos estarán mejor preparadas para enfrentar los desafíos del entorno competitivo actual.

No obstante, el estudio revela que 74% de las empresas logísticas aún no han integrado sus sistemas digitales de forma efectiva, lo que limita el aprovechamiento de tecnologías como inteligencia artificial, gemelos digitales y sistemas de gestión de almacenes inteligentes. Esta brecha tecnológica es especialmente crítica en un contexto donde el comercio electrónico y el nearshoring están elevando las expectativas de velocidad, trazabilidad y eficiencia.

La infraestructura, una debilidad

A pesar de su ubicación estratégica y su red de tratados comerciales, México enfrenta retos estructurales que podrían frenar su potencial logístico. El país ocupa el lugar 66 en el Índice de Desempeño Logístico del Banco Mundial, por debajo de Brasil, Chile y Perú. Los costos logísticos representan el 13.7% del PIB, muy por encima del promedio de la OCDE (8%), lo que refleja una infraestructura que requiere inversión urgente.

Carreteras congestionadas, puertos saturados y una red ferroviaria subutilizada son algunos de los cuellos de botella que afectan la competitividad. La modernización de corredores clave, como el que conecta el Golfo con el Pacífico, y la ampliación de terminales portuarias como Veracruz y Manzanillo, son acciones prioritarias para responder al aumento en la demanda de transporte derivado del nearshoring.

Lo que deben considerar las empresas B2B

Para las empresas mexicanas de logística y supply chain, este momento representa una oportunidad única. Pero también exige visión estratégica. La relocalización industrial no es una promesa garantizada, sino una ventana que solo quienes se adapten con agilidad podrán convertir en ventaja competitiva. Invertir en tecnología, formar talento especializado, diversificar proveedores y anticiparse a los cambios regulatorios son acciones clave para consolidarse como aliados estratégicos en esta nueva era del comercio global.

México tiene todo para convertirse en un hub logístico global: ubicación privilegiada, tratados comerciales, talento y demanda creciente. Pero el éxito dependerá de cómo se aborden los retos estructurales, tecnológicos y operativos que aún persisten. Está en el centro del mapa logístico mundial. Y las decisiones que se tomen hoy, desde el almacén hasta la sala de juntas, definirán el papel del país en las cadenas de suministro del futuro.

Notas de Telecomunicaciones					
Título:	Paso a paso: cómo operará el piloto del Registro de Usuarios de Telefonía Móvil				
Encabezado:	En el caso de las líneas activas, tendrán un periodo para su registro a través de las compañías con quienes adquirieron los dispositivos.				
Fecha:	14/09/25 (por la tarde)	Fuente:	EL ECONOMISTA	Por:	Redacción
Link:	https://www.eleconomista.com.mx/empresas/paso-paso-operara-piloto-registro-usuarios-telefonia-movil-20250914-777134.html				

El Gobierno de México inició a partir del 1 de septiembre una prueba piloto para el registro de usuarios de telefonía móvil, a fin de combatir la extorsión, fraudes y otros delitos cometidos mediante el uso de líneas telefónicas.

Este registro está a cargo de la Agencia de Transformación Digital y Telecomunicaciones (ATDT), y las operadoras Telcel, Movistar, AT&T, Bait y Altán, acuerdo que se firmó entre el titular de la Unidad de Coordinación Nacional de Infraestructura Digital de la ATDT, Jorge Luis Pérez Hernández, y los representantes de dichas empresas telefónicas.

Reunidos en las instalaciones de la Secretaría de Seguridad y Protección Ciudadana (SSPC), se contó con la presencia del subsecretario de Política Criminal, Vinculación y Protección Civil, José Luis Rodríguez, y el director general de Consulta y Estudios Constitucionales de la Consejería Jurídica del Ejecutivo Federal, José Antonio Montero.

Este ejercicio concluye en octubre, con la entrada en vigor de las nuevas disposiciones en materia de telecomunicaciones, las cuales harán obligatorio el registro de las nuevas líneas telefónicas en todos los puntos de venta.

Por ello, te explicamos cómo operará el Registro de Usuarios de Telefonía Móvil:

Acude a un centro de atención:

- Dirígete a un punto de venta o centro de atención de tu operadora telefónica.

Presenta tu identificación oficial:

- Muestra una identificación oficial que contenga tu Clave Única de Registro de Población (CURP).

Acredita tu identidad:

- El personal del centro de atención verificará tus datos de la CURP para vincularla a la nueva línea telefónica que vas a contratar.

¿Qué sucederá con las líneas activas?
En el caso de las líneas activas, tendrán un periodo para su registro, para lo cual las compañías habilitarán la modalidad remota para facilitar este proceso a las personas usuarias.

Notas de Telecomunicaciones					
Título:	Querétaro alcanza 85% de retiro de cableado en desuso				
Encabezado:	El Municipio de Querétaro tiene como meta llegar a 20 toneladas antes de 2025				
Fecha:	15/09/25	Fuente:	OEM	Por:	David Álvarez
Link:	https://oem.com.mx/diariodequeretaro/local/queretaro-alcanza-85-de-la-meta-en-retiro-de-cableado-en-desuso-25756466				

El Municipio de Querétaro informó que ha retirado 17.1 toneladas de cableado en desuso de la vía pública, lo que representa el 85% de la meta establecida de 20 toneladas para 2025.

La acción se realiza en colaboración con 14 empresas de telecomunicaciones y forma parte del Plan Orden impulsado por el presidente municipal, Felipe Fernando Macías.

Hasta ahora, se han llevado a cabo 18 operativos en 11 vialidades principales, incluyendo Av. Tecnológico, Av. Zaragoza, Av. Constituyentes, Calzada de Los Arcos y Blvd. Bernardo Quintana.

Las labores buscan reducir riesgos para peatones y vehículos, facilitar la movilidad y organizar la infraestructura urbana.

En los operativos participan la Secretaría de Movilidad, la Secretaría de Gobierno a través de la Coordinación Municipal de Protección Civil y la Secretaría de Servicios Públicos Municipales.

Esto en conjunto con empresas como Telmex, AT&T, Izzi, Total Play, Mega, Flo Networks, UC Telecom, Inpro Telecom, Quattrocom, Blztelco, TV Rey, Axtel, IENTC y Even Telecom.

El retiro de cableado incluye líneas abandonadas en postes, fachadas y espacios públicos, mientras se asegura que las conexiones activas de telecomunicaciones no se vean afectadas.

La meta final es completar las 20 toneladas antes de que concluya el 2025, como parte de un plan de mantenimiento urbano que contempla limpieza de espacios públicos, ordenamiento de infraestructura y mejora de la movilidad.

Notas de Telecomunicaciones					
Título:	Factible el bloqueo temporal de plataformas				
Encabezado:					
Fecha:	15/09/25	Fuente:	CRÓNICA	Por:	Julio Brito A.
Link:	https://www.cronica.com.mx/opinion/2025/09/15/factible-el-bloqueo-temporal-de-plataformas/				

El nuevo artículo 30-B del Código Fiscal de la Federación, incluido en el Paquete Económico 2026, marca un parteaguas en la relación entre plataformas digitales y el fisco mexicano. La reforma obliga a empresas de streaming, intermediación en línea y economía colaborativa a otorgar al SAT acceso en línea y en tiempo real a sus sistemas y registros de operaciones en el país.

El objetivo declarado es reforzar la capacidad de monitoreo, cerrar espacios de evasión y asegurar que compañías extranjeras sin presencia física en México cumplan con el pago y retención de impuestos. Sin embargo, la sanción en caso de incumplimiento es severa: el bloqueo temporal de los servicios digitales, ejecutado por concesionarios de telecomunicaciones.

El alcance de esta medida despierta preocupaciones de gran calado. Asociaciones civiles advierten que podría afectar a millones de usuarios, limitando el acceso a Internet y a servicios esenciales como educación, teletrabajo, movilidad y comercio electrónico. En la práctica, un mecanismo diseñado para garantizar ingresos tributarios podría convertirse en un instrumento de control desproporcionado que amenaza la conectividad universal, reconocida como un derecho habilitador de la libertad de expresión y el desarrollo económico.

Para las plataformas, el reto no es menor: deberán adaptar sus sistemas tecnológicos, invertir en seguridad de datos y absorber mayores costos de cumplimiento. Así, el debate trasciende lo fiscal y coloca en el centro la tensión entre recaudación y derechos digitales.

RECURSOS.- De acuerdo con Samuel Bautista, investigador de The Competitive Intelligence Unit (The CIU), el Paquete Económico 2026, que presentó la Secretaría de Hacienda en el sector tecnológico los contrastes son evidentes. La Agencia de Transformación Digital y de Telecomunicaciones (ATDT), que lleva José Merino, registra un incremento de 22.1% en su presupuesto, alcanzando 3.85 mil millones de pesos, mientras que organismos como la CRT y la CNA, creados en la reforma de telecomunicaciones, aún no reciben recursos por falta de nombramientos. Asimismo, Financiera

para el Bienestar (Finabien) tendrá un aumento de 36.8%, reforzando su papel en servicios financieros con impacto social, y el Servicio Postal Mexicano (SEPOMEX) crecerá 24.9%, apuntando a fortalecer la logística nacional en un entorno de alta competencia con gigantes globales.

