

Notas de Electrónica					
Título:	Con un 'Cuarto Limpio', IPN impulsa elaboración de semiconductores				
Encabezado:	Este tipo de tecnología se usa para la elaboración de semiconductores, hasta procesos vinculados con la cadena de suministro.				
Fecha:	25/01/26 (por la tarde)	Fuente:	MILENIO	Por:	Alma Paola Wong
Link:	https://www.milenio.com/ciencia-y-salud/ipn-impulsa-elaboracion-de-semiconductores				

- Infraestructura clave:

- El Instituto Politécnico Nacional (IPN), a través del Laboratorio Nacional de Micro y Nanotecnologías (LNunT), cuenta con un Cuarto Limpio Clase 100 (ISO 5) certificado por la Secihti.
- Equipado con filtros ULPA que retienen partículas de hasta 0.1 micrómetros y un flujo de aire laminar en 200 m², garantiza un ambiente controlado indispensable para la producción de semiconductores.

- Formación de talento especializado:

- El laboratorio prepara profesionales en microelectrónica, nanotecnología, MEMS, celdas solares, sensores y dispositivos de película delgada.
- Responde a la creciente demanda global de expertos en semiconductores, un sector estratégico para la industria tecnológica.

- Aplicaciones industriales y médicas:

- Se trabaja principalmente con silicio (Si), base de microprocesadores, chips y dispositivos electrónicos.
- Colaboración con la Escuela Superior de Medicina (ESM) para producir semiconductores micrométricos que apoyen el diagnóstico temprano de enfermedades como el cáncer.

- Impacto estratégico:

- La certificación permite aplicar técnicas avanzadas de diseño, fabricación y caracterización de procesadores a distintas escalas.
- Esto se traduce en mayor rapidez y capacidad de respuesta de los dispositivos, fortaleciendo la cadena de suministro nacional y la competitividad global.

En síntesis: El IPN consolida su papel como referente en la producción de semiconductores en México, combinando infraestructura de alto nivel, investigación aplicada y formación de talento para atender tanto necesidades industriales como médicas.

Notas de Electrónica					
Título:	Costa Rica no cierra puertas a ser el primer país del hemisferio en entrar al Pax Silica, la nueva iniciativa de EE.UU. para desarrollo de semiconductores				
Encabezado:	Costa Rica mantiene la apuesta por convertir a los semiconductores en uno de los pilares de su producción industrial. En...				
Fecha:	26/01/26	Fuente:	EL OBSERVADOR	Por:	Tomás Gómez

Link:	https://observador.cr/costa-rica-no-cierra-puertas-a-ser-el-primer-pais-del-hemisferio-en-entrar-al-pax-silica-la-nueva-iniciativa-de-ee-uu-para-desarrollo-de-semiconductores/
-------	---

- Apuesta estratégica de Costa Rica

- El país busca consolidar a los semiconductores como pilar de su producción industrial.
- Ya participa en la CHIPS Act de EE. UU. y ahora analiza integrarse a Pax Silica, la nueva alianza tecnológica impulsada por Washington.
- El ministro de Comercio Exterior, Manuel Tovar, expresó interés en que la iniciativa se expanda hacia América Latina.

- Pax Silica: objetivos y alcance

- Lanzada en diciembre por EE. UU., busca construir una cadena de suministro segura y próspera de silicio y tecnologías asociadas.
- Áreas clave: semiconductores, inteligencia artificial, manufactura avanzada, logística, energía y minerales críticos.
- Propósito: reducir dependencias, proteger capacidades estratégicas y garantizar el desarrollo de tecnologías transformadoras.
- Participantes iniciales: Japón, Corea del Sur, Singapur, Holanda, Reino Unido, Israel, Emiratos Árabes Unidos y Australia.

- Relaciones internacionales de Costa Rica

- El país ya mantiene vínculos con varios miembros de Pax Silica (Israel, Japón, Australia, Corea del Sur, Emiratos Árabes Unidos).
- Busca aprovechar estas relaciones para integrarse y fortalecer su papel en la resiliencia de cadenas de suministro y en el ecosistema de IA y semiconductores.

- Líneas de acción de Pax Silica

- Asegurar la cadena tecnológica global (software, conectividad, semiconductores, energía).
- Impulsar proyectos conjuntos en diseño, fabricación y empaquetado de chips.
- Promover coinversiones estratégicas y proteger tecnologías sensibles.
- Construir ecosistemas tecnológicos confiables (TIC, fibra óptica, centros de datos).

