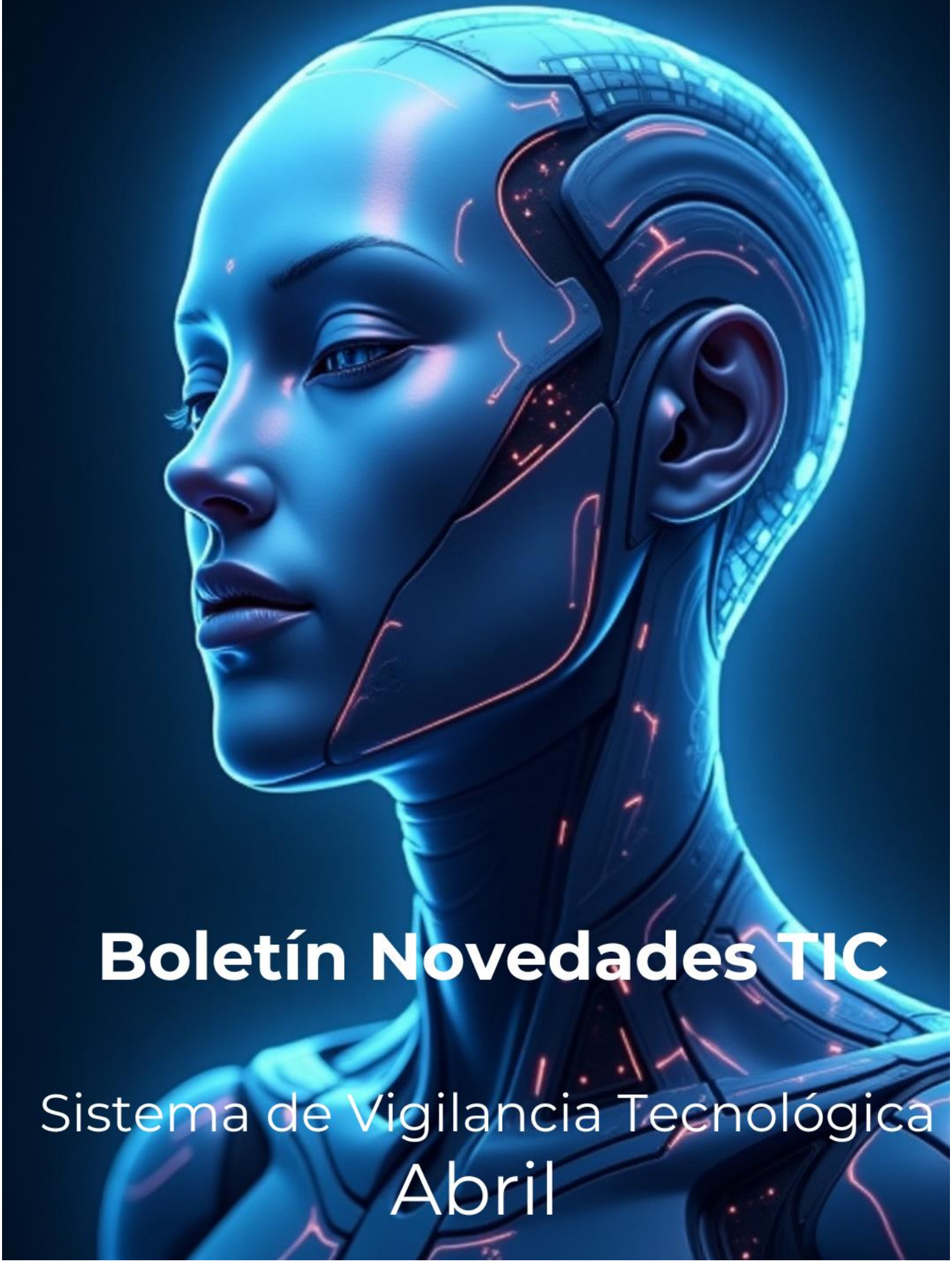
Ministerio de Comunicaciones



Boletín Novedades TIC

Sistema de Vigilancia Tecnológica

Abril

TENDENCIAS

1. CHINA QUIERE GANAR LA CARRERA DE LA IA REGALANDO LOS SERVICIOS QUE OTROS COBRAN

Fecha: 30/04/2025

China ha empezado 2025 liberando modelos como Qwen 3 y DeepSeek R1, socavando las suscripciones occidentales y empujando la IA hacia la commodity.

Alibaba acaba de lanzar Qwen 3, su familia de modelos de IA con capacidades de razonamiento "híbrido", apenas tres meses después de que DeepSeek sacudiera la industria con R1. No es una coincidencia: ambas empresas chinas han adoptado una estrategia diametralmente opuesta a la de Estados Unidos.

Mientras OpenAI reserva las mejores funciones y amplía límites a quien paga al menos 20 dólares al mes (con más permisividad si son 200), y Google reserva sus funciones avanzadas a los suscriptores, los gigantes chinos publican modelos de código abierto con licencias casi sin restricciones, gratis para uso personal o comercial. No es altruismo, sino un ataque directo al modelo de negocio occidental, basado en que el mero acceso a un gran modelo justifica el pago.

Qwen 3 llega en ocho variantes: desde versiones ligeras de 600 M de parámetros que caben en un móvil hasta un titán de 235 B que rivaliza con o3 y Gemini 2.5 Pro. Todas permiten alternar entre respuestas rápidas y razonamiento paso a paso —el rasgo que OpenAI vende como diferencial—, pero sin peajes.