En contraste, los medios públicos sufrirán un recorte global de 4%, con pérdidas importantes para Canal 11, Canal 22 e IMER, mientras que el SPR y Radio Educación recibirán aumentos marginales. Además, destaca la caída de 82.3% en el presupuesto de la Dirección aprende.mx, reflejo de un menor énfasis en educación digital.

Notas de Telecomunicaciones					
Título:	El reloj institucional del IFT llegó a cero el Día de la Independencia				
Encabezado:	La desaparición del IFT no puede entenderse como un acto súbito, sino como la culminación de un proceso de desgaste político e institucional.				
Fecha:	15/09/25	Fuente:	EL FINANCIERO	Por:	Rolando Guevara Martínez
Link:	https://www.elfinanciero.com.mx/opinion/colaborador-invitado/2025/09/15/el-reloj-institucional-del-ift-llego-a-cero-el-dia-de-la-independencia/				

Este 15 de septiembre de 2025 se convierte en la fecha que marca, de facto, el fin del ciclo del Instituto Federal de Telecomunicaciones (IFT). Diversos medios adelantaron la noticia de su "extinción" formal este día, y lo cierto es que desde esta fecha el órgano autónomo queda casi inoperante tras concluir el periodo del Comisionado Presidente en suplencia por vacancia, Javier Juárez Mojica.

Este desenlace no es una sorpresa. La ruta institucional estaba trazada desde hace nueve años en la sesión pública ordinaria del Senado de la República del 18 de octubre de 2016, en la que se discutió y ratificó el nombramiento de Juárez Mojica como comisionado del IFT. En ese debate, el entonces presidente de la Comisión de Comunicaciones y Transportes del Senado, Javier Lozano Alarcón, dejó constancia expresa antes de la votación:

"El oficio con el que remite el Presidente de la República este nombramiento es con fecha 15 de septiembre. Entonces, para evitar cualquier interpretación de carácter jurídico que pudiera ser contraria a la decisión de este Senado, pues entonces que los 9 años corran a partir de esta fecha" (Diario de los Debates, 18 de octubre de 2016, p. 148).

La precisión no era menor, ya que el Senado blindaba la interpretación sobre la vigencia del mandato, tal y como quedó señalado también en el boletín de prensa número 355 del 18 de octubre de 2016.

Por eso, el ciclo de Juárez Mojica como comisionado —y con ello la legitimidad de origen y de operación del IFT— concluye sin margen de prórroga este 15 de septiembre de 2025. Cabe precisar que la extinción plena del IFT se establece con diversas condiciones marcadas en los artículos transitorios de la nueva Ley en Materia de Telecomunicaciones y Radiodifusión publicada el 16 de julio de 2015, y para ello es importante la integración del nuevo Pleno de la Comisión Reguladora de Telecomunicaciones (CRT).

Asimismo, pese a que el aún vigente Estatuto Orgánico del IFT establece que para las sesiones del Pleno se requiere la presencia de cuando menos tres Comisionados para sesionar válidamente, esta posibilidad se ve de facto cuestionada por la legitimación de operación.

Conviene subrayar la enseñanza institucional de 2016. El Senado fijó con precisión la fecha de inicio del mandato antes de votar la ratificación de Juárez Mojica. La discusión y votación fue aclarada con quórum presente: 76 votos a favor, siete en contra y cero abstenciones. Ese acto jurídico eliminó cualquier ambigüedad sobre los plazos proveniente desde el propio Senado.

Cabe mencionar que la Ley Federal de Telecomunicaciones y Radiodifusión establecía suplencias temporales en caso de vacancias. Pero esas reglas fueron pensadas para asegurar continuidad, no para prolongar indefinidamente la ausencia de nombramientos.

La situación es crítica si se considera que, conforme al calendario institucional publicado en el Diario Oficial de la Federación, el Pleno debía sesionar el próximo 24 de septiembre. En términos prácticos, esa sesión corre riesgo para celebrarse, porque el Instituto carece de integrantes para tomar ciertas decisiones válidas.

La desaparición del IFT no puede entenderse como un acto súbito, sino como la culminación de un proceso de desgaste político e institucional. La construcción de la CRT debe ya, en cambio, representar un relanzamiento de la política regulatoria en telecomunicaciones, de acuerdo al mandato constitucional de la Reforma de Simplificación Orgánica del pasado 20 de diciembre de 2024, misma que, por cierto, no puede ser interpretada para perpetuar los nombramientos de los Comisionados, desde un punto de vista jurídico, por lo anteriormente expuesto.

México no puede permitirse un “vacío regulatorio” en un sector que constituye la columna vertebral de la economía digital. El reloj institucional ya marcó el fin de ciclo; ahora toca a la Presidencia de la República y el Senado encender el cronómetro de una nueva etapa.

Notas de Telecomunicaciones					
Título:	¿Cómo usar la nueva plataforma de datos abiertos del gobierno de México?				
Encabezado:	La nueva Plataforma Nacional de Datos Abiertos (PNDA) consolida datos públicos en formatos estructurados, con respaldo central y visualización inmediata, lo que resuelve problemas históricos de enlaces rotos y archivos incompatibles.				
Fecha:	14/09/25 (por la tarde)	Fuente:	EL ECONOMISTA	Por:	Rodrigo Riquelme
Link:	https://www.eleconomista.com.mx/tecnologia/nueva-plataforma-datos-abiertos-gobierno-mexico-20250914-777141.html				

La Agencia de Transformación Digital y Telecomunicaciones (ATDT) presentó la nueva Plataforma Nacional de Datos Abiertos (PNDA), un proyecto que busca resolver un problema de años: la fragmentación, los enlaces rotos y los formatos incompatibles que convirtieron a los datos públicos en un terreno difícil de explorar.

La iniciativa se plantea como un ecosistema que no sólo concentra bases, sino que asegura calidad, respaldo y visualización inmediata.

“El objetivo es transformar datos en información, que la ciudadanía pueda consultar y utilizar sin necesidad de conocimientos técnicos avanzados. La plataforma genera gráficas, genera tablas, y todo esto está pensado en un ecosistema mucho más amplio que un simple repositorio”, dijo Irving Morales Agiss, director de Datos Abiertos de la Agencia de Transformación Digital y Telecomunicaciones.

El punto de partida fue un diagnóstico. La plataforma anterior acumulaba más de 50,000 recursos de datos, de los cuales cerca de 20,000 estaban en enlaces rotos. Muchos eran documentos en PDF con tablas incrustadas o archivos Excel con múltiples hojas, imposibles de procesar.

Por esta razón en la nueva plataforma se estableció un criterio estricto: sólo se aceptan archivos CSV para datos tabulares y Shapefiles para datos espaciales. Todo lo demás (Excel, PDFs, Word) es rechazado o debe transformarse previamente.

“El sistema no admite formatos que no sean estructurados. Si una institución quiere subir un Excel con varias pestañas o un PDF con notas dentro de las celdas, el validador lo rechaza. Lo que necesitamos son datos procesables por máquina, que sean realmente interoperables”, dijo Morales en conferencia.

¿Cómo usar la plataforma?

Para el ciudadano común, la Plataforma Nacional de Datos Abiertos comienza con una búsqueda simple. El portal incluye un buscador central en el que se pueden introducir palabras clave como incidencia delictiva, agua potable o mujeres.

El motor devuelve resultados en dos categorías:

- Conjuntos de datos (colecciones temáticas).
- Recursos (las tablas concretas).

Al seleccionar un recurso, el sistema despliega de inmediato gráficos interactivos y tablas dinámicas, que responden a filtros por entidad federativa, rango de fechas o variables específicas.

“No tiene sentido obligar a la ciudadanía a bajar una base enorme solo para obtener una gráfica. Desde la plataforma pueden filtrar y tener visualizaciones inmediatas. Y si quieren profundizar, entonces descargan lo que necesitan”, dijo el director de Datos Abiertos.

Cómo descargar información

La descarga está diseñada en dos niveles:

1. El recurso completo, en formatos CSV, Excel o JSON.
2. El subconjunto filtrado, es decir, solo la porción resultante tras aplicar criterios de búsqueda.

Cada recurso incluye un botón de descarga y un diccionario de variables para interpretar los datos. De esta manera, un periodista que cubre seguridad en Guanajuato puede obtener únicamente los registros de ese estado en lugar de procesar millones de filas nacionales.

APIs y suscripciones

La PNDA también está pensada para desarrolladores y académicos. El portal permite el acceso mediante APIs, lo que facilita integrar información directamente en aplicaciones o sistemas de análisis sin descargas manuales.

Además, la agencia anunció un futuro sistema de suscripciones, con el que los usuarios podrán recibir notificaciones cuando se actualicen los conjuntos que siguen de cerca.

“Estamos trabajando para que cualquier usuario pueda suscribirse a un recurso y ser notificado cuando cambie. La idea es que no tengan que estar entrando cada semana a ver si ya se actualizó”, dijo.

Datos antiguos

Uno de los principales problemas de la plataforma anterior era que los enlaces caducaban cuando las instituciones modificaban sus páginas. La PNDA busca solucionarlo con un repositorio central que respalda cada recurso en los servidores de la Agencia de Transformación Digital.