En síntesis: Costa Rica busca posicionarse como actor relevante en la nueva arquitectura global de semiconductores y tecnologías críticas, aprovechando su relación con países miembros de Pax Silica y su experiencia previa con la CHIPS Act.

Notas de Electrónica					
Título:	China desarrolla "chips de fibra" tan finos como un cabello.				
Encabezado:	Científicos chinos acaban de lograr un gran avance en la tecnología de semiconductores al desarrollar con éxito un chip flexible, del grosor de una fibra capilar, con un potente rendimiento de procesamiento. Esta innovación promete transformar la ropa común en dispositivos inteligentes para el control de la salud y el control remoto.				
Fecha:	26/01/26	Fuente:	VIETNAM	Por:	Báo Pháp Luật Việt Nam
Link:	https://www.vietnam.vn/es/trung-quoc-che-tao-chip-soi-mong-nhu-toc				

- Innovación clave:

- Un equipo liderado por el profesor Peng Huisheng desarrolló un circuito integrado basado en fibra (CIF).
- En lugar de usar obleas rígidas de silicio, los transistores se fabrican sobre una lámina de polímero enrollada en forma de cable microscópico.

- Características técnicas:

- Diámetro similar al de un cabello humano.
- Contiene docenas de capas de circuitos eléctricos apilados.
- Densidad: 100,000 transistores por centímetro de longitud.
- Capaz de realizar tareas complejas: adquisición de señales, procesamiento de datos y reconocimiento de imágenes con IA.

- Durabilidad comprobada:

- Resiste doblado, estiramiento y lavado con agua y detergente.
- La carcasa de polímero flexible protege los componentes internos.
- Incluso soportó el paso de un camión de 15.6 toneladas sin daños ni pérdida de rendimiento.

- Impacto tecnológico:

- Transforma las fibras inteligentes: de simples sensores a tejidos con capacidad de procesamiento ("cerebro informático").
- Compatible con procesos textiles industriales, lo que facilita la producción masiva.

- Aplicaciones potenciales:

- Salud: camisetas que monitorean signos vitales en tiempo real; implantes blandos más compatibles con el cuerpo; interfaces cerebro-computadora para personas con discapacidad.
- Entretenimiento: guantes de realidad virtual ligeros y realistas.
- Industria textil: prendas inteligentes conectadas y funcionales.

En síntesis: Los chips de fibra representan un punto de inflexión en la electrónica portátil y médica, al integrar procesamiento avanzado directamente en los tejidos, con alta resistencia y viabilidad industrial.

Notas de Electrónica					
Título:	China y el nuevo telón de acero digital: la carrera por el trono de los microprocesadores				
Encabezado:					
Fecha:	25/01/26 (por la tarde)	Fuente:	EL NUEVO DIARIO	Por:	
Link:	https://elnuevodiario.com.do/china-y-el-nuevo-telon-de-acero-digital-la-carrera-por-el-trono-de-los-microprocesadores/				

- El poder del silicio

- Los microprocesadores son considerados el "petróleo del futuro", esenciales para la economía digital, la seguridad nacional y la innovación tecnológica.
- El dominio en semiconductores define ventajas en IA, ciberseguridad y defensa militar.

- Occidente vs. China
 - Occidente mantiene hegemonía gracias a la alianza entre EE. UU. (diseño), ASML (maquinaria) y TSMC (manufactura).
 - China busca romper su dependencia con el plan Made in China 2025, impulsando autosuficiencia mediante subsidios, talento y ecosistemas locales.
 - Las sanciones estadounidenses (2018–2025) intentaron frenar el avance chino, pero aceleraron la inversión interna.
- El caso Huawei
 - Sancionada en 2019, se convirtió en símbolo de resiliencia.
 - Desarrolló HarmonyOS y el chip Kirin 9000S (7nm) fabricado en China, demostrando capacidad local.
 - Entre 2020–2025, China invirtió más de 100 mil millones de dólares en su industria de semiconductores.
- Avances chinos bajo sanciones
 - SMIC produce chips de 7nm desde 2023.
 - En 2026, China presentó un prototipo de máquina EUV, clave para chips sub-5nm.
 - Mercado chino de semiconductores: 393 mil millones de dólares en 2025, con 30% del mercado global de equipos.
 - Plan Quinquenal 2026–2030: autosuficiencia en herramientas, innovación en IA y expansión en materiales avanzados como carburo de silicio (SiC).
- Estrategia occidental
 - “Bloqueo de precisión”: prohibición de máquinas EUV de ASML y subsidios vía CHIPS Act (52 mil millones USD) para repatriar producción.
 - Bajo Trump (2025–2026) hubo alivios parciales: venta de chips Nvidia H200 permitida, aunque China ya prioriza soluciones locales.
 - Expertos estiman que China está solo dos años detrás en diseño de semiconductores.
- Implicaciones globales
 - Tensiones en Taiwán impulsan diversificación hacia Europa, India y Vietnam.
 - Riesgo de desacoplamiento total: mayores costos y menor innovación, aunque con competencia más amplia.
 - China proyecta liderar capacidad de producción hacia 2030 con un mercado de 295 mil millones USD.
 - Occidente ajusta hacia un modelo de “derisking” selectivo, equilibrando seguridad y comercio.

