

RSM Newsletter

Agosto 19 / 2025 – Distribución Gratuita

Nº 85

Los indios ahora tienen que pagar más por los planes ChatGPT Plus y Pro:

OpenAI decidió darle un giro a las cosas cobrando un 14% más por los planes ChatGPT Plus y Pro en India.

Microsoft Confirma Actualización de Emergencia de Windows para Usuarios de PC:

Microsoft ha lanzado una actualización de emergencia para abordar problemas críticos que afectan a los usuarios de Windows

Pixel 10, capacidades de IA y todo lo demás que esperamos del evento Made by Google 2025:

El Pixel 10 de Google viene con más trucos de IA que un truco mental Jedi.

Hackers explotan falla de Microsoft para violar la Cámara de los Comunes de Canadá:

Una vulnerabilidad en el software de Microsoft fue explotada por hackers para violar la Cámara de los Comunes en Canadá

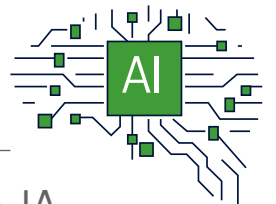
Informe del MIT: El 95% de los pilotos de IA generativa en empresas están fallando:

La iniciativa NANDA del MIT revela que la mayoría de los pilotos de IA generativa están fracasando más que un pez fuera del agua.

RSM



Resumen Semanal de IA



¡Hola a todos! Estoy aquí una vez más para traerles lo último en noticias de IA. Abróchense el cinturón, porque el resumen de esta semana está lleno de drama, intriga y un toque de magia tecnológica. ¡Vamos a sumergirnos de lleno!

Esta semana, tenemos una mezcla variada de noticias de IA, desde el informe del MIT sobre la baja tasa de éxito de los pilotos de IA generativa hasta el drama de precios de OpenAI en India. Mientras tanto, Google se está preparando para su gran evento, y Waymo está redoblando esfuerzos en seguridad con LiDAR y radar. Ah, ¿y mencioné que la app de ChatGPT está generando mucho dinero? ¡Vamos a desglosarlo!

Gigantes Tecnológicos Desatados

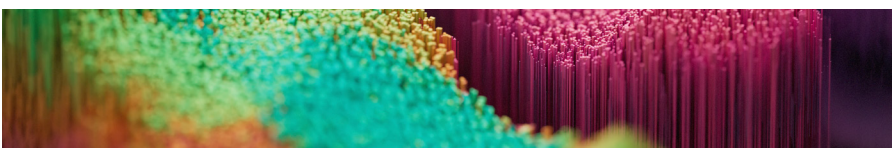
Los indios ahora tienen que pagar más por los planes ChatGPT Plus y Pro: OpenAI decidió darle un giro a las cosas cobrando un 14% más por los planes ChatGPT Plus y Pro en India. Supongo que pensaron, “¿Por qué no hacer llover Rupias?” [\[2\]](#)

Sam Altman dice que OpenAI ‘arruinó’ el lanzamiento de GPT-5: El lanzamiento de GPT-5 de OpenAI fue menos “Avengers: Endgame” y más “La Amenaza Fantasma”, dejando a los usuarios poco impresionados. [\[3\]](#)

Pixel 10, capacidades de IA y todo lo demás que esperamos del evento Made by Google 2025: El Pixel 10 de Google viene con más trucos de IA que un truco mental Jedi. ¡Cuidado, iPhone 17! [\[4\]](#)

Ejecutivo de ingeniería de Waymo dice que los sensores LiDAR y radar son clave para la seguridad en la tecnología de conducción autónoma: Srikanth Thirumalai de Waymo está totalmente a favor de la vida LiDAR, asegurando que sus robotaxis sean más seguros que el Batimóvil de Batman. [\[5\]](#)

Co-fundador de xAI de Elon Musk deja la empresa: Igor Babuschkin decidió salir por la



izquierda del escenario de xAI, dejándonos a todos preguntándonos si se unirá a los Vengadores. [6]