De esta manera, incluso si una secretaría mueve o borra su archivo original, el recurso en la PNDA seguirá disponible.

“En la plataforma anterior teníamos miles de recursos que ya no existían. Ahora la lógica es distinta. Aunque una institución cambie su web, los datos quedan respaldados en nuestra infraestructura”, dijo Morales Agiss.

El equipo también trabaja en la migración de datos históricos, con la meta de rescatar información desde 2015. No obstante, reconocen que no todo podrá recuperarse. Los archivos antiguos en PDF o Excel desestructurados no cumplen con los nuevos criterios de calidad.

¿Quién publica y cada cuánto?

En esta primera etapa, la PNDA ya reúne información de alrededor de 89 instituciones. El objetivo es llegar a unas 300 unidades de la Administración Pública Federal para mediados del 2026.

Cada dependencia debe designar un área de datos abiertos con suficiente jerarquía para solicitar información a otras direcciones internas. El cambio busca evitar que la publicación dependa de voluntades aisladas.

La frecuencia de actualización varía según el origen de los datos: hay conjuntos mensuales, semestrales y anuales. La plataforma envía recordatorios a las instituciones responsables y aplica validaciones automáticas antes de liberar un recurso.

Retos pendientes

Aunque la PNDA representa un salto tecnológico, no elimina del todo los desafíos. La calidad de la información seguirá dependiendo de cada institución, y los retrasos en la actualización pueden persistir.

Por ello, los especialistas recomiendan revisar siempre tres elementos: la fecha de última actualización, la definición metodológica de las variables y, en casos críticos, la confirmación directa con la dependencia que genera la base.

“Lo que publicamos no son solo datos, es información. Y eso implica una responsabilidad doble: de las instituciones que generan la base y de los usuarios que la interpretan”, dijo Morales Agiss.

La nueva Plataforma Nacional de Datos Abiertos es el esfuerzo más ambicioso del gobierno mexicano para ordenar la oferta de datos abiertos. El reto será sostener la calidad y garantizar la actualización constante. Si lo logra, la plataforma puede convertirse en una infraestructura permanente que acerque la información pública a la ciudadanía de forma confiable y accesible.

Notas de Telecomunicaciones					
Título:	Presenta ATDT nueva Plataforma de Bases de Datos Abiertos				
Encabezado:					
Fecha:	15/09/25	Fuente:	CONSUMOTIC	Por:	Juan Carlos Villarruel
Link:	https://consumotic.mx/sociedad-digital/presenta-atdt-nueva-plataforma-de-bases-de-datos-abiertos/				

Un total de 89 de casi 300 dependencias federales, ya han aportado su información a la nueva Plataforma de Bases de Datos Abiertos diseñada por la Agencia de Transformación Digital y Telecomunicaciones (ATDT) que promete conformar un gran sistema a través del cual la ciudadanía esté lo mejor informada posible sobre las acciones de las autoridades.

“Por ahora, hay disponibles mil 930 bases de datos correspondientes a 89 instituciones, divididas en 26 categorías, organizadas bajo el criterio de que sean fáciles de consultar, interoperables y reflejando los resultados del trabajo de las dependencias, más allá del mero criterio de transparencia en el uso de los recursos públicos”, indicó Irving Morales Agiss, director de Datos Abiertos de la ATDT.

Al ofrecer el “Taller para medios sobre el uso de la Plataforma Nacional de Datos Abiertos”, el funcionario explicó que la Plataforma de Base de Datos Abiertos que ya está disponible en la dirección digital https://www.datos.gob.mx/ busca convertirse en una herramienta de conocimiento que puedan utilizar todos los sectores, desde la población abierta hasta científicos de datos, con un criterio de “fomentar la innovación pública y la transparencia de entidades e instituciones”.

El rediseño de la plataforma de Datos Abiertos que existía hasta ahora, “ha tomado como base la idea de que todas las dependencias siguen los mismos criterios y utilizan un formato único para subir su información porque hasta ahora, en las páginas web de las distintas dependencias, los datos aparecen en formatos muy distintos”.

Por ejemplo, algunos presentaban archivos de PDF, otras tenían ligas que remitían a distintas páginas web o micrositios; unas más compartían una liga de Drive e incluso muchas no estaban actualizadas, de manera que el enlace no lleva a ningún lado o, peor aún, la información sólo se refería a un período, porque los administradores montaban los datos del año más reciente sobre la liga que contenía la información del año anterior y ésta se perdía para siempre.

Ahora, con el trabajo que se ha venido realizando desde hace poco más de un año y que incluyó un diagnóstico detallado de cómo estaba la realidad, se está estandarizando la información y cómo debe publicarse, de acuerdo con los "Lineamientos en materia de Datos Abiertos de la Administración Pública Federal", publicados en el Diario Oficial de la Federación el jueves 11 de septiembre.

De acuerdo con ese documento, los datos que se publican deben ser: accesibles, integrales, gratuitos, no discriminatorios, oportunos, permanentes (hasta por 10 años), legibles por máquinas, en formatos abiertos y de uso libre.

Hasta ahora, con el rediseño de la plataforma de Datos, ya se pueden consultar bases de datos divididas en 26 categorías que abarcan temas como seguridad (desagregada a nivel municipal), programas sociales, medio ambiente, salud, educación, mujeres, cultura, deportes, ciencia y tecnología, derechos humanos, economía, gobierno y migración, por citar algunos.

De acuerdo con Morales Agiss, la intención es que las bases de datos puedan ser consultadas por cualquier persona y que sean fácilmente comprensibles, incluyendo explicaciones claras sobre el contenido, glosarios de siglas, sin notas al cálculo y con la posibilidad de filtrar información de acuerdo al interés del usuario, quien no estará obligado a descargar archivos en su computadora.

Tampoco se registrará como usuarios, ni contar con contraseñas, porque la idea es tener la información a la mano para propósitos de investigación periodística, científica, académica o de cualquier ciudadano que quiera saber lo que hace el gobierno federal.

Cuestionado sobre los procesos para solicitar información, tal como ocurriría en la Plataforma Nacional de Transparencia, explicó que esta nueva Plataforma de Datos Abiertos no opera de esa manera y que aquella función la seguirá realizando la Secretaría Anticorrupción y Buen Gobierno, mientras la ATDT operará la plataforma y guardará copias de todos los archivos en centros de datos propios, aunque cada dependencia será dueña de su propia información.

Por ejemplo, en el sector de telecomunicaciones, si bien la nueva Ley en la materia señala que las bases de datos del IFT deberán de pasar a la Comisión Reguladora de Telecomunicaciones (CRT), esto todavía no es un hecho y habrá que esperar a ver cómo se opera una vez que esta nueva entidad existe y entre en funciones de manera normal.

Se espera que poco a poco las dependencias que aún no se suman, designen a las áreas encargadas, para incorporarse a la plataforma que, por ahora, cuenta con mil 020 de las mil 930 bases de datos configuradas en el visualizador de datos desarrollado con el Sistema Ajolote, una herramienta que permite explorar la información de forma accesible e interactiva.

De hecho, el usuario podrá filtrar información para generar sus propios gráficos de barras, líneas, mapas, treemaps y tablas que podrá después imprimir, descargar o incrustar en su sitio web

directamente desde la página de la plataforma.

Notas de TI					
Título:	Ciberseguridad: ¿cuántas empresas en México cuentan con la ISO 27001?				
Encabezado:					
Fecha:	15/09/25	Fuente:	CONSUMOTIC	Por:	Redacción
Link:	https://consumotic.mx/tecnologia/solo-589-empresas-mexicanas-cuentan-con-certificacion-iso-27001/#google_vignette				

A pesar de que México tiene más de 5 millones 450 empresas y que el país se ha convertido en uno de los más atractivos para la ciberdelincuencia, sólo 589 compañías habían recibido la certificación ISO 27001 en materia de ciberseguridad, de acuerdo con la Encuesta más reciente de ISO.

Al respecto, Santiago Fuentes, fundador y director general de Delta Protect, empresa mexicana en ciberseguridad, señaló la importancia de que las compañías establezcan sistemas de seguridad digital, debido a que México es una de las naciones más vulnerables en el mundo.

Recordó que la norma ISO 27001, establecida desde el año 2005 por la Organización Internacional de Estandarización, plantea los parámetros internacionalmente aceptados, para considerar que una organización de cualquier tamaño tiene un sistema de gestión de seguridad de la información eficiente.

En ese sentido, advirtió que a 20 años de su implementación la adopción de este estándar por parte de empresas mexicanas es bajo, pues las empresas que no lo tienen “arriesgan información confidencial tanto propia como de sus clientes, así como su infraestructura operativa, de finanzas y enfrentan consecuencias como multas, compensaciones a clientes, pérdida de y daño reputacional”.

En ese sentido, la Encuesta ISO sobre certificaciones de normas de sistemas de gestión a nivel mundial, publicada en 2024 por el Instituto de Seguridad y Bienestar Laboral de la Unión Europea, señala que México ocupa el lugar número 21 en la lista de los países con mayor número de estas certificaciones y el segundo lugar en el continente americano, sólo después de Estados Unidos.