En síntesis: La carrera por los semiconductores redefine el orden mundial. China, con inversión estatal masiva y avances tecnológicos, acorta la brecha con Occidente. El resultado decidirá no solo quién lidera la innovación, sino el futuro de la humanidad digital.

Notas de Telecomunicaciones	
Título:	Registro celular, impacto a la población
Encabezado:	La medida se impulsa como una respuesta directa al aumento de la extorsión y el fraude telefónico

Fecha:	26/01/26	Fuente:	EL HERALDO DE MÉXICO	Por:	Darío Celis
Link:	https://heraldodemexico.com.mx/opinion/2026/1/26/registro-celular-impacto-la-poblacion-762414.html#google_vignette				

- Medida en vigor:

- Desde el 9 de enero de 2026, cada línea móvil debe vincularse a una identidad validada con CURP y documentos oficiales.
- Objetivo: combatir extorsión y fraude telefónico.

- Magnitud del reto:

- México cerró 2025 con 160 millones de líneas activas, de las cuales 85% son de prepago (anónimas y de alta rotación).
- Regularizar este universo exige registrar 1 millón de líneas diarias hasta junio de 2026, un desafío técnico extremo.

- Impacto en operadores:

- Telcel, AT&T, Movistar, Bait y Altán Redes deben asumir la identificación, resguardo de datos y validaciones biométricas.
- No existe padrón centralizado: los datos quedan bajo custodia de las empresas, que cargan con los riesgos legales y reputacionales.
- Primeros días: plataformas saturadas, fallas en validaciones y vulnerabilidades detectadas, generando desconfianza.

- Reacción ciudadana:

- Usuarios temen filtraciones de datos sensibles, dada la historia de vulnerabilidades en México.
- El enojo se dirige a las marcas: la suspensión de líneas no registradas afecta directamente la relación cliente-operador.
- En prepago, la lealtad es mínima, lo que aumenta el riesgo de abandono masivo.

- Debate sobre eficacia:

- El gobierno afirma que 90% de las extorsiones se realizan vía telefónica, pero muchas provienen de plataformas digitales y números virtuales fuera del control de operadores.
- El registro ordena el mercado formal, pero no neutraliza esquemas criminales adaptativos.
- Experiencia previa: el Panaut fue invalidado por la Suprema Corte; el nuevo modelo insiste en que no centraliza datos, aunque el efecto práctico es similar.

- Conclusión:

- La política busca eliminar el anonimato en telefonía móvil, trasladando al sector privado una función de seguridad pública.
- El problema no es la intención, sino la implementación: tiempos poco realistas, riesgos operativos y costos desproporcionados para las empresas.
- Telcel, AT&T y Movistar enfrentan el mayor desgaste, al tener que invertir millones y absorber la frustración de los usuarios.

En síntesis: El registro obligatorio de líneas móviles en México es una política con objetivos legítimos, pero su ejecución genera tensiones técnicas, económicas y sociales, dejando a los operadores en el centro del conflicto.

Notas de TI					
Título:	Señala OCDE pros y contras de usar IA en servicios públicos				
Encabezado:					
Fecha:	26/01/26	Fuente:	CONSUMOTIC	Por:	Juan Carlos Villarruel
Link:	https://consumotic.mx/tecnologia/senala-ocde-pros-y-contras-de-usar-ia-en-servicios-publicos/				