Estamos ante el “momento Linux” de la IA. China no quiere levantar jardines vallados, sino dinamitar la lógica comercial que sostiene a las grandes tecnológicas estadounidenses.

Cada lanzamiento abierto que roza el nivel de los sistemas propietarios erosiona su valor percibido. ¿Por qué pagar 20 dólares al mes por ChatGPT si puedes montar gratis Qwen 3 con un rendimiento similar? La presión sobre OpenAI, Google o Anthropic crece con cada iteración asiática.

Marc Benioff lo resumió tras el terremoto de DeepSeek: "Los modelos y la interfaz ya son commodities; el valor está en los datos". China lo ha interiorizado antes que Silicon Valley.

La jugada supone ventajas claras:

- Sortea en parte las restricciones de chips al exprimir la eficiencia.
- Moviliza a una comunidad global que mejora y despliega su tecnología.
- Fija estándares de facto que, con el tiempo, encauzarán todo el ecosistema.

La tesis es clara: los modelos básicos serán una utilidad más. El negocio estará en las aplicaciones y en los datos que las nutran. No es casual que Alibaba alardee de que Qwen ya acumula más de 100 000 derivados, por encima de los basados en Llama.

Silicon Valley se enfrenta a una disyuntiva: persistir y arriesgarse a la irrelevancia o abrirse y sacrificar ingresos a corto plazo. La paradoja también es clara: el libre

mercado occidental está siendo retado por firmas chinas bajo la bandera del open source.

Mientras Musk acelera con Grok 3.5 y OpenAI sigue mostrando el camino a pasar por caja mes a mes, China avanza sin freno: más potencia por menos coste hasta que pagar por IA resulte tan absurdo como pagar por un sistema operativo.

Disponible en:
https://www.xataka.com/robotica-e-ia/china-quiere-ganar-carrera-ia-regalando-servicios-que-otros-cobran

2. ADIÓS A LAS CAPTURAS DE PANTALLA EN WHATSAPP: LA APLICACIÓN MANDARÁ NOTIFICACIONES A QUIENES LES HAGAN PANTALLAZOS

Fecha: 30/04/2025

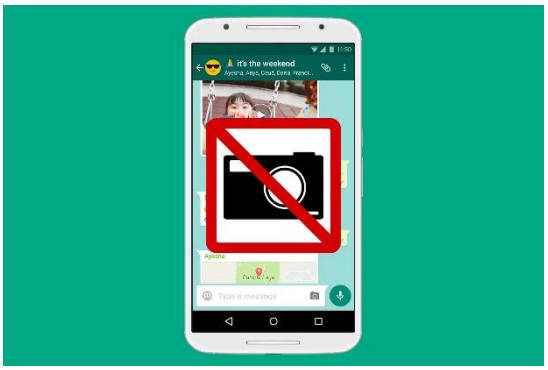
WhatsApp odia a los chismosos.

Las capturas de pantalla parecen tener los días contados en WhatsApp. El servicio de mensajería de Meta está trabajando en una actualización, que entre otras cosas destaca por enviar notificaciones que avisen cuando otro usuario les hizo un pantallazo.

Afortunadamente, para los chismosos, las notificaciones de capturas de pantalla serían sólo para los estados de WhatsApp, emulando la función que desde hace muchos años tiene activa Snapchat.

El adelanto de esta nueva función lo dio a conocer la gente de Android Authority, especialistas en todo lo que tiene que ver con el servicio de mensajería de Meta. En una reseña informaron que las notificaciones a las capturas de pantalla aparecen en WhatsApp para Android (versión 2.25.12.19), que se encuentra en modo Beta para desarrolladores.

“No hemos visto indicios de que WhatsApp vaya a avisar a los usuarios cuando alguien haga una captura de pantalla de su estado. Esperamos que esto se deba simplemente a que la función aún se encuentra en las primeras etapas de desarrollo”, informaron en el sitio antes mencionado.



De implementarse, esta función se añadiría a las modificaciones que ha hecho WhatsApp en materia de seguridad para sus usuarios.

Desde el año pasado prohibió que se guardara, o se capture, la foto de perfil de los usuarios, y si añaden estas actualizaciones a los estados, estaríamos en presencia de un servicio de mensajería mucho más seguro.

Disponible en:
https://www.fayerwayer.com/moviles/2025/04/17/adios-a-las-capturas-de-pantalla-en-whatsapp-la-aplicacion-mandara-notificaciones-a-quienes-les-hagan-pantallazos/

3. LOS AUDITORES EUROPEOS REBAJAN LAS PRETENSIONES DE FABRICACIÓN DE LA LEY DE CHIPS

Fecha: 29/04/2025

El Viejo Continente solo alcanzaría una cuota de mercado del 11,7% mientras que el objetivo se cifraba en el 20% para 2030.

Europa no alcanzará el objetivo de lograr una cuota del 20% del mercado mundial de microchips para 2030, tal y como postulaba la Ley de Chips de 2023. Así lo afirma un estudio de la Corte Europea de Auditores, que rebaja estas pretensiones y cifra en un 11,7% el máximo alcanzable debido a la limitación de recursos y a la intensa

competencia mundial, copada principalmente por Estados Unidos y China.

De este modo, los 86.000 millones de euros de inversión destinados se antojan "insuficientes" en comparación con la cuantía a nivel global, que entre los años 2020 y 2023 ascendió a 405.000 millones.

De hecho, el Parlamento Europeo (PE), calificando el reglamento de "demasiado lento", instaba hace escasas semanas a la Comisión Europea (CE) a lanzar un programa de apoyo a la industria orientado a la inversión en inteligencia artificial (IA) y a hacer del Viejo Continente un enclave "atractivo como polo de I+D, producción e inversión".