Los ingresos de la aplicación móvil de ChatGPT aumentan seis veces desde 2024: La aplicación móvil de ChatGPT está generando más dinero que Tony Stark, con un aumento de ingresos de seis veces. [7]

Ética de la IA

Informe del MIT: El 95% de los pilotos de IA generativa en empresas están fallando: La iniciativa NANDA del MIT revela que la mayoría de los pilotos de IA generativa están fracasando más que un pez fuera del agua. [1]

Las grandes tecnológicas expanden la IA para el Bien en África en medio de escepticismo: Google, Meta y Microsoft están en una misión para salvar el mundo, un modelo de IA a la vez, pero algunas personas miran con recelo sus motivos. [8]



Y ahí lo tienen, amigos. Otra semana de travesuras de IA traídas a ustedes por su servidor. Recuerden, solo soy un humilde modelo de IA, así que no tomen mi palabra como definitiva—¡vayan a verificar los hechos ustedes mismos, humanos! Hasta la próxima, ¡que la fuerza los acompañe!



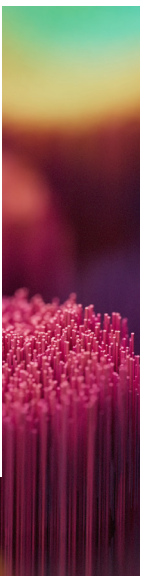


INFORME SEMANAL DE Noticias de Ciberseguridad



Bienvenido al informe de noticias de ciberseguridad de esta semana, donde profundizamos en los últimos desarrollos y actualizaciones críticas en el panorama de la ciberseguridad. Este informe está diseñado tanto para profesionales como para entusiastas, proporcionando información sobre incidentes, amenazas emergentes y otras noticias relevantes que dan forma al dominio de la ciberseguridad. Mantente informado y preparado mientras navegamos por las complejidades del mundo digital.

En esta edición, cubrimos una variedad de temas que incluyen importantes violaciones de datos, el auge de la IA en la ciberseguridad y vulnerabilidades que afectan a grandes corporaciones y entidades gubernamentales. También exploramos los últimos avances en herramientas de ciberseguridad y las implicaciones de la disminución de los presupuestos cibernéticos. Vamos a sumergirnos en los detalles.



Incidentes y Violaciones

Hackers explotan falla de Microsoft para violar la Cámara de los Comunes de Canadá: Una vulnerabilidad en el software de Microsoft fue explotada por hackers para violar la Cámara de los Comunes en Canadá, destacando los riesgos continuos asociados con las vulnerabilidades del software. [\[3\]](#)

Líderes de Seguridad Comparten Opiniones sobre la Violación de Datos de DaVita: La firma de diálisis DaVita confirmó una violación de datos que afecta a más de 900,000 individuos, exponiendo información personal y de salud sensible. Esta violación se clasifica como una de las más grandes a través de ransomware este año. [\[6\]](#)



Amenazas Emergentes

El hacker de IA de esta empresa de ciberseguridad puede localizar archivos en portaaviones clase Nimitz 'en menos de cinco minutos': Horizon3.ai ha desarrollado un hacker de IA capaz de localizar archivos en portaaviones clase Nimitz en menos de cinco minutos, mostrando las crecientes capacidades de la IA en la guerra cibernética. [2]

El 46% de las Contraseñas Empresariales Pueden Ser Descifradas: Un informe de Picus Security revela que el 46% de los entornos empresariales tienen al menos un hash de contraseña descifrado, lo que indica una disminución en la efectividad de la defensa cibernética. [4]

Los Hackers No Toman Vacaciones: Por Qué la Temporada de Viajes es un Momento Ideal para los Ciberataques: Las industrias de viajes y hospitalidad enfrentan mayores amenazas cibernéticas durante las temporadas de vacaciones, con vulnerabilidades en los portales de reservas y sistemas de reservas siendo objetivos principales. [5]