- Potencial de la IA: Automatizar y personalizar servicios, detectar fraudes y apoyar a funcionarios.
- Principales riesgos: Sesgos en datos, falta de transparencia, ampliación de brechas digitales, baja calidad de información y sistemas obsoletos.
- Adopción desigual: Varía entre países y funciones.
 - 57% de los casos analizados se enfocan en automatización y personalización de servicios.
 - 45% en diseño y prestación de servicios públicos.
 - 29% en participación ciudadana y gobierno abierto.
 - 25% en justicia y acceso a la justicia.
 - 22% en aplicación de la ley y gestión de riesgos.
- Áreas con menor uso: Evaluación de políticas públicas, administración tributaria y gestión de la función pública, limitadas por sistemas obsoletos y regulaciones estrictas.
- Madurez tecnológica: Algunos sectores emplean aprendizaje automático; otros dependen de enfoques normativos tradicionales.
- Retos clave:
 - Falta de marcos para medir impacto y retorno de inversión.
 - Escasez de competencias digitales.
 - Dificultades para acceder y compartir datos de calidad.
 - Costos financieros y leyes obsoletas.
- Recomendaciones de la OCDE:
 - Fortalecer habilitadores para una IA confiable.
 - Establecer salvaguardas para anticipar riesgos.
 - Involucrar a actores sociales en la implementación.
 - Seguir el Marco de la OCDE para una IA Confiable en el Sector Público como guía estratégica.

En síntesis: La IA ofrece beneficios claros para gobiernos, pero su éxito depende de superar barreras técnicas, regulatorias y sociales, garantizando transparencia y confianza ciudadana.

Notas de TI	
Título:	IA, ciberseguridad y soberanía de datos impulsarán disputas legales

Encabezado:					
Fecha:	26/01/26	Fuente:	CONSUMOTIC	Por:	Redacción
Link:	https://consumotic.mx/tecnologia/temen-abogados-incremento-de-disputas-legales-derivadas-del-uso-tecnologico/#google_vignette				

- Principales motores de disputas
 - IA y ciberseguridad: 8 de cada 10 abogados ven estas áreas como detonantes de conflictos legales.
 - Soberanía y localización de datos: regulaciones crecientes amplifican riesgos.
 - Geopolítica y comercio internacional: aranceles, sanciones y controles de exportación preocupan al 79% de los encuestados.
- Áreas críticas de exposición
 - Ciberseguridad y privacidad de datos: primer riesgo en disputas e investigaciones.
 - Fiscalidad internacional: precios de transferencia y el Impuesto Mínimo Global (OCDE, Pilar Dos) con impacto reputacional.
 - Operaciones y cadena de suministro: 78% teme fallas de proveedores, logística y escasez de mano de obra.
- Brechas de preparación
 - 38% de las empresas reconoce presupuestos insuficientes para litigios futuros.
 - Solo 39% considera tener recursos adecuados.
 - Deficiencias clave:
 - Preservación de datos forenses (52%).
 - Coordinación transfronteriza (48%).
 - Protocolos internos de investigación (45%).
- Investigaciones transfronterizas
 - 82% teme enfrentar una investigación multiagencia en los próximos 12 meses.
 - La globalización, antes vista como protección, ahora se percibe como vulnerabilidad.
- Conclusión del informe
 - La digitalización acelerada y las tensiones geopolíticas incrementan la complejidad del riesgo legal.
 - Panorama manejable si las organizaciones invierten en:
 - Gobernanza corporativa y cumplimiento normativo.
 - Coordinación transfronteriza.
 - Gestión robusta del dato y gobernanza de la IA.

En síntesis: La IA y la ciberseguridad son ya el principal foco de disputas legales globales. Las empresas deben reforzar preparación, gobernanza y coordinación internacional para contener riesgos en un entorno cada vez más fragmentado.

Notas de TI	
Título:	El Instituto Politécnico Nacional ofrece apoyo en ciberseguridad para la Copa Mundial FIFA 2026

Encabezado:					
Fecha:	26/01/26	Fuente:	RADIO FORMULA MORELOS	Por:	Luis Herrera
Link:	https://radioformulamorelos.com/ipn-ciberseguridad-fifa-2026/				

Puntos Clave:

- Apoyo del IPN: El Instituto Politécnico Nacional ofrece transferencia de tecnología y protocolos de respuesta para reforzar la seguridad digital del Mundial.
- Enfoque de ciclo completo: Acciones antes, durante y después del torneo: prevención, contención, erradicación y aprendizaje.
- Protección de datos críticos: Se priorizan boletaje, telecomunicaciones, banca electrónica y plataformas públicas.
- Cooperación trinacional: México, Estados Unidos y Canadá coordinan esfuerzos, complementados con capacidades académicas.
- Ciberresiliencia como meta: No se busca “cero incidentes”, sino cero colapsos en servicios críticos.