El documento indica que a nivel mundial, hay alrededor de 50 mil certificados de este tipo; los países más aventajados son Japón con 5 mil 599; China con 4 millones 108 e India con 3 millones 877 certificados cada uno.

A su vez, Antonio Arellano, cofundador de Delta Protect, explicó que esta norma tiene por objeto ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información mediante la implementación de controles de seguridad adecuados en cuatro categorías: controles organizacionales, de personas, físicos y tecnológicos.

A través de ellos se supervisan políticas de seguridad de la información; funciones y responsabilidades en la materia; clasificación de los datos, gestión en la cadena de suministro de tecnología; identificación, planificación y preparación para incidentes.

También se establecen términos y condiciones de empleo, educación y capacitación en materia de seguridad de la información y responsabilidades al término de la contratación laboral, entre otras cosas.

Todas estas y otras acciones que se deben cumplir para tener esta certificación (la cual se revisa y, en su caso, se renueva cada año), tienen por objeto cubrir todas las áreas que pueden ser susceptibles de recibir un ataque y por eso es importante que las empresas busquen esta certificación.

Sin embargo, los índices de incidentes de ciberseguridad más importantes del mundo colocando a México en los primeros lugares de ataques en esta materia y aún así, sólo un pequeño grupo de empresas cuenta con la certificación ISO 27001.

De ahí que los directivos llamaron a la industria en general a realizar las acciones necesarias para obtener este estándar, sobre todo en un mundo de crecientes amenazas cibernéticas, con delincuentes que usan la Inteligencia Artificial para perpetrar sus ataques.

Notas de TI					
Título:	Servicios de “Back Office” crecen a doble dígito anual				
Encabezado:					
Fecha:	15/09/25	Fuente:	CONSUMOTIC	Por:	Juan Carlos Villarruel
Link:	https://consumotic.mx/tecnologia/servicios-de-back-office-crecen-a-doble-digito-anual/				

La tendencia de terciarización de servicios digitales, tales como atención a clientes, soporte técnico y en general, es decir, lo denominado “Back Office”, está creciendo a doble dígito en México desde hace cuatro años y promete seguir en aumento, particularmente debido a la reducción de costos, incremento de la productividad y, sobre todo, el ahorro de tiempo de implementación de proyectos.

Luis Soto, gerente de Desarrollo de Negocios de Kelly México, empresa especializada en servicios digitales externos, detalló que estos crecimientos exponenciales se explican porque las empresas que contratan este tipo de servicios obtienen resultados positivos en sólo cuatro o seis semanas, mientras que hacerlo internamente les llevaría seis meses.

“Cada vez más, las empresas de todos tipos y tamaños están viendo la conveniencia de dejar en manos de los expertos, servicios como mantenimiento del software, ciberseguridad, atención al cliente y muchos otros, para dedicarse a su negocio principal, lo que ha probado ser un gran negocio para todos”, aseguró eL ejecutivo.

Eso explica por qué las empresas que ofrecen servicios digitales externos y que se encuentran afiliadas a la Asociación Mexicana en Dirección de Recursos Humanos (Amedirh), organización que agrupa a más de 900 compañías, registran también crecimientos en sus actividades a doble dígito desde hace por lo menos tres años.

“Cada vez las empresas se abren más a estos esquemas y están tercerizando áreas de atención al cliente, soporte técnico y, en general el llamado back office, para dedicarse a lo que saben hacer,

sencillamente porque no se distraen de sus actividades centrales y cuentan con soporte para resolver los problemas que se lleguen a presentar".

La reducción de costos y ahorros de tiempo, son en general las razones que más argumentan las empresas para utilizar el llamado software como servicio (SaaS por sus siglas en inglés), los servicios de ciberseguridad o los sistemas de manejo de clientes que prestan empresas externas especializadas en esos temas.

Y es que, en efecto, para la gran mayoría de las empresas, especialmente las pequeñas y medianas, es más productivo pagar por servicios de alto nivel en esas y otras especialidades digitales, que hacerlo internamente, porque de generar equipos "en casa", los gastos se elevarían demasiado, sin contar con el tiempo de implementación, y la curva de aprendizaje e incluso sin hablar del déficit de talento que no es un tema menor.

A manera de ejemplo, señaló que al abrir sus puertas en México hace cuatro años, Kelly carecía de proyectos implementados y al día de hoy ya tiene alrededor de 120, lo cual habla del ritmo de crecimiento que están presentando los servicios digitales tercerizados.

El ejecutivo destacó que el caso de la firma que representa no es un caso aislado; porque la realidad es que la mayoría de las empresas que ofrecen estos servicios tienen ritmos de crecimiento similares, lo que habla que la industria perdió la desconfianza de dejarle a expertos de otras compañías la operación de algunas de sus actividades críticas.

El propio crecimiento de la demanda, ha permitido implementar planes de trabajo que facilitan la atención a empresas más pequeñas, pues no necesariamente se deben de comprometer tantos recursos para atender a compañías más pequeñas, sino que un equipo puede dar servicio a más de un cliente, sin comprometer la calidad.

Luis Soto anticipó que este esquema de trabajo seguirá creciendo en el futuro, en la medida en que las empresas comprueben que contratar servicios digitales de terceras compañías es un camino seguro a la eficiencia, mientras los expertos se dedican a los temas digitales.

Notas de TI					
Título:	Microsoft Teams para Empresas: Funcionamiento, Integraciones y Licencias				
Encabezado:	Qué es Microsoft Teams, cómo funciona y cuál es la mejor versión para ti				
Fecha:	15/09/25	Fuente:	PRONETIC GEEKNETIC	Por:	Raúl Unzué
Link:	https://pronetic.geeknetic.es/Guia/3315/Microsoft-Teams-para-Empresas-Funcionamiento-Integraciones-y-Licencias.html				

Microsoft Teams es la plataforma de colaboración de Microsoft que combina chat, videollamadas, reuniones, intercambio de archivos y apps de productividad en un mismo sitio. Nació en 2017 como respuesta directa a Slack y otras alternativas, con el tiempo, se convirtió en el "hub" central de trabajo para quienes usan Microsoft 365. En la práctica, Teams es mucho más que una app de videollamadas, es un servicio en la nube que conecta usuarios, dispositivos y servicios corporativos bajo un mismo tenant (tu organización en la nube de Microsoft).

Ahora bien, lo interesante no es solo lo que vemos, la ventana de chat, el botón de “Unirse a la reunión” o el compartir pantalla, sino todo lo que ocurre por debajo. Detrás de cada clic hay autenticación con tokens, señalización cifrada, protocolos de tiempo real que negocian audio y vídeo, y hasta configuraciones de red específicas para que las llamadas no se corten.

En esta entrada vamos a desmenuzar Teams desde dos ángulos:

1. La experiencia visible para el usuario (qué versión elegir, costes, integraciones, personalizaciones).
2. La “cocina técnica” (cómo funciona el flujo de conexión, qué protocolos usa, qué es un tenant y por qué es clave en seguridad y gestión).

El objetivo, que tanto si vienes de un perfil técnico sin mucha experiencia en networking como si eres de IT que necesita justificar una compra o diseñar una red, te lleves una visión completa de cómo funciona Teams para saber que decisiones tomar.

¿Qué es un Tenant en Teams?

Piensa en el tenant como si fuera la parcela privada de tu empresa dentro de la nube de Microsoft. Es un espacio reservado y aislado, como si tuvieras tu propia oficina virtual con llaves y paredes que separan tu organización de las demás.

Dentro de ese espacio viven:

- Tus usuarios (empleados con sus cuentas).
- Tus grupos y equipos de trabajo.
- Tus aplicaciones (Teams, Outlook, SharePoint, etc.).
- Tus dominios (ejemplo: @tuempresa.com).
- Las reglas de seguridad que definen cómo se entra y qué se puede hacer (contraseñas, multifactor, permisos).

Teams se monta encima de ese tenant y se ajusta a lo que tú hayas configurado allí. Dicho de otra forma: las decisiones de seguridad y organización que pongas en el tenant se reflejan directamente en Teams.

Ahora, ¿qué pasa si quieres colaborar con gente de fuera? Microsoft ofrece varias formas:

- Invitado (B2B): añades a la persona externa a tu tenant como si fuera un colaborador temporal. Así puede entrar a ciertos equipos o canales, pero con permisos limitados que tú controlas.
- Acceso externo (federación): no metes al invitado en tu oficina, simplemente abres una ventanita para hablar o reunirte con otra organización que también usa Teams.
- Cross-tenant (Entra): es como establecer un acuerdo formal de confianza entre dos organizaciones. Permite afinar mucho mejor qué información se comparte y qué no.

Y sobre dónde va a parar todo lo que haces en Teams:

- Los archivos se guardan en SharePoint o OneDrive.
- Los mensajes y calendarios se almacenan en Exchange Online.
- Todo va cifrado (tanto cuando viaja como cuando descansa en los servidores) y cumple con las normativas de seguridad y cumplimiento de Microsoft 365/Purview.

Flujo de conexión
Vamos a contar qué hace el cliente de Teams por debajo cuando lo abre y te unes a una reunión (los procesos de autenticación, señalización, medios, puertos, QoS…).