"En el momento de su fijación, el objetivo [lograr esa cuota del 20%] era demasiado ambicioso", ha señalado Annemie Tutelboom, miembro del Tribunal de Cuentas Europeo, encargada de la auditoría, durante una rueda de prensa. "Ser ambicioso es algo bueno. Sin embargo, en este campo no estamos ni cerca.

Se fijan planes y se alcanzan porque se quiere demostrar que la UE es un actor serio en este campo, capaz de contar con estrategias serias. Este tipo de fiabilidad y previsibilidad es importante para todos los actores, especialmente en microchips, un campo que requiere un volumen tan grande de inversión".

De este retroceso, el estudio arraiga otras problemáticas como el hecho, tal y como se citó en la conferencia de prensa, de que Europa no compite de forma aislada y de que sus rivales, potencialmente del Sudeste Asiático y de Estados Unidos, se encuentran en una posición de "fuerza" con estrategias "avanzadas".

De hecho, Tutelboom indicaba que "ponerse al día con el presente no es suficiente. Hay que ser capaces de satisfacer la demanda en un período de 10 años".

En tercer lugar, la directiva también hablaba de las competencias fragmentadas del Viejo Continente. "Ante este escenario nos encontramos ante varias preocupaciones que son necesarias abordar para sacar el máximo partido de la política". Por ejemplo, citaba, la gran mayoría de las inversiones se concentra en un pequeño número de Estados miembro.

Además, "seguimos siendo increíblemente vulnerables en cuanto se refiere al acceso de materias primas necesarias y tenemos uno de los precios de la energía más altos del mundo". En este sentido, "los aranceles globales y las prohibiciones a la exportación crean el potencial de colapso de las cadenas de suministro".

Por último, el documento pone sobre la mesa cuestiones en torno a cómo se canaliza el dinero hacia los proyectos. "La producción de microchips comparte retos similares con otras formas de política industrial de la UE, por lo que hay riesgos específicos en la forma de aplicar la financiación".

Disponible en:
https://www.computerworld.es/article/3973671/los-auditores-europeos-rebajan-las-pretensiones-de-fabricacion-de-la-ley-de-chips.html

4. HP ASEGURA QUE, EN 2026, EL 50 % DEL MERCADO SERÁN PCS CON IA INTEGRADA

Fecha: 29/04/2025

La compañía anuncia la paulatina integración de la inteligencia artificial en todos sus portátiles que ofrecerán así más velocidad, seguridad y privacidad.

La inteligencia artificial está transformándolo todo, de eso no hay duda, con la IA generativa como claro exponente. Trabajar, aprender, crear o incluso relacionarnos… Todo hoy es distinto con la IA. Pero precisamente esa expansión sin precedentes de esta tecnología está suponiendo también un claro desafío.

Prácticamente todos los actuales modelos de inteligencia artificial se consumen vía la nube y eso implica latencias más altas de lo deseable, un gran consumo energético o una privacidad y seguridad menor de lo necesario.

Para solventar todos estos obstáculos, pero sobre todo para ofrecer experiencias de trabajo más fluidas, seguras y personalizadas para profesionales de todos los sectores, HP acaba de presentar su propuesta de PCs con inteligencia artificial integrada, es decir con NPU de entre 40 y 50 tops de rendimiento.

Un mercado que, en España, según datos de Pablo Ugarte, director general de sistemas personales de HP Iberia, supondrá en 2025 al menos un 6% del total de equipos comercializados y en 2026, el año en el que esperan realmente brote este sector, estos ya representarán alrededor de la mitad de sistemas personales vendidos, sobre todo gracias a que “los precios de estos equipos, que actualmente se sitúan en torno a los 1.000 euros, irán descendiendo progresivamente”.

Más velocidad y seguridad

Entre las bondades de estos AI PCs “una mayor velocidad de respuesta y menor latencia en el trabajo con los modelos de IA que en caso de consultas a soluciones alojadas en la nube pública”, apuntaba Ugarte que añadía además que ayudan a conseguir un menor gasto energético de los centros de datos y una mayor privacidad y seguridad.

“Ya que las empresas y los empleados tienen un mayor control sobre la información que intercambian con la IA si lo hacen en local y desde un PC, pues operan en entornos más protegidos que los que usan los grandes modelos, como ChatGPT”.

Es el llamado Edge AI o la inteligencia artificial en el extremo, según explicaba Melchor Sanz, CTO de ventas de HP Iberia. “Estamos ante una nueva era en el puesto de trabajo. La computación en la nube para la IA es limitada, costosa y en muchas ocasiones poco sostenible; al situar la IA en el edge puedes distribuir computación entre los ordenadores personales y otros dispositivos, pues HP, por ejemplo, está llevando capacidades de IA a impresoras o equipos de red y colaboración”, afirmaba.

Y para muestra la de la propia HP que para posicionarse en el mercado de los AI PCs ha incorporado en algunos de sus equipos opciones de NPU, como los de la serie HP EliteBook 8, diseñados para empresas, la serie HP EliteDesk 8, que lleva las posibilidades de la inteligencia artificial al

ámbito de los ordenadores de sobremesa o la estación de trabajo HP ZBook Ultra G1a, con procesador AMD Ryzen y hasta 16 núcleos.

Además, HP complementa sus PC optimizados para la inteligencia artificial con la herramienta AI Companion "que personaliza la configuración de la máquina en función de las necesidades del usuario. Va aprendiendo del usuario y es capaz de resumir documentos complejos en segundos, ofrecer respuestas instantáneas, incluso sin conexión a internet. Es un asistente inteligente", señalaba Marta Fuentes, responsable de Equipos de sobremesa profesional y Monitores de HP Iberia.