Contexto:

- El Mundial 2026 depende de infraestructura digital para boletos, movilidad, pagos y transmisión.
- Un fallo menor (ej. proveedor de QR) puede escalar a caos operativo.
- La propuesta del IPN se asemeja a un “ensayo general” tecnológico con simulaciones de fallos y protocolos claros de mando y comunicación.

Áreas de impacto:

- Boletaje: Prevención de fraude, phishing y reventa con autenticación multifactor y monitoreo de anomalías.
- Telecomunicaciones y pagos: Continuidad operativa como parte de la seguridad; ataques pueden generar caos físico y pérdidas económicas.
- Datos personales: Minimización y control de acceso en múltiples puntos de captura (apps, kioscos, voluntariado).
- Infraestructura crítica: Estadios conectados, nube y cadena de suministro requieren arquitectura coherente para evitar fallos sistémicos.

Conclusión:

La ciberseguridad en FIFA 2026 será un componente esencial de orden público, economía y confianza social. El IPN busca que el torneo no sea un “laboratorio de vulnerabilidades”, sino un ejemplo de servicios digitales robustos y resilientes bajo presión.

Notas de TI					
Título:	Cuatro ciberataques por segundo en México: los archivos más comunes son PDF y facturas				
Encabezado:	Ciberdelincuentes usan facturas y archivos adjuntos para propagar troyanos. Analistas recomiendan evitar descargar archivos sospechosos.				
Fecha:	25/01/26 (por la tarde)	Fuente:	RADIO FORMULA MORELOS	Por:	Gerardo Farell
Link:	https://elceo.com/tecnologia/troyanos-equipos-facturas-archivos/				

Puntos Clave:

- Frecuencia alarmante: En México se registran cerca de cuatro ciberataques por segundo, según el Plan Nacional de Ciberseguridad.

- Archivos cotidianos como señuelo: Facturas, reportes fiscales y documentos laborales son usados para infiltrar malware sin levantar sospechas.

- Tipos de archivos más explotados:

- Ejecutables (.exe, .msi, .scr): ejecutan código malicioso a distancia.
- Office (.docx, .xlsm, .pptm): piden habilitar macros y descargan troyanos.
- PDF maliciosos: contienen procesos ocultos que redirigen a descargas dañinas.
- Comprimidos y scripts (.zip, .rar, .iso, .js, .vbs, .lnk): disfrazan malware con nombres engañosos como factura.pdf.exe.

- Consecuencias graves: robo de contraseñas y datos bancarios, acceso remoto para espionaje, manipulación del sistema, instalación de más amenazas y pérdida de archivos.

Contexto adicional:

- Los ataques suelen intensificarse en enero, con archivos disfrazados de actualizaciones, reportes de fin de año o facturas.
- La ingeniería social es clave: los delincuentes aprovechan la urgencia y confianza en documentos comunes para inducir al usuario a abrirlos.

Conclusión:

La tendencia muestra que la ciberseguridad en México enfrenta un reto crítico: los atacantes usan archivos comunes como vehículos de infección, lo que exige mayor conciencia, capacitación y protocolos de protección tanto en usuarios como en organizaciones.

Notas de TI					
Título:	Fortalece DGETI Tlaxcala su oferta educativa con nuevas carreras tecnológicas				
Encabezado:	Fueron cinco los nuevos planes de estudio presentados, pero ya desde el semestre pasado son impartidos en algunos planteles				
Fecha:	26/01/26	Fuente:	EL SOL DE TLAXCALA	Por:	Jesús Lima
Link:	https://oem.com.mx/elsoldetlaxcala/local/fortalece-dgeti-tlaxcala-su-oferta-educativa-con-nuevas-carreras-tecnologicas-27930324				

Puntos Clave:

- Nuevas carreras técnicas: Se incorporaron opciones del catálogo nacional como inteligencia artificial, ciberseguridad, comercio electrónico, urbanismo y desarrollo sostenible, e inteligencia de negocios.

- Distribución por planteles:

- Huamantla y Calpulalpan: Ciberseguridad.
- San Pablo del Monte: Inteligencia artificial, comercio electrónico y urbanismo/desarrollo sostenible.
- Tetla: Inteligencia artificial.

