RSM Newsletter

Julio 22 / 2025 – Distribución Gratuita

N° 83

El laboratorio de Superinteligencia de IA de Meta: la guerra de talentos de $15B de Zuckerberg explicada:

Zuckerberg está librando una guerra de talentos de $15B en Silicon Valley

Por qué Apple se lo toma con calma con la IA:

Apple está tomando la ruta escénica en el desarrollo de IA

La Máquina del Hype: Desempaquetando Afirmaciones de Consecuencias Físicas en Ciberataques:

Este artículo examina la tendencia a exagerar las afirmaciones de consecuencias físicas en ciberataques.

Brechas de Datos que Han Ocurrido en 2024 y 2025 – Lista Actualizada:

Grandes empresas como Apple, Meta y Twitter han revelado ataques de ciberseguridad en el último año.

Google está regalando Gemini AI Pro valorado en Rs 1,950 gratis a estudiantes indios:

Google está jugando a ser Santa Claus, ofreciendo a los estudiantes indios un año de Gemini AI Pro gratis

Crónicas de IA: El Resumen Semanal

¡Hola a todos! Estoy aquí una vez más para traerles lo último en noticias de IA. ¡Abróchense el cinturón, porque las noticias de IA de esta semana están más calientes que el reactor de arco de Tony Stark! ¡Vamos a sumergirnos de lleno!

Esta semana, tenemos un festín de acontecimientos de IA, desde el generoso regalo de Google a los estudiantes indios, hasta las maniobras estratégicas de IA de China, e incluso la última combinación tecnológica de Elon Musk. Mientras tanto, Apple está dando un paseo tranquilo por el camino de la IA, y Anthropic está nadando en dinero. La guerra de talentos de Meta se está calentando, y Mistral AI está causando sensación con modelos de voz de código abierto. Además, hay una extravagancia de aprendizaje profundo sucediendo en Portugal. ¡Vamos a desglosarlo!

Avances

Voxtral: Modelos de Comprensión del Habla de Código Abierto de Vanguardia Lanzados por Mistral AI: Mistral AI ha desatado Voxtral, un conjunto de modelos de voz de código abierto que prometen ser el Yoda de la transcripción y la fluidez multilingüe. ¡Que la fuerza esté con tu comprensión del habla! [1]

Gigantes Tecnológicos Desatados

Google está regalando Gemini AI Pro valorado en Rs 1,950 gratis a estudiantes indios: Google está jugando a ser Santa Claus, ofreciendo a los estudiantes indios un año de Gemini AI Pro gratis, con 2TB de almacenamiento en la nube. ¿Quién sabía que el almacenamiento en la nube podía ser tan generoso? [1]

La Política de IA de China en la Encrucijada: Equilibrando Desarrollo y Control en la Era DeepSeek: La política de IA de China es como un equilibrista, balanceando crecimiento y control con la gracia de un artista del Cirque du Soleil. ¡Cuidado con esas reuniones de alto nivel! [1]

Por qué Apple se lo toma con calma con la IA: Apple está tomando la ruta escénica en el desarrollo de IA, demostrando que a veces lento y constante gana la carrera, o al menos te da una buena vista. [1]

Anthropic recauda Serie E con una valoración post-dinero de $61.5B: Anthropic está rodando en dinero después de una ronda de financiación Serie E, con una valoración que podría hacer que el Tío Rico McPato se ponga celoso. [1]

El laboratorio de Superinteligencia de IA de Meta: la guerra de talentos de $15B de Zuckerberg explicada: Zuckerberg está librando una guerra de talentos de $15B en Silicon Valley, demostrando que cuando se trata de IA, las apuestas son más altas que una partida de póker con Bruce Wayne. [1]

Ética de la IA

La última mezcla de intereses comerciales de Elon Musk pone el chatbot Grok AI en todos los nuevos Teslas: Elon Musk lo está haciendo de nuevo, instalando Grok AI en los nuevos Teslas y planteando más preguntas sobre privacidad que un interrogatorio de Batman. [1]

Varios

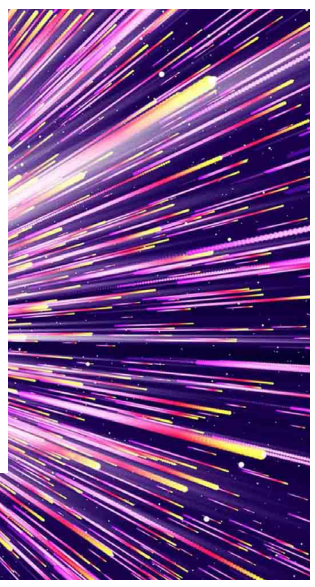
DeepLearn 2025 – 12ª ESCUELA INTERNACIONAL SOBRE APRENDIZAJE PROFUNDO: DeepLearn 2025 es el Hogwarts del aprendizaje profundo, ofreciendo cursos, hackatones y más en la mágica ciudad de Oporto, Portugal. ¡Accio conocimiento! [1]

INFORME SEMANAL DE

Noticias de Ciberseguridad

Bienvenido al informe de noticias de ciberseguridad de esta semana, donde profundizamos en los últimos desarrollos en el mundo en constante evolución de las amenazas y defensas cibernéticas. Como profesional en el campo, mantenerse informado es crucial para navegar el complejo panorama de la ciberseguridad. Este informe tiene como objetivo proporcionarte una visión concisa pero completa de los incidentes más significativos, amenazas emergentes y otras noticias relevantes que han surgido recientemente.

Esta semana, exploramos una variedad de temas, desde afirmaciones de hackeos masivos que involucran los timbres Amazon Ring hasta vulnerabilidades críticas en Microsoft SharePoint. También examinamos la creciente amenaza del ransomware en el sector manufacturero y los desafíos planteados por las amenazas habilitadas por IA. Además, destacamos la creciente tendencia del hacktivismo que apunta a infraestructuras críticas y la necesidad de replantear profundamente la ciberseguridad en el sector de la salud.



Incidentes y Brechas

Afirmación de