"La IA es una herramienta que está transformando la manera en la que trabajamos, colaboramos o tomamos decisiones y HP quiere que sus usuarios puedan disfrutar de todo ese valor", concluía.

Disponible en:
https://www.silicon.es/hp-2026-el-50-del-mercado-seran-pcs-con-ia-2567113

5. ¿PODRÍA EL APAGÓN EN ESPAÑA Y PORTUGAL HABER SIDO UN CIBERATAQUE?

Fecha: 29/04/2025

"Ciberataque" fue la palabra que muchos tenían en mente cuando recientemente grandes zonas de España y Portugal quedaron sumidas en un apagón.

Las autoridades están investigando la causa raíz, y los primeros informes apuntan a un fallo técnico provocado por un "fenómeno atmosférico poco común". Sin embargo, ha habido especulaciones —aún no descartadas— de que un ciberataque podría estar detrás del incidente.

El apagón generalizado interrumpió el transporte, las comunicaciones y la vida cotidiana en toda la península ibérica. Todo comenzó con la desconexión de una línea eléctrica internacional clave, lo que provocó interrupciones en cascada en las redes regionales. El corte de electricidad, que en algunas zonas se prolongó durante varias horas, fue provocado por una avería en la red de transmisión de alta tensión operada por Red Eléctrica de España (REE).

Pero, ¿por qué tantos llegaron de inmediato a la conclusión de que se trataba de un ciberataque? La sospecha de una actividad maliciosa pone de manifiesto hasta qué punto existe una creciente preocupación a nivel global por los ciberataques y los impactos devastadores que podrían tener.

¿Por qué se sospechó inicialmente de un ciberataque?

Las primeras noticias sobre el apagón recordaron el ataque de ransomware a Colonial Pipeline en 2021, en la costa este de Estados Unidos. Sin embargo, tanto Red Eléctrica de España (REE) como Redes Energéticas Nacionales (REN) de Portugal descartaron una intrusión maliciosa tras revisar los registros SCADA, la telemetría y los datos de los cortafuegos. A pesar de ello, en los momentos posteriores al incidente, varios indicios llevaron a las autoridades y a los observadores a considerar la posibilidad de un ciberataque:

- **Fallos simultáneos en múltiples puntos:** La naturaleza repentina y coordinada de los cortes en subestaciones geográficamente

dispersas imitaba características de eventos en la red eléctrica inducidos por ciberataques, como los ocurridos en Ucrania en 2015 y 2016.

- **Interrupciones en las comunicaciones:** El colapso temporal de los servicios móviles e internet alimentó la especulación pública sobre un posible ataque sistémico, especialmente al fallar los sistemas de respaldo en algunas zonas.
- **Contexto geopolítico y momento del incidente:** El apagón tuvo lugar en un periodo de alta alerta cibernética en toda Europa, en medio de una creciente inestabilidad geopolítica, lo que incrementó la vigilancia y la sensibilidad ante posibles amenazas.
- **Retraso en los análisis forenses digitales:** La falta de claridad inmediata por parte de los operadores de red permitió que la especulación llenara el vacío informativo antes de que Red Eléctrica de España (REE) y la ENTSO-E (Red Europea de Gestores de Redes de Transporte de Electricidad) completaran sus diagnósticos iniciales.

A día de hoy, un ciberataque no ha sido completamente descartado por todas las partes, ya que el Instituto Nacional de Ciberseguridad (INCIBE) de España sigue investigando las causas.

¿Por qué querrían los hackers atacar la red eléctrica de un país?

Los actores estatales suelen explorar o atacar redes eléctricas para obtener ventaja en conflictos más amplios. Deshabilitar la generación o transmisión de energía puede minar la moral de la población civil, interrumpir la logística militar y enviar un mensaje coercitivo sin recurrir al enfrentamiento directo. En el contexto ruso-ucraniano, los ataques de 2015–2016 contra la red eléctrica de Ucrania por parte del grupo Sandworm demostraron cómo los apagones precisos —provocados mediante malware como BlackEnergy— pueden utilizarse como herramienta de presión geopolítica.

Por su parte, los ciberdelincuentes motivados por razones económicas ven en las compañías energéticas —que suelen ser grandes, altamente automatizadas y dependientes de controles digitales— objetivos rentables para ataques de ransomware. Cifrar respaldos de sistemas SCADA o estaciones de trabajo de los operadores puede paralizar rápidamente las operaciones, presionando a las víctimas a pagar rescates para restablecer el servicio. Grupos como BlackCat/ALPHV y LockBit 3.0 han intensificado sus ataques contra empresas del sector energético e infraestructuras críticas.

Más allá de las interrupciones inmediatas, los adversarios también pueden utilizar intrusiones en la red para mapear arquitecturas de control, extraer datos de procesos confidenciales y desarrollar malware personalizado. En los últimos años, el grupo chino RedEcho ha sido acusado de infiltrarse en las redes eléctricas de la India.

¿Cuáles son los indicios de un ciberataque a una red eléctrica?

Los operadores de red y los equipos de seguridad buscan una serie de anomalías tanto en los entornos de TI (redes

administrativas) como en los de TO (tecnología operativa/SCADA) al evaluar una posible intrusión. Los indicadores de advertencia más comunes incluyen:

Reconocimiento de red no explicado

- Exploración repentina de puertos o sondeo de protocolos ICS/SCADA (por ejemplo, IEC 60870-5-104, DNP3) desde direcciones IP externas o segmentos internos inusuales.
- Despliegue temprano de malware en activos no críticos como “prueba” para validar el acceso antes de un ataque completo.