- Xiloxoxtla y Santa Cruz Guadalupe (Chiautempan): Ciberseguridad e inteligencia de negocios.
- Cobertura estatal: La DGETI cuenta con ocho planteles de nivel medio superior (7 CBTis y 1 CETis en Chiautempan).
- Oferta total: 24 carreras técnicas en áreas industrial, tecnológica, comercial, de servicios y salud, con formación dual y en ambos turnos.
- Carrera única: Enfermería en el CBTis 303 (Xiloxoxtla), la única opción en Tlaxcala a nivel medio superior.
- Sistema Dual: 95 estudiantes combinan estudio y práctica en empresas.
- Inclusión: Los CAED atienden a 135 alumnos con discapacidad en Tlaxcala, Huamantla y Tetla.

Conclusión:

La DGETI en Tlaxcala fortalece su oferta educativa con carreras alineadas a tendencias tecnológicas y de innovación, mientras mantiene programas de inclusión y formación dual que vinculan a los estudiantes con el sector productivo.

Notas de TI					
Título:	Ciberseguridad, el reto pendiente para consolidar la confianza de pagos y finanzas digitales				
Encabezado:					
Fecha:	25/01/26 (por la tarde)	Fuente:	PLANO INFORMATIVO	Por:	
Link:	https://planoinformativo.com/1123391/ciberseguridad-el-reto-pendiente-para-consolidar-la-confianza-de-pagos-y-finanzas-digitales/				

Puntos Clave:

- Confianza digital en México:
 - 8 de cada 10 mexicanos dicen sentirse capaces de protegerse en línea.
 - Sin embargo, fraude y estafas siguen siendo el principal obstáculo.
 - 36% de los consumidores identifica estos riesgos como su mayor frustración en transacciones digitales.
- Madurez digital y vulnerabilidad:
 - México avanza en pagos electrónicos, banca en línea y comercio digital.
 - 80% de los usuarios recibió al menos un intento de estafa en el último año.
 - Solo 17% fue víctima directa, pero el impacto emocional es significativo.
- Confianza en actores clave:
 - Instituciones financieras: 76% de confianza.
 - Redes de pago globales (ej. Mastercard): 66%.
 - La confianza es vista como motor estratégico para el crecimiento económico.

- Estafas más comunes:

- Phishing y llamadas fraudulentas, con mayor incidencia en adultos mayores (28% vs. 17% en jóvenes).
- Nueva amenaza: uso de IA para generar contenido falso, que solo 15% de los encuestados cree poder identificar con certeza.

- Impacto en PYMES:

- 78% de los consumidores, tras sufrir fraude, prefieren comprar en comercios grandes o conocidos.
- Esto aumenta el riesgo de exclusión digital para negocios pequeños sin soluciones de seguridad avanzadas.

Conclusión:

La ciberseguridad se consolida como habilitador del crecimiento económico en México. El reto es mantener el ritmo de innovación sin erosionar la confianza de los usuarios, en un entorno donde las expectativas de seguridad son cada vez más altas y las amenazas más sofisticadas.

Notas de TI					
Título:	La IA está reforzando la ciberseguridad contra las crecientes ciberamenazas				
Encabezado:					
Fecha:	26/01/26	Fuente:	TYN	Por:	Julio César Castrejón
Link:	https://tynmagazine.com/la-ia-esta-reforzando-la-ciberseguridad-contra-las-crecientes-ciberamenazas/				

- IA como doble filo: La inteligencia artificial potencia tanto la productividad como los riesgos de seguridad.

- Amenazas externas: Ciberdelincuentes usan IA para perfeccionar phishing y ingeniería social, creando mensajes convincentes y difíciles de detectar.

- Defensa con IA: Las organizaciones líderes ya integran IA en sus sistemas de seguridad para detectar amenazas en tiempo real.

- Riesgos internos:

- IA en la sombra: Empleados usan herramientas no autorizadas, exponiendo datos y ampliando superficies de ataque.
- Deepfakes y ataques a aplicaciones de IA: 62% de las organizaciones sufrió ataques con deepfakes; 32% reportó explotación de aplicaciones.

- Preparación insuficiente: Solo 1 de cada 10 empresas está lista para enfrentar ciberamenazas potenciadas por IA; 63% carece de estrategia cohesionada.

- Gobernanza necesaria: La IA debe tratarse como capa fundamental de la arquitectura empresarial, con reglas claras de acceso a datos e infraestructura.

Conclusión:



La seguridad empresarial entra en una nueva era: combatir la IA con IA. Las organizaciones que integren la inteligencia artificial como capacidad de seguridad —no solo como herramienta de productividad— estarán mejor posicionadas para anticipar, identificar y neutralizar amenazas en un entorno digital cada vez más sofisticado.