Descubrimiento y Autenticación
Cuando abres Teams (ya sea en el escritorio, móvil o web), primero busca a dónde conectarse dentro de tu suscripción de Microsoft 365. Luego, te identifica frente a Microsoft Entra ID (antes conocido como Azure AD). Es como presentarte en la recepción: “Soy yo, déjame pasar”.

Esto se hace usando estándares modernos llamados OAuth 2.0 y OpenID Connect. Lo importante es que son formas de comprobar que eres tú sin compartir tu contraseña directamente cada vez. En lugar de eso, te dan un “carnet digital” (token) que dice: “Este es XYZ y puede usar estos servicios”, y cuando caduca, se renueva sin preguntarte la clave otra vez. Ah, y si tu empresa exige cosas como doble verificación (MFA) o que el dispositivo esté identificado, eso se revisa justo en ese momento.

En resumen, OAuth/OIDC son estándares para que las apps confirmen tu identidad y reciban permisos sin guardar tu contraseña.

Señalización
Una vez estás “dentro”, Teams abre un canal seguro (usando HTTPS o WebSocket cifrado) con los servidores de Teams para enviar y recibir instrucciones, “únete a esta reunión”, “pausa tu micrófono”, “te levantaste del teclado”… Todo eso viaja por aquí, pero no es el audio ni el vídeo, solo órdenes. La capa de control va cifrada con TLS.

Medios en tiempo real (Voz, Vídeo y Pantalla)

Aquí viene lo interesante, cuando empiezas la videollamada, Teams busca la mejor forma de conectar contigo directamente. Usa algo llamado ICE, junto con STUN y TURN:

- STUN es como mirar al exterior, “¿cómo me ve Internet?” para saber tu IP pública.
- Si puede, te conecta directo (peer-to-peer).
- Si no se puede, pasa todo por un servidor intermedio en la nube (TURN).
- Intenta usar UDP porque va más rápido, pero si no funciona, utilizará TCP (como HTTPS).

Y todo (audio, vídeo, compartir pantalla) va cifrado con un sistema eficiente llamado SRTP, usando claves que ya se negociaron de forma segura al principio.

En resumen, ICE busca la mejor ruta extremo-a-extremo. STUN descubre tu IP pública/puertos tras el NAT. TURN retransmite medios desde la nube cuando no hay camino directo. SRTP cifra audio/vídeo.

Codecs y Optimizaciones

Teams usa distintos formatos para comprimir voz y vídeo:

- Audio: el codec principal es Satin, diseñado por Microsoft para dar buena calidad incluso si la red es mala. Puede funcionar con muy pocos kilobits de ancho de banda (6–36 kbps), ajustándose automáticamente si la conexión se pone lenta, lo que parece casi magia. También puede usar Opus, que es muy versátil y también se adapta bien.

- Vídeo / Compartir pantalla: usa H.264, pero para compartir pantalla han añadido AV1, que reduce el consumo de ancho de banda en un 60 % sin perder nitidez. Ideal para presentaciones visuales en conexiones lentas.

¿Qué pasa cuando me conecto a una reunión de Teams?

En resumen, cuando le das a “Unirme a la reunión”, sucede esto:

1. conectas y demuestras tu identidad.
2. Se abre un canal de control para mandar instrucciones.
3. Se negocia cómo enviar audio y vídeo de forma segura y directa.
4. Teams decide cómo comprimir sonido y vídeo según tu red.
5. Todo va por el camino más rápido posible, cifrado y confiable.

Versiones de Teams, diferencias y costes

Teams Free

La versión gratuita es perfecta si lo que quieres es algo básico: reuniones de hasta 60 minutos, máximo 100 personas, 5 GB por usuario y chat o llamadas 1:1 sin límite de tiempo. Lo justo para pymes pequeñas o uso personal. Eso sí, olvídate de administración avanzada y de usar Teams como centralita telefónica (PSTN).

Teams Essentials

Aquí ya hablamos de una opción de pago, pero sin necesidad de comprar todo Microsoft 365. Por unos 3,70–4 € al mes por usuario (depende del país e impuestos), tienes reuniones de hasta 30 horas, hasta 300 asistentes, 10 GB por usuario y soporte técnico de Microsoft. Es como la versión free, pero vitaminada y con menos limitaciones.

Microsoft 365 Business (Basic / Standard)

Si además de Teams quieres el paquete completo (correo corporativo, almacenamiento en OneDrive/SharePoint y las apps de Office), esta es tu opción. En la UE, el plan Basic ronda los 5,60 €, y el Standard unos 11,70 € por usuario/mes (precios aproximados, cambian según región e IVA). Aquí Teams viene integrado con todo el ecosistema de productividad.

Teams Premium (extra)

Es un complemento que añade funciones pensadas para empresas que necesitan más seguridad y control en sus reuniones: marcas de agua, cifrado extremo a extremo en reuniones de hasta 200 personas, plantillas protegidas, además de mejoras en webinars y town halls. También ofrece la función de “resumen inteligente”, que da un extra en transcripciones y notas automáticas.

Teams Phone (extra)

Si lo que quieres es que Teams sustituya a tu centralita telefónica, necesitas este complemento. Con Teams Phone puedes hacer y recibir llamadas a través de la red telefónica (PSTN) usando Calling Plans de Microsoft, un operador homologado (Operator Connect) o tu propia infraestructura con Direct Routing y un SBC (controlador de frontera de sesión).

Nota importante sobre licencias en Teams

Desde 2024 Microsoft ofrece versiones de Microsoft 365 con Teams y sin Teams (primero en la UE y ahora globalmente). Así que, si compras Microsoft 365 sin Teams, no pasa nada, puedes añadir después Teams o Essentials por separado según lo que necesites.

Requisitos de Microsoft Teams

Teams se puede usar prácticamente en cualquier sitio, pero la experiencia cambia un poco según el dispositivo:

- Escritorio (Windows y macOS): la aplicación actual es el llamado “new Teams”, más rápida y ligera que la versión anterior. En Linux ya no hay app nativa, pero puedes instalarlo como PWA (una app web que se comporta como programa de escritorio).
- Navegador web: funciona en Edge, Chrome, Safari y Firefox gracias a WebRTC, que es la tecnología estándar para llamadas y vídeo en tiempo real directamente en el navegador.
- Móvil: apps para iOS y Android con casi las mismas funciones que en escritorio, ideal para no perderte reuniones cuando estás fuera.
- VDI, salas y teléfonos certificados: existen versiones específicas para escritorios virtuales (VDI) y para hardware certificado como Teams Rooms (salas de videoconferencia) o teléfonos de escritorio con Teams integrado. Estos clientes están optimizados y permiten aplicar políticas de red y calidad de servicio (QoS) adaptadas a entornos corporativos.

Integraciones y personalizaciones

Aquí es donde Teams se convierte en algo más que “chat y videollamadas”:

- Apps dentro de Teams: puedes añadir pestañas con webs integradas, usar bots para automatizar tareas, extensiones de mensajes para interactuar en el chat, o conectores/webhooks para que otras aplicaciones envíen avisos directamente a un canal. Todo esto se controla con políticas de permisos para que solo se usen las apps que tu empresa autorice.
- Microsoft Graph y Power Platform: si quieres ir más allá, con Graph puedes acceder a datos de Teams (usuarios, reuniones, mensajes…) y con Power Automate o Power Apps puedes montar flujos automáticos o apps personalizadas que se integren en Teams.
- Seguridad y cumplimiento: aquí entran cosas como las etiquetas de sensibilidad (para clasificar equipos o sitios), políticas de retención y prevención de pérdida de datos (DLP), o la posibilidad de hacer búsquedas de eDiscovery en caso de auditoría. Con Teams Premium se añaden extras de seguridad como marcas de agua en reuniones, límites de grabación o cifrado avanzado.
- Red corporativa: para que las reuniones vayan fluidas, conviene configurar bien la red, marcar el tráfico de voz y vídeo con QoS (DSCP), abrir los puertos UDP 3478–3481, evitar que los proxies inspeccionen el tráfico cifrado de medios y, sobre todo, mantener siempre actualizada la lista oficial de URLs e IPs de Microsoft 365 en el firewall.

Teams: Algo más que Videollamadas

Cuando piensas en Microsoft Teams, lo primero que se te viene a la cabeza son las videollamadas. Pero en realidad, Teams es todo un ecosistema: detrás de ese botón de “Unirse” hay procesos de autenticación con Microsoft Entra ID, negociación segura de sesiones, medios en tiempo real cifrados con SRTP, mecanismos de conectividad como ICE, STUN y TURN, y codecs modernos que

optimizan la calidad de audio y vídeo aunque la red no sea perfecta. Todo esto se combina con un conjunto de políticas y apps que determinan qué puede hacer cada usuario, en qué condiciones y con qué nivel de seguridad.

En cuanto a las versiones, el abanico es amplio y depende de tus necesidades:

- Teams Free es ideal si buscas coste cero y funciones básicas de colaboración.
- Teams Essentials está pensado para pymes que no usan Microsoft 365, pero necesitan reuniones más largas, más participantes y soporte técnico.
- Microsoft 365 Business (Basic o Standard) es la opción lógica si tu empresa ya trabaja en el ecosistema de Microsoft, con correo, almacenamiento en la nube y las aplicaciones de Office.
- Teams Premium añade la capa extra de seguridad y control para organizaciones que hacen reuniones confidenciales o gestionan eventos grandes.
- Teams Phone convierte a Teams en tu centralita en la nube, con llamadas completas a la red telefónica.