Acceso no autorizado y abuso de credenciales

- Intentos de acceso fallidos o inusuales repetidos a unidades terminales remotas (RTU) o interfaces hombre-máquina (HMI) fuera de las ventanas normales de mantenimiento.
- Uso de cuentas de servicio o credenciales que nunca habían accedido a los sistemas de control de red.

Secuencias de comandos ICS anómalas

- Envío remoto de comandos de apertura o anulación a interruptores o relés de protección sin una alarma o señal de sensor válida que lo justifique.
- Activación repetida de interruptores o reconectadores en patrones que no coinciden con las acciones del operador de red.

Discrepancias en la integridad de los datos

- Incongruencias entre las mediciones en tiempo real de sensores y los registros SCADA (por ejemplo, valores constantes nominales de frecuencia o voltaje pese a fluctuaciones físicas evidentes).
- Desajustes en GPS o marcas de tiempo que sugieren manipulación de registros o “desfase temporal” de eventos.

Artefactos de malware y cambios en el sistema de archivos

- Detección de frameworks de malware específicos para ICS (como Industroyer/CrashOverride) o puertas traseras relacionadas en equipos del sistema de control.
- Aparición de nuevos ejecutables, imágenes de firmware alteradas o servicios inesperados ejecutándose en PLCs/RTUs.

Interrupción de la supervisión y alertas

- Pérdida o corrupción de registros de eventos en entornos tanto de TI como de TO (por ejemplo, archivos de logs ausentes o rastros de auditoría sobrescritos).
- Fallo de canales de comunicación redundantes (como enlaces satelitales o fuera de banda) que coincide de forma sospechosa con la caída del enlace principal.

Anomalías coordinadas y de múltiples vectores

- Interrupciones simultáneas en el suministro eléctrico y en las TIC (redes de telecomunicaciones, servidores NMS) que superan lo que podría explicar una sola falla física.
- Evidencia de una “cadena de ataque” que avanza desde una intrusión en TI (por ejemplo, phishing, infección de estaciones de trabajo) hacia el dominio de TO.

¿Podrían las contraseñas débiles desempeñar un papel en los ataques a redes eléctricas?

Las contraseñas débiles o por defecto son uno de los puntos de entrada más simples y comunes que un atacante puede aprovechar para infiltrarse tanto en los entornos de TI como en los de TO (SCADA/ICS) de un operador de red eléctrica. A continuación, se explica cómo podrían influir en una posible vulneración de la red:

Brecha inicial mediante acceso remoto

- Muchas empresas del sector eléctrico exponen VPNs, portales RDP o paneles de gestión web para labores de monitoreo y mantenimiento remoto. Si estos están protegidos con credenciales débiles, predecibles o por defecto (sin cambios), un atacante puede acceder fácilmente mediante fuerza bruta o reutilización de credenciales filtradas. El riesgo se multiplica si no se aplica una autenticación multifactor (MFA) efectiva

Movimiento lateral

- Una vez dentro de la red corporativa (LAN), los atacantes buscan cuentas de “puente” que les permitan avanzar hacia la zona operativa. Si las cuentas de servicio o los accesos administrativos a HMI/PLC siguen protegidos por contraseñas débiles, el compromiso puede propagarse rápidamente dentro del entorno OT.3. Reutilización de credenciales
- Incluso si la red eléctrica está bien segmentada, los usuarios suelen reutilizar contraseñas entre los entornos de oficina y los sistemas de control. Ataques de phishing o registros de teclas en el buzón corporativo de un ingeniero pueden permitir a los atacantes obtener credenciales válidas que también funcionen en las puertas de enlace OT. En el apagón de Ucrania en 2015, los atacantes primero recolectaron credenciales legítimas antes de emitir comandos destructivos a los interruptores.
- 

¿Ciberataque o advertencia preventiva?

En última instancia, el apagón en la península ibérica sirvió como un recordatorio contundente de los riesgos potenciales que enfrentan las infraestructuras críticas ante posibles ciberataques. En medio de un colapso repentino de la red, fue demasiado fácil saltar a la hipótesis del ataque cibernético, alimentada por titulares recientes y la creciente ansiedad geopolítica. Incluso si la causa real resulta ser un fenómeno natural —como sugieren las evidencias actuales—, la amenaza tangible de una intrusión dirigida exige máxima vigilancia.

Los operadores deben tratar cada incidente como una oportunidad para reforzar sus defensas: desde la implementación estricta de políticas de contraseñas seguras y autenticación multifactor, hasta una segmentación de red rigurosa y una

monitorización continua de anomalías las 24 horas del día. Si algo ha dejado claro este episodio, es que la mejor respuesta frente a fallos técnicos o ataques maliciosos no es el pánico, sino la preparación.

Disponible en:
https://www.silicon.es/brandvoice/podria-el-apagon-en-espana-y-portugal-haber-sido-un-ciberataque

6. MEGATENDENCIAS DE CIBERSEGURIDAD: ANÁLISIS Y ESTRATEGIAS ANTE LA EXPANSIÓN DE LA SUPERFICIE DE ATAQUE

Fecha: 28/04/2025

Las megatendencias de ciberseguridad para 2025 revelan un panorama desafiante, impulsado por el uso de la IA, la expansión de la superficie de ataque y la creciente sofisticación de los ciberataques. Organizaciones de todos los sectores deberán adoptar estrategias de Zero Trust, fortalecer la capacitación interna y actualizar sus soluciones.