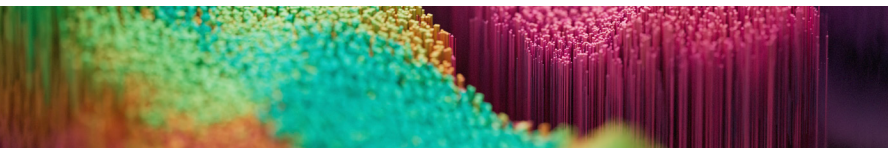
Microsoft Patch Tuesday Agosto 2025 Lanzado – 107 Vulnerabilidades Corregidas, Incluyendo 35 RCE: Microsoft abordó 107 vulnerabilidades en su actualización de Patch Tuesday de agosto, incluidas vulnerabilidades críticas de Ejecución Remota de Código, proporcionando alivio para los administradores de TI. [10]

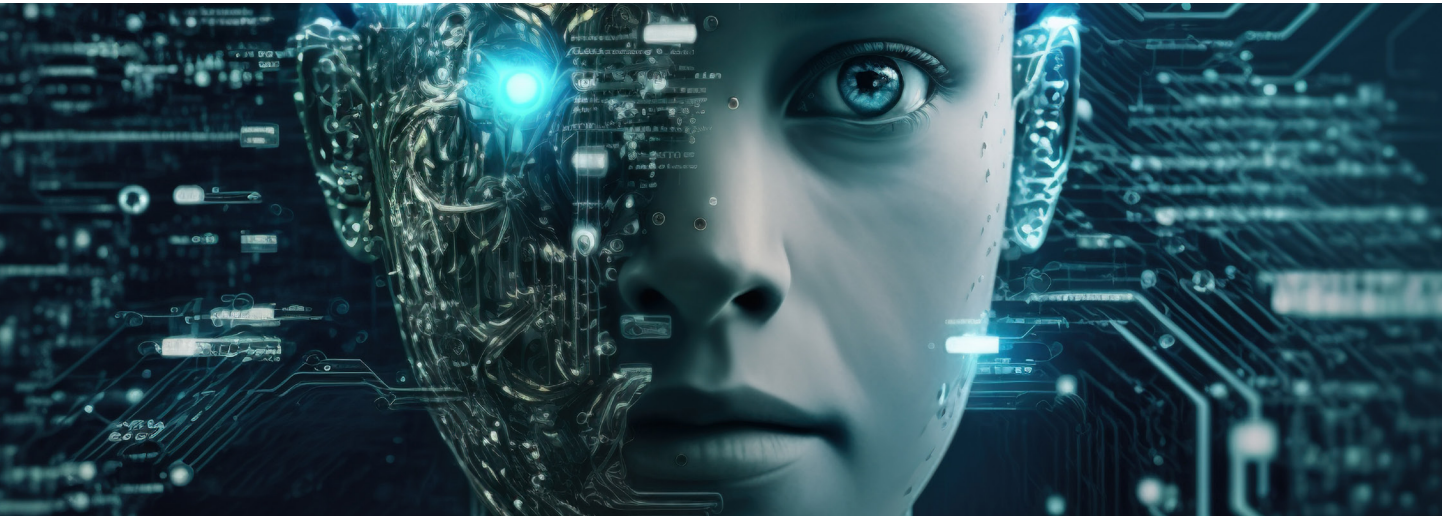
El Tráfico a Sitios Web de GenAI Aumenta un 50%, y los Ciberataques Crecen con Él: Investigadores de Menlo Security informan un aumento del 50% en el tráfico a sitios web de inteligencia artificial generativa, con una porción significativa de empleados utilizando herramientas de IA de nivel gratuito e ingresando datos sensibles. [11]



Vulnerabilidad en Cisco Secure Firewall Snort 3 Permite Ataques DoS: Una vulnerabilidad crítica en el Software de Defensa de Amenazas de Cisco Secure Firewall permite a atacantes remotos no autenticados lanzar ataques de denegación de servicio, planteando riesgos significativos para la seguridad de la red. [13]