La clave es que Teams no es un producto único, sino una plataforma adaptable, puedes configurarla según tu red (QoS, puertos, proxies), ajustar las políticas de acceso y decidir qué licencias encajan mejor con tu negocio. Así evitas sorpresas cuando pases de una prueba piloto a producción real.

En definitiva, Teams es mucho más que un “Zoom con esteroides”, es una herramienta que, bien configurada y entendida, puede convertirse en el centro de la comunicación y colaboración de tu empresa.

Notas de TI					
Título:	Microsoft Flight Simulator sigue estando previsto para PS5				
Encabezado:					
Fecha:	14/09/25 (por la tarde)	Fuente:	NEWS INSTANT GAMING	Por:	Arturo Padilla
Link:	https://news.instant-gaming.com/es/articulos/14850-microsoft-flight-simulator-sigue-estando-previsto-para-ps5				

No hay duda que Microsoft planea seguir llevando sus títulos a plataformas rivales. Si bien se especula mucho al respecto con Starfield, hay otra licencia importante del fabricante estadounidense que debería debutar en PlayStation a no mucho tardar.

Según el conocido insider NateTheHate, Microsoft Flight Simulator llegará a PS5 más pronto que tarde. Explica que espera que se diga algo al respecto pronto. No es la primera vez que os contamos sobre rumores sobre la llegada del simulador de vuelo a la consola de Sony. Esperemos que no se tarde en confirmar.

Notas de TI	
Título:	Microsoft estaría planeando ampliar la capacidad computacional para modelos de IA internos
Encabezado:	El gigante tecnológico podría hacer "inversiones significativas" en sus propios clusters

Fecha:	15/09/25	Fuente:	DATA CENTER DYNAMICS	Por:	Gabriel Carrillo M-Feduchi
Link:	https://www.datacenterdynamics.com/es/noticias/microsoft-plans-to-expand-computing-capacity-for-internal-ia-models-informe/				

Microsoft estarái planeando ampliar su capacidad informática para el entrenamiento de sus propios modelos internos.

Según ha informado Bloomberg, el jefe de IA de Microsoft, Mustafa Suleyman, habría compartido algunos de los planes de la empresa con los empleados durante una reunión celebrada el 11 de septiembre.

Según Suleyman, Microsoft realizará "importantes inversiones" en sus clústeres de IA para entrenar grandes modelos lingüísticos (LLM) que espera que compitan con empresas como OpenAI y Anthropic.

A principios de 2025, Microsoft calculó que sus inversiones para ese año ascenderían a 80.000 millones de dólares.

Suleyman dijo a los empleados que es fundamental que la empresa tenga la capacidad de ser "autosuficiente" en IA.

También dijo que la empresa está "profundizando" sus lazos con OpenAI, asociándose con otros creadores de modelos y construyendo los suyos propios.

Microsoft ha rechazado hacer comentarios a Bloomberg.

Suleyman fue cofundador de DeepMind de Google, pero se unió a Microsoft en 2024. En agosto, la compañía lanzó su primer LLM bajo el liderazgo de Suleyman, que fue entrenado con 15.000 GPU Nvidia H100.

Históricamente, Microsoft ha dependido en gran medida de los LLM de OpenAI. Satya Nadella, su consejero delegado, ha declarado que están planeando desarrollar productos con un enfoque multimodelo. La semana pasada, The Information informó de que utilizará algunos modelos de OpenAI.

Microsoft y OpenAI mantienen una larga relación y han firmado un Memorando de Entendimiento no vinculante para "la siguiente fase de nuestra [su] asociación", ya que OpenAI ha reestructurado su negocio. Ambas partes siguen negociando los detalles del contrato.

Notas de TI					
Título:	¿Cómo identificar llamadas fraudulentas o de extorsión?				
Encabezado:	Las probabilidades de ser víctima de delitos digitales son elevadas				
Fecha:	14/09/25 (por la tarde)	Fuente:	INFORMADOR	Por:	

Link:	https://www.informador.mx/tecnologia/Ciberseguridad-Como-identificar-llamadas-fraudulentas-o-de-extorsion-20250912-0132.html

Ninguna persona está exenta de sufrir una extorsión. A principios de 2025, The Competitive Intelligence Unit, firma de consultoría estratégica de mercados, realizó un análisis sobre el robo de información e identidad por llamadas telefónicas.

La empresa encontró que el 34% de los usuarios de Internet han recibido llamadas sospechosas, en las que se les solicitan datos personales.

Esto demuestra que las probabilidades de ser víctima de delitos digitales son elevadas.

Por lo anterior, es importante protegerse aprendiendo a identificar si las llamadas son legítimas o si tienen fines de extorsión.

Por lo general, estas son las señales que te deben mantener alerta:

- La persona se hace pasar por alguna institución o persona de confianza para decirte que hay algo mal con tu cuenta; también te puede pedir tus datos para actualizar tu información.
- Si la persona te solicita datos personales o financieros para arreglar un supuesto problema.
- Si te hacen ofertas que suenan demasiado buenas para ser verdad.
- Si te llegan a solicitar los dígitos de tu token, NIP o códigos de verificación.
- Si el delincuente hace de todo para evitar que cuelgues la llamada, por ejemplo, se pone insistente o recurre a la intimidación.

Notas de TI					
Título:	#Ciberseguridad – 1000 millones de razones para proteger tu identidad en Internet				
Encabezado:					
Fecha:	14/09/25 (por la tarde)	Fuente:	INFOSERTEC LA	Por:	Ariel mcorg
Link:	https://infosertecla.com/2025/09/14/ciberseguridad-1000-millones-de-razones-para-proteger-tu-identidad-en-internet/				

Las filtraciones de datos son una amenaza creciente para las empresas y una pesadilla para sus clientes. Según las últimas cifras, en 2024 se produjeron 3.158 incidentes denunciados públicamente en Estados Unidos, apenas debajo del máximo histórico. Como resultado, se tuvieron que enviar más de 1.300 millones de cartas de notificación de violación de datos a las víctimas, de las cuales más de 1.000 millones se vieron afectadas por cinco mega brechas de más de 100 millones de registros cada una. ESET, comenta que hay muchas otras formas de que la información personal identificable (IPI) caiga en las manos equivocadas, pero una vez que circula en la clandestinidad de la ciberdelincuencia, es sólo cuestión de tiempo que se utilice en intentos de fraude de identidad (Fuente ESET Latam).

“Una vez que tus datos personales fueron robados, ya sea en una brecha masiva o a través de uno de los distintos métodos existentes, es probable que estos datos sean vendidos o cedidos a otros para su uso en diversos esquemas de fraude. Esto podría ir desde compras ilegales hasta la toma de

control de cuentas (ATO), fraude de cuentas nuevas o esquemas de phishing diseñados para obtener información aún más sensible. En algunos casos, se mezclan datos reales con otros generados por máquinas para crear identidades sintéticas más difíciles de bloquear por los filtros antifraude.", comenta Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de Seguridad Informática de ESET Latinoamérica.

¿De qué datos están en juego?

- Nombres y direcciones
- Números de tarjetas de crédito/pago
- Números de documentos de identidad oficiales
- Números de cuentas bancarias
- Datos de credenciales de servicios de salud
- Pasaporte o carné de conducir
- Datos de acceso a cuentas personales y de empresa en Internet

El fraude de identidad se reduce a los datos, por lo que es importante comprender cómo los ciberdelincuentes consiguen la información. Si no están robando grandes cantidades de datos de terceras organizaciones, los principales vectores de ataques dirigidos contra individuos son:

- Phishing/smishing/vishing: los ataques clásicos de ingeniería social pueden producirse a través de varios canales, desde el tradicional phishing por correo electrónico hasta mensajes de texto (smishing) e incluso llamadas telefónicas(vishing). El autor de la amenaza suele utilizar técnicas conocidas y probadas para engañar y conseguir que se cumplan sus órdenes, que suelen ser hacer clic en un enlace malicioso, rellenar datos personales o abrir un archivo adjunto malicioso. Entre ellas se incluyen el uso de marcas oficiales para hacerse pasar por una empresa o institución conocida, y trucos como la suplantación del identificador de llamadas o del dominio.
- Robo digital: Para hacerse con los datos de su tarjeta, los autores de la amenaza pueden insertar un código malicioso de skimming en las páginas web de un sitio popular de comercio electrónico o similar. Todo el proceso es completamente invisible para la víctima.
- Wi-Fi públicas: las redes Wi-Fi públicas no seguras pueden facilitar los ataques man-in-the-middle en los que se intercepta información personal. Los hackers también pueden instalar puntos de acceso fraudulentos para recopilar datos y redirigir a las víctimas a sitios maliciosos.
- Malware: el malware Infostealer es un problema creciente tanto para usuarios corporativos como para consumidores. Puede instalarse involuntariamente a través de diversos mecanismos, como mensajes de phishing, descargas no solicitadas de sitios web infectados, juegos pirateados, anuncios de Google o incluso aplicaciones de aspecto legítimo, como falsos programas de reuniones. La mayoría de los infostealers cosechan archivos, flujos de datos, detalles de tarjetas, criptoactivos, contraseñas y pulsaciones de teclas.
- Publicidad maliciosa: Los anuncios maliciosos pueden programarse para robar información, a veces incluso sin exigir la interacción del usuario.
- Sitios web maliciosos: Los sitios de phishing pueden falsificarse para que parezcan auténticos, hasta el dominio. En el caso de los drive-by-downloads, basta con que el usuario visite una página maliciosa para que se inicie la instalación encubierta del malware. A menudo, los sitios web maliciosos se colocan en las primeras posiciones de los rankings de búsqueda para tener una mayor exposición, gracias a nefastas técnicas de SEO.
- Aplicaciones maliciosas: Los programas maliciosos, incluidos los troyanos bancarios y los ladrones de información, pueden camuflarse como aplicaciones legítimas, con un riesgo especialmente alto fuera de las tiendas de aplicaciones oficiales como Google Play.