Cada año, los principales analistas y expertos de la industria identifican las “megatendencias” de tecnología que definirán el curso de la Transformación Digital de las empresas, y en ellas la ciberseguridad es principal.

Las tendencias en ciberseguridad para 2025 apuntan a un panorama complejo y desafiante, marcado por la omnipresencia de la Inteligencia Artificial (IA) tanto en la creación como en la defensa contra malware, la creciente importancia de asegurar la cadena de suministro, la sofisticación de los ataques multivectoriales y la evolución del phishing gracias a la GenAI.

Esto implica que las organizaciones deberán priorizar la detección de amenazas impulsada por IA, la gestión de riesgos en todo su ecosistema, la integración de soluciones de seguridad para una respuesta coordinada y la capacitación continua de los usuarios, adoptando un enfoque de seguridad Zero Trust donde la desconfianza se convierte en una estrategia clave.

Esta información resulta esencial para que los líderes de TI y seguridad anticipen los desafíos y desarrollen estrategias de protección efectivas. Conocer, entender e implementar estrategias es fundamental para el negocio, en cualquiera que sea la industria.

Sin embargo, la cantidad de información llega a ser tan abrumadora, y combinada con la velocidad en la que se produce, a veces puede ser difícil apreciar por completo la importancia vital de la ciberseguridad dentro de un contexto de mercado más amplio, incluso para las personas que trabajan en la industria de TI, que además escasean.

En el mundo existe un déficit de personas expertas en seguridad informática estimado en 3.500.000 profesionales para 2025

Entendiendo este contexto, Kaspersky, empresa global de ciberseguridad y privacidad digital, comparte las tendencias de seguridad más desafiantes que impactan actualmente en la industria IT.

La Megatendencia de la expansión de la Superficie de Ataque

El informe destaca la expansión de la superficie de ataque como una megatendencia crítica en ciberseguridad. Este fenómeno implica el incremento en los

puntos de entrada que los ciberdelincuentes pueden explotar, lo cual intensifica la complejidad de la protección de activos digitales.

Según la Security Industry Association (SIA), la ciberseguridad se posiciona como una preocupación primordial en la industria de la seguridad.

De hecho, un estudio de la SIA revela que la ciberseguridad supera a la Inteligencia Artificial (IA) en la mente de los líderes de la industria de la seguridad como la tendencia de mayor impacto.

Tendencias específicas de TI y su impacto en la Ciberseguridad

Analistas de Gartner, IDC y Frost & Sullivan han identificado tendencias específicas que están transformando el panorama de la ciberseguridad:

- Transformación digital y trabajo híbrido: La adopción generalizada del trabajo remoto y los entornos de nube ha difuminado el perímetro de la red tradicional, lo que ha creado nuevas vulnerabilidades.
- Sofisticación de los ciberataques: Los ataques son cada vez más sofisticados, selectivos y difíciles de detectar, lo que exige soluciones de seguridad más avanzadas.
- Escasez de profesionales de ciberseguridad: La carencia de personal calificado representa un desafío adicional para las organizaciones que buscan proteger sus activos digitales.

Ante estas tendencias, se recomienda que los líderes de seguridad y gestión de riesgos (SRM) se enfoquen en:

- El factor humano: Fortalecer la capacitación y concientización de los empleados.
- Tecnologías de seguridad: Implementar soluciones que ofrezcan visibilidad y capacidad de respuesta integral.
- Enfoque proactivo: Adoptar una postura proactiva ante las amenazas y consolidar las herramientas de seguridad.

El informe de Kaspersky, que cuenta con un extenso portafolio de productos de seguridad para proteger a empresas, también subraya la rápida evolución del panorama de amenazas. Los ciberataques son cada vez más frecuentes, sofisticados y dirigidos, y son perpetrados por delincuentes profesionales organizados.

- El 51 % de las empresas tiene dificultades para detectar e investigar amenazas avanzadas con sus herramientas actuales.

La protección de la infraestructura organizacional en el entorno actual exige una estrategia de ciberseguridad robusta y adaptable. Si le preocupa la creciente sofisticación de las ciberamenazas profundice cómo las soluciones de ciberseguridad de última generación pueden fortalecer la protección de su organización.

Disponible en:
https://impactotic.co/ciber-seguridad/megatendencias-de-ciberseguridad-claves-y-estrategias/

7. LA PRIVACIDAD DE WHATSAPP PARECÍA A PRUEBA DE BOMBAS. HASTA QUE UN FISCAL DEL ESTADO INTENTÓ BORRAR MENSAJES INCRIMINATORIOS

Fecha: 24/04/2025

La privacidad de nuestras conversaciones en WhatsApp parecía garantizada por el cifrado de extremo a extremo, pero hay formas de acceder a ellas a pesar de todo

Las copias de seguridad de WhatsApp no están cifradas por defecto: es probable que esa haya sido la clave para recuperar las conversaciones borradas del fiscal general

El fiscal general del Estado, Álvaro García Ortiz, creyó haber eliminado mensajes que podrían ayudar a incriminarle en un delito de revelación de secretos. En realidad, no fue así, porque da igual que borres tus mensajes en WhatsApp: Google los guarda igual. Ahora el Tribunal Supremo ha recibido documentación de Google/Meta que ayudará en el proceso.

El auto es de momento secreto y no sabemos exactamente qué información han remitido estas compañías, pero podemos elaborar varias hipótesis para contestar a dos preguntas. La primera, ¿se ha logrado acceso a los mensajes borrados? Y la segunda ¿cómo se han logado leer dichos mensajes?

Qué ha pasado. El fiscal general del Estado, Álvaro García Ortiz, fue imputado en octubre de un delito de revelación de secretos, como indicaron entonces en El Confidencial. La imputación está referida a la supuesta filtración a la prensa de los correos de la pareja de Isabel Díaz Ayuso o de haber dado órdenes a otros fiscales para que lo hicieran. El mismo diario informó en febrero de que el mismo día en el que se abrió la causa, García Ortiz borró los mensajes de WhatsApp de su móvil, lo restauró y cambió de dispositivo.

Petición a Google y Meta. El Tribunal Supremo, indicaban en El País en enero, lleva tiempo intentando recopilar información sobre el caso. Se realizó una petición a las delegaciones irlandesas de Google y WhatsApp (Meta) a través de Eurojust, una agencia para la cooperación judicial en casos criminales. La petición realizada intentaba recuperar "la información vinculada a aplicaciones de mensajería instantánea instaladas en dos dispositivos móviles de Álvaro García Ortiz, así como en una cuenta de correo electrónico". Según El Mundo, esa petición acabó siendo reenviada a Estados Unidos después de que Irlanda le indicase que la petición de información debía hacerse a este país.

Una carpeta ZIP. Según El Confidencial, el magistrado del Tribunal Supremo Ángel Luis Hurtado ha indicado que la recuperación de los datos parece haber sido exitosa. Google o Meta (no se especifica cuál) remitieron documentación en forma de una carpeta comprimida con formato ZIP. Estos nuevos datos, indica el magistrado en la resolución a la que ha tenido acceso El Confidencial, se analizarán pericialmente, y el resultado de esa investigación confirmará si la recuperación de los datos ha sido efectivamente "exitosa". es si han podido leer esos mensajes y cómo lo han conseguido. Hay varias hipótesis.

Hipótesis 1: metadatos. Durante la investigación, la UCO también registró los dispositivos electrónicos de la fiscal jefa provincial de Madrid, Pilar Rodríguez, señalan en 20Minutos. Rodríguez fue la persona con la que supuestamente mantuvo contacto García Ortiz en la imputación por el delito de revelación de secretos. Ella no borró sus mensajes ni restauró su móvil, así que la UCO sí pudo acceder a las conversaciones a través de su dispositivo, como señalan en El Confidencial. El contenido de la carpeta ZIP en poder del magistrado también podría haber sido remitido por Meta/WhatsApp, que no habría enviado los mensajes —no puede, teóricamente no tiene acceso a ellos—, pero sí los metadatos de esas conversaciones de García Ortiz. Dichos metadatos podrían servir para cotejar y contrastar los mensajes de Rodríguez, aportando así pruebas para la imputación del fiscal general.

Hipótesis 2: copias de seguridad sin cifrar. En WhatsApp los usuarios pueden hacer copias de seguridad de sus mensajes en servicios en la nube como los de Google Drive o Apple iCloud, pero atención: por defecto esas copias de seguridad no están cifradas. Son los usuarios los que deben proactivamente habilitar el cifrado en las copias de seguridad, y quizás García Ortiz no lo hizo. Eso hubiera provocado que Google, a la que se solicitó ayuda, pudiera acceder a esos datos para remitírselos al magistrado del caso.

Hipótesis 3: acceso físico al dispositivo. La forma más obvia de acceder a los mensajes de WhatsApp de un usuario es la de tener acceso físico a su dispositivo móvil. En ese caso expertos forenses pueden, con las herramientas oportunas, obtener la clave para descifrar los mensajes de la base de datos de WhatsApp, incluso si estos han sido borrados. Aquí García Ortiz borró los mensajes y restauró el terminal a su estado de fábrica, lo que probablemente hizo imposible recuperarlos desde el dispositivo aun teniendo acceso físicamente.

El cifrado de extremo a extremo está ahí. Hay que aclarar que WhatsApp lleva años haciendo uso de un protocolo de cifrado de extremo a extremo para todas las conversaciones. Solo quien envía el mensaje y quien (o quienes) lo reciben pueden leerlos, pero ninguna otra persona o entidad puede descifrar esos mensajes. Ni siquiera Meta, a través de cuyos servidores se envían y reenvían textos, imágenes, vídeo o cualquier otro tipo de contenido.

Si quieres borrar tus mensajes, cuidado con las copias de seguridad. Los usuarios de WhatsApp no pueden hacer nada con los metadatos, que sí guarda Meta, pero sí con los mensajes si quieren borrarlos de forma efectiva. Como nos enseña este caso, no basta con borrarlos de nuestro teléfono: si hacemos copias de seguridad de nuestros mensajes, es importante activar el cifrado de dichas copias de seguridad.

Pero aviso especial sobre las copias de seguridad. Cuidado especial con el cifrado de las copias de seguridad, porque no funciona como el cifrado extremo a extremo. Las copias se cifran con una clave/contraseña que solo conoces tú, y que por tanto conviene que sea fuerte para no poder ser rota con ataques de fuerza bruta, por ejemplo. WhatsApp de hecho da la opción de crear una clave de 64 dígitos, pero... lo hace ella.

Suspicacias. Aquí entra el debate sobre cómo gestionan esa contraseña de cifrado en Google/Apple/Meta, y si pueden descifrarla de algún modo para potenciales peticiones judiciales. Sea como fuere, la otra solución, por supuesto, es no hacer copias de seguridad de los mensajes a no ser que lo consideres absolutamente imprescindible. Todo este proceso levanta suspicacias sobre si la copia de seguridad es realmente vulnerable por parte de las propias Meta y Google/Apple.

Disponible en:
https://www.xataka.com/privacidad/privacidad-whatsapp-parecia-a-prueba-bombas-que-fiscal-estado-intento-borrar-mensajes-incriminatorios

8. SE FILTRA EL PLAN DE APPLE PARA "SURFEAR" LOS ARANCELES: 50 MILLONES DE IPHONE SERÁN FABRICADOS EN INDIA

Fecha: 17/04/2025

Apple quiere que el iPhone salga del medio del cruce entre los Estados Unidos y China.

iPhone es el producto que le da de comer a Apple. Si bien el gigante de Cupertino desarrolla otros dispositivos interesantes, ninguno se puede igualar con su familia de celulares. Es por eso que, la reciente guerra comercial entre China y los Estados Unidos tiene de cabeza, a la empresa de la manzana mordida.

Pocos quisieran estar en los zapatos de Tim Cook en este momento. Los aranceles que el gobierno norteamericano le puso a los productos provenientes de China (por ahora 145%) afectan profundamente a las ganancias que Apple obtiene, por concepto de la venta de los iPhone.

Pierden por todos lados: si asumen el costo de los aranceles van a caer sus ingresos y si elevan el precio de los celulares, van a disminuir las ventas. Es por eso que los equipos financieros de Apple han diseñado un plan estratégico para al menos sobrevivir al 2025, según filtraron varios medios especializados.

India se pone 'manos a la obra'

Apple tiene sus fábricas más importantes en China, como el caso de Foxconn. Pero también tiene galpones de producción en la India, Vietnam y Tailandia. Lo negativo es que estos tres países, ni siquiera juntos, son capaces de igualar la producción del gigante de Asia.

Entonces, según reporte de Applesfera, Tim Cook habría ayudado a las fábricas de India y a sus proveedores a comprar maquinaria que les sirva para incrementar la producción, y así intentar llegar a 50 millones de iPhones antes de que cierre el 2025.

Eso significa que India incrementaría en un 40% la producción. Para el lado de Vietnam y Tailandia también habrían realizado movimientos similares, pero las fuentes citadas por el medio antes mencionado no informa sobre cantidades, así como lo hizo con India.

Los informes reportan que no sólo fabricarán iPhones, también producirán Mac, iPad y AirPods.

¿Por qué Apple no fabrica sus iPhone en los Estados Unidos?

A pesar de todos estos problemas, Apple podría invertir en una fábrica en los Estados Unidos, con todo y las condiciones laborales que esto representa. También

podría mejorar las estructuras de India, Vietnam o algún otro país en donde estén operando, pero la realidad es que tienen un problema mayor de fondo: la calidad.

"Estados Unidos carece de personal cualificado" para los trabajos que se realizan en las fábricas que hay en China. Encontrar de nuevo la calidad y optimización en los procesos, es lo que hace que Apple se quiera aferrar al gigante de Asia.

Tim Cook, por consecuencia, busca llegar a una especie de acuerdo de excepción con Donald Trump. Algo que les permita quedar exentos de los aranceles, para sostener la estabilidad de la empresa y el precio de sus dispositivos.

Disponible en:
https://www.fayerwayer.com/moviles/2025/04/17/se-filtra-el-plan-de-apple-para-surfear-los-aranceles-50-millones-de-iphone-seran-fabricados-en-india/

ENRED@DOS

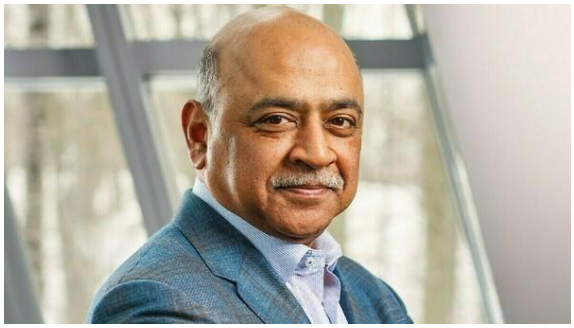
¡Bienvenidos a la sección Enred@dos! Un espacio para aprender y divertirte con las TICs en nuestros ratos de ocio.

ANÍMATE A PROBAR

1. FRASES INSPIRADORAS DE GENIOS DE LA TECNOLOGÍA

- "Eliminemos la fricción y los procesos físicos; es muchísimo lo que podemos lograr. Y, por cierto, se puede ganar dinero. Pero por eso digo que el propósito y la rentabilidad van de la mano"

-"La adopción de la nube híbrida y la inteligencia artificial son fundamentales para la transformación digital de las empresas y el avance tecnológico"



Arvind Krishna, Director Ejecutivo de IBM

2. CINEMANÍA

Nos complace proponer esta vez la telenovela brasileña Hombre Nuevo, una historia llena de giros y sorpresas que se desarrolla dentro de un contexto tecnológico. El genio de la computación Jonás Marra ganó fama y fortuna en Silicon Valley, en California, con su conglomerado tecnológico. Sin embargo, en la cumbre del éxito, un secreto lo pone ante conflictos que lo llevan a una nueva vida y un nuevo amor.

Tráiler Disponible en:
https://www.youtube.com/watch?v=bxZlPEVxUVs

3. MEME TECH

4. INFOGRAFÍA

Durante este mes fue tendencia en las redes sociales, la generación de imágenes con inteligencia artificial, simulando el contenido del famoso estudio de animación japonés Ghibi. Sin embargo, se dio a conocer que el uso desmedido de esta tecnología, tiene severas consecuencias ambientales.