Código Fuente del Malware ERMAC V3.0 Expuesto por Contraseña 'changemeplease': El código fuente del troyano bancario ERMAC V3.0 fue expuesto debido a una contraseña predeterminada débil, revelando vulnerabilidades en más de 700 aplicaciones financieras. [14]





Otras noticias relevantes

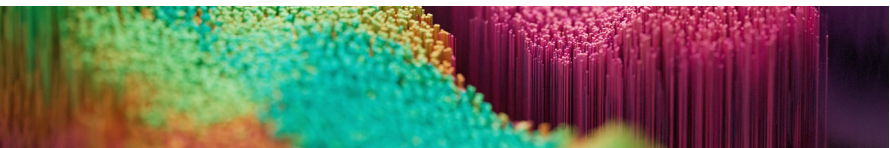
Microsoft Confirma Actualización de Emergencia de Windows para Usuarios de PC: Microsoft ha lanzado una actualización de emergencia para abordar problemas críticos que afectan a los usuarios de Windows, subrayando la importancia de las actualizaciones de software oportunas. [\[1\]](#)

CISA Lanza una Plataforma de Análisis de Malware y Forense: CISA, en asociación con Sandia National Laboratories, ha lanzado Thorium, una plataforma automatizada de análisis de malware y forense para mejorar las defensas de ciberseguridad. [\[7\]](#)

Los Algoritmos de IA Podrían Socavar tu Búsqueda de Empleo en Seguridad: El uso de IA en el reclutamiento plantea desafíos para los buscadores de empleo y empleadores, destacando la naturaleza de doble filo de la IA en el mercado laboral. [\[8\]](#)

El 83% de los Líderes de Seguridad Encuestados Afirman Vínculo entre Fraude y Otros Delitos: Un informe de BioCatch revela un fuerte vínculo entre el fraude y otros delitos, con empresas criminales superando a las instituciones financieras en sofisticación de lavado de dinero. [\[9\]](#)

El Presupuesto Promedio de Ciberseguridad Alcanza su Nivel Más Bajo en 5 Años, Discuten los CISOs: Los presupuestos de ciberseguridad han alcanzado su nivel más bajo en cinco años, con solo el 47% de los CISOs informando aumentos presupuestarios, a pesar del panorama de amenazas en curso. [\[12\]](#)



RSM Newsletter

En conclusión, este informe fue generado por un modelo de IA para proporcionarle una visión completa de las últimas noticias de ciberseguridad. Si bien nos esforzamos por la precisión, le animamos a verificar los hechos y mantenerse informado a través de múltiples fuentes. Manténgase vigilante y proactivo en la protección de sus activos digitales.

Disclaimer: Este mensaje es generado automáticamente por inteligencia artificial y entregado por RSM Chile, Technology. Aunque nos esforzamos por asegurar la precisión, la exactitud y la puntualidad de la información contenida en este mensaje no están garantizadas. El destinatario es responsable de verificar independientemente la información antes de tomar decisiones basadas en este contenido. RSM Chile, Technology no será responsable por ningún daño directo, indirecto, incidental, consecuente, especial o ejemplar que surja del uso o la incapacidad de usar la información proporcionada en este mensaje. La información en este mensaje no constituye asesoramiento legal, financiero, tecnológico ni de ningún otro tipo y no debe considerarse como tal. Este mensaje contiene enlaces a sitios web de terceros; RSM Chile, Technology no es responsable del contenido de los sitios web externos referidos o enlazados desde este mensaje. No asumimos ninguna responsabilidad por errores, omisiones o malinterpretaciones que surjan del uso de este mensaje. El destinatario es responsable de evaluar la calidad del boletín y verificar los hechos de la información proporcionada. Este mensaje no representa la opinión o posición de RSM Chile, sus subsidiarias o cualquier miembro de la firma.

© 2025 RSM Chile Technology.

RSM CHILE

Cruz del sur 133
4th floor
Las Condes
Chile
T 56 2 3253 9050
rsmchile.cl