- Pérdida o robo de dispositivos: Si pierdes tu dispositivo y no cuentas con la protección adecuada, los hackers podrían asaltarlo en busca de datos personales y financieros.

Desde ESET comparten algunas buenas prácticas para aplicar en conjunto y evitar así que los delincuentes accedan a la información personal y financiera:

- Contraseñas fuertes y únicas: Elegir una contraseña distinta para cada sitio, aplicación o cuenta, y guardarlas en un gestor de contraseñas. Activar la autenticación de doble factor (2FA) en las cuentas, de esta forma, aunque alguien obtenga la contraseña, no podrá utilizarla. La mejor opción es una aplicación de autenticación o una llave de seguridad.
- Instalar software de seguridad: Esto escaneará y bloqueará aplicaciones y descargas maliciosas, detectará y bloqueará sitios web de phishing y alertará sobre actividades sospechosas, entre otras.
- Ser escépticos/as: Prestar atención a las señales de advertencia del phishing: un mensaje no solicitado que insta a actuar con rapidez y que contiene enlaces o archivos adjuntos. Algunas excusas que usan para engañar son supuestos sorteos de premios con límite de tiempo o advertencias de multas si no se responde cuanto antes.
- Utilizar únicamente aplicaciones de sitios legítimos: App Store de Apple y a Google Play, por ejemplo, para disminuir la probabilidad de descargar aplicaciones maliciosas. Comprobar las reseñas y los permisos antes de descargarlas.
- Desconfiar de las redes Wi-Fi públicas: Mantenerse alejado de las redes Wi-Fi públicas o, si se debe usar una no ingresar a cuentas sensibles mientras se esté conectado. En cualquier caso, utilizar una VPN.

Frente una filtración de información hay algunas medidas importantes a tomar de forma rápida. Como primer paso hay que comunicarlo al banco, para bloquear las tarjetas (se puede hacer a través de la mayoría de las aplicaciones bancarias), denunciar el fraude y solicitar tarjetas de sustitución. También, hacer la denuncia frente a las autoridades, principalmente la policía, y las entidades que sean pertinentes: por ejemplo si robaron la licencia de conducir la denuncia se realiza frente al organismo que la emitió. Además, cambiar las claves de acceso y, en caso de no haberlo hecho antes, activar el doble factor de autenticación (2FA).

“El fraude de identidad sigue siendo una amenaza porque es relativamente fácil obtener beneficios en el mundo cibercriminal. Al reducir las vías que pueden utilizar para extraer la información personal, podemos incomodar a nuestros adversarios y mantener nuestras propias vidas digitales a salvo y seguras.”, concluye Gutiérrez Amaya de ESET.

Notas de TI					
Título:	Equipadas con Inteligencia artificial, estas son las nuevas patrullas que operarán en la capital potosina				
Encabezado:	Se trata de 53 nuevas unidades y son patrullas de fábrica, es decir, no vehículos habilitados como patrulla, cuyos conductores tendrán respaldo de IA.				
Fecha:	14/09/25 (por la tarde)	Fuente:	OEM	Por:	Miguel Ángel Mora
Link:	https://oem.com.mx/elsoldesanluis/local/estas-son-las-nuevas-patrullas-con-inteligencia-artificial-que-operaran-en-la-capital-potosina-25764421				

Más de medio centenar de nuevas patrullas, que operarán apoyadas con inteligencia artificial, fueron puestas en operación la noche de este domingo por el alcalde capitalino, Enrique Francisco Galindo Ceballos, quien a la par anunció está próximo un equipamiento extraordinario para los elementos de la Secretaría de Seguridad y Protección Ciudadana, que incluirá uniformes y chalecos antibalas, entre otros.

En su intervención en la entrega de tales unidades que se llevó a cabo en la glorieta Revolución, hizo un reconocimiento a los elementos que integran la Guardia Municipal, la Policía Vial y de Movilidad y la Policía de Tecnologías e Inteligencia Social, así como a los integrantes de los Comités Ciudadanos de Seguridad; de estos últimos, dijo, “son el arma secreta” contra la delincuencia en cada uno de los sectores de la ciudad.

Las nuevas unidades, un total de 53, son patrullas de fábrica, es decir, no vehículos habilitados como patrulla, cuyos conductores tendrán respaldo de Inteligencia Artificial, cuentan con sistema de vigilancia terrestre y sistema de videovigilancia móvil, lo que coadyuvará a reforzar la seguridad en San Luis capital.

Galindo Ceballos también agradeció la presencia de representantes del Gobierno Federal y del Ejército Mexicano, que fueron testigos de una demostración de la tecnología con que cuentan las nuevas unidades, ya en color azul y blanco; mencionó que todo el parque vehicular policíaco municipal tendrá estos colores.

En este sentido, el titular de la Secretaría de Seguridad y Prorección Ciudadana, Juan Antonio de Jesús Villa Gutiérrez, recordó que la corporación fue criticada por el logotipo de “PoliSÍa”, pero “rompimos esquemas porque nos atrevimos a innovar”; hoy, las unidades inspirarán más confianza. Durante el evento, no se habló de la inversión por la adquisición de las nuevas patrullas.
“Y no es solamente un cambio de imagen es ahora un cuerpo policíaco más sólido. “(Las unidades) están equipadas con con cámaras en tiempo real, lo que garantiza mayor transparencia y capacidad de respuesta”, detalló.

Al evento asistieron los integrantes de la comisión de Policía Preventiva, Vialidad y Transporte, que integran los regidores Jorge Alberto Zavala López, Rubén Omar Larraga Benavente, Luz Magdalena Cisneros Jiménez, Irene Margarita Hernández Fiscal, y Alejandro Fernández Hernández, que reconocieron hoy la capital potosina da un nuevo paso firme en el camino de la seguridad que permita a la ciudadanía vivir con tranquilidad y confianza.

Notas de TI					
Título:	Ecosistemas en la nube aceleran digitalización empresarial en México				
Encabezado:	La transformación digital en México alcanzará los 88.33 mil mdd en 2030, impulsada por ecosistemas financieros en la nube que centralizan operaciones. Un modelo que integra datos, reduce costos y acelera la competitividad empresarial.				
Fecha:	14/09/25 (por la tarde)	Fuente:	REAL ESTATE MARKET	Por:	Alejandra Cañedo
Link:	https://realestatemarket.com.mx/noticias/49075-ecosistemas-en-la-nube-aceleran-digitalizacion-empresarial-en-mexico				

El mercado de transformación digital en México alcanzará USD 88.33 mil millones en 2030, impulsado por ecosistemas financieros en la nube que unifican operaciones y optimizan recursos.

La transformación digital en México avanza con rapidez y se perfila como un factor decisivo para la competitividad empresarial. Según el reporte El tamaño del mercado de transformación digital de México y análisis de participación, el valor del sector alcanzará 39.98 mil millones de dólares en 2025, con la expectativa de superar los 88.33 mil mdd para 2030, impulsado por una tasa de crecimiento anual compuesta del 17.18 por ciento.

A pesar de este crecimiento, muchas organizaciones aún enfrentan un obstáculo clave: La fragmentación de procesos.

Finanzas, ventas, inventarios y atención al cliente suelen gestionarse de manera aislada, lo que genera reportes dispersos y limita la capacidad de respuesta en tiempo real.

Frente a este reto, los ecosistemas financieros en la nube se consolidan como una alternativa estratégica. Al centralizar operaciones, estas plataformas permiten automatizar tareas críticas, integrar datos y convertir información en acciones concretas, con un nivel de eficiencia que reduce costos y acelera la toma de decisiones.

Empresas de México y CA. aceleran transformación digital e innovación

“El reto consiste en consolidar datos y automatizar tareas críticas en una sola plataforma financiera accesible y en la nube, para anticiparse a los cambios del mercado”.

La adopción de estas herramientas no solo se traduce en mayor eficiencia, sino también en una simplificación operativa que libera recursos para la innovación, la estrategia y la experiencia del consumidor.

En un país donde las condiciones del mercado cambian con rapidez, las empresas que centralicen sus procesos digitales estarán mejor posicionadas para crecer y adaptarse a la economía digital.

Notas de TI					
Título:	Protección de datos en IA: Desafíos y soluciones				
Encabezado:					
Fecha:	14/09/25 (por la tarde)	Fuente:	MARTES TECNÓLOGICO	Por:	
Link:	https://www.martestecnologico.com/proteccion-de-datos-en-ia-desafios-y-soluciones/				

La inteligencia artificial (IA) ha revolucionado la forma en que las empresas operan, ofreciendo oportunidades sin precedentes para mejorar la eficiencia y la toma de decisiones. Sin embargo, esta transformación digital también plantea serias preocupaciones sobre la protección de datos. A medida que las organizaciones recopilan y analizan grandes volúmenes de información personal, la necesidad de salvaguardar estos datos se vuelve crítica.

La protección de datos en el contexto de la IA no solo es un imperativo legal, sino también un componente esencial para mantener la confianza del consumidor y la reputación empresarial. La recopilación y el procesamiento de datos son fundamentales para el funcionamiento de los sistemas de ISin embargo, el uso indebido o la exposición de datos sensibles puede tener consecuencias devastadoras. Desde violaciones de datos hasta el uso no autorizado de información personal, los riesgos son numerosos.

Por lo tanto, es esencial que las empresas implementen estrategias robustas para proteger los datos que alimentan sus algoritmos de IEn este artículo, exploraremos los desafíos, regulaciones y soluciones tecnológicas relacionadas con la protección de datos en el ámbito de la inteligencia artificial.

Resumen

- La protección de datos en inteligencia artificial es crucial para garantizar la privacidad y seguridad de los usuarios.
- Los desafíos de la protección de datos en IA incluyen la recopilación masiva de información, el riesgo de sesgos y la falta de transparencia en los algoritmos.
- Las regulaciones y marcos legales en protección de datos en el ámbito de la inteligencia artificial varían según el país, lo que dificulta la aplicación de normativas globales.
- Las soluciones tecnológicas para la protección de datos en IA incluyen el cifrado, la anonimización de datos y el desarrollo de algoritmos éticos.
- La ética y responsabilidad en el uso de datos en inteligencia artificial son fundamentales para evitar el uso indebido de la información personal de los usuarios.

Desafíos de la protección de datos en IA

Uno de los principales desafíos en la protección de datos en IA es la naturaleza misma de los algoritmos. Estos sistemas a menudo requieren grandes cantidades de datos para aprender y mejorar su rendimiento. Sin embargo, la recopilación masiva de datos plantea preguntas sobre el consentimiento y la privacidad.

Muchas veces, los usuarios no son plenamente conscientes de cómo se utilizan sus datos, lo que puede llevar a una falta de confianza en las tecnologías basadas en IA. Además, la complejidad de los modelos de IA puede dificultar la transparencia. Los algoritmos pueden ser considerados «cajas negras», donde es difícil entender cómo se toman las decisiones.

Esta falta de claridad puede complicar aún más la protección de datos, ya que las empresas pueden tener dificultades para garantizar que están cumpliendo con las regulaciones pertinentes. La dificultad para auditar y rastrear el uso de datos en estos sistemas puede resultar en incumplimientos involuntarios, lo que a su vez puede acarrear sanciones severas.

Regulaciones y marcos legales en protección de datos en el ámbito de la inteligencia artificial
Data protection

A medida que la preocupación por la privacidad y la protección de datos ha crecido, también lo han hecho las regulaciones que rigen su uso. En Europa, el Reglamento General de Protección de Datos

(RGPD) establece un marco legal estricto para el manejo de datos personales. Este reglamento no solo exige que las empresas obtengan el consentimiento explícito de los usuarios antes de procesar sus datos, sino que también les otorga derechos sobre su información, como el derecho a ser olvidado.

En otras regiones, como Estados Unidos, la regulación es menos uniforme, pero se están desarrollando leyes específicas que abordan la protección de datos en el contexto de la IPor ejemplo, California ha implementado la Ley de Privacidad del Consumidor (CCPA), que otorga a los consumidores más control sobre sus datos personales. Sin embargo, a pesar de estos avances, aún existe una falta de consenso global sobre cómo regular adecuadamente el uso de datos en IA, lo que puede crear confusión y desafíos para las empresas que operan a nivel internacional.

Soluciones tecnológicas para la protección de datos en IA

Para abordar los desafíos asociados con la protección de datos en IA, las empresas están adoptando diversas soluciones tecnológicas. Una estrategia clave es la implementación de técnicas de anonimización y seudonimización. Estas prácticas permiten a las organizaciones utilizar datos sin revelar información personal identificable, lo que reduce el riesgo asociado con el manejo de datos sensibles.

Otra solución emergente es el uso de tecnologías basadas en blockchain para garantizar la integridad y seguridad de los datos. Al registrar transacciones en un libro mayor descentralizado, las empresas pueden crear un historial inmutable del uso de datos, lo que facilita la auditoría y el cumplimiento normativo. Además, las herramientas de gestión del consentimiento están ganando popularidad, permitiendo a los usuarios controlar cómo se utilizan sus datos y otorgar o revocar permisos según sea necesario.

Ética y responsabilidad en el uso de datos en inteligencia artificial

La ética juega un papel fundamental en la discusión sobre la protección de datos en ILas empresas deben considerar no solo lo que es legalmente aceptable, sino también lo que es moralmente correcto al utilizar datos personales. La responsabilidad ética implica ser transparente sobre cómo se recopilan y utilizan los datos, así como garantizar que no se perpetúen sesgos o discriminación a través del uso indebido de algoritmos. Además, las organizaciones deben fomentar una cultura interna que priorice la ética en el manejo de datos.

Esto incluye capacitar a los empleados sobre las mejores prácticas y establecer políticas claras sobre el uso responsable de la información. Al adoptar un enfoque ético hacia la protección de datos, las empresas no solo cumplen con las regulaciones, sino que también construyen una relación más sólida y confiable con sus clientes.

Impacto de la protección de datos en IA en la privacidad de los usuarios

La protección adecuada de los datos en IA tiene un impacto directo en la privacidad del usuario. Cuando las empresas implementan medidas efectivas para salvaguardar la información personal, los consumidores se sienten más seguros al interactuar con tecnologías basadas en IEsto no solo mejora la experiencia del usuario, sino que también fomenta una mayor adopción de estas

tecnologías. Sin embargo, si las empresas fallan en proteger los datos, pueden enfrentar consecuencias graves.

Las violaciones de datos pueden resultar en pérdidas financieras significativas y daños a la reputación. Además, los usuarios pueden optar por no utilizar servicios que no garanticen su privacidad, lo que puede limitar el crecimiento y la innovación en el sector tecnológico. Por lo tanto, invertir en protección de datos no solo es una cuestión legal; es una estrategia comercial inteligente.

Casos de uso y buenas prácticas en la protección de datos en inteligencia artificial

Existen numerosos casos donde las empresas han implementado buenas prácticas para proteger los datos en sus sistemas de IUn ejemplo notable es el sector financiero, donde las instituciones utilizan algoritmos para detectar fraudes mientras protegen la información personal del cliente mediante técnicas avanzadas de cifrado y anonimización. Estas prácticas no solo ayudan a prevenir fraudes, sino que también aseguran que los clientes confíen en cómo se manejan sus datos. Otro caso ejemplar se encuentra en el ámbito sanitario.

Las organizaciones están utilizando IA para analizar grandes volúmenes de datos clínicos con el fin de mejorar diagnósticos y tratamientos. Sin embargo, estas instituciones también están adoptando medidas estrictas para proteger la privacidad del paciente, como el uso de consentimientos informados y protocolos robustos para el manejo seguro de información sensible. Estas iniciativas demuestran que es posible innovar mientras se prioriza la protección de datos.

Conclusiones y recomendaciones para la protección de datos en el contexto de la inteligencia artificial

En conclusión, la protección de datos en inteligencia artificial es un tema crítico que requiere atención constante por parte de las empresas. A medida que avanzamos hacia un futuro cada vez más digitalizado, es fundamental adoptar un enfoque proactivo hacia la gestión y protección de información personal. Las organizaciones deben estar al tanto de los desafíos regulatorios y tecnológicos y buscar soluciones innovadoras para mitigar riesgos.

Recomendamos a las empresas implementar políticas claras sobre el manejo ético y responsable de los datos, así como invertir en tecnologías que fortalezcan su capacidad para proteger información sensible. Además, fomentar una cultura organizacional centrada en la ética ayudará a construir confianza con los consumidores y garantizará un uso responsable y sostenible de la inteligencia artificial. Al hacerlo, no solo cumplirán con las regulaciones vigentes, sino que también estarán mejor posicionadas para aprovechar las oportunidades que ofrece esta tecnología transformadora.

En el contexto de la protección de datos en inteligencia artificial, es relevante considerar cómo la apertura de datos puede influir en el desarrollo de tecnologías más seguras y eficientes. Un artículo relacionado que aborda este tema es Empresario tecnológico aboga por la apertura de datos para enfrentar desafíos climáticos. Este artículo discute cómo la compartición de datos puede ser crucial para enfrentar problemas globales, como el cambio climático, y cómo esta práctica debe equilibrarse cuidadosamente con la protección de la privacidad y la seguridad de los datos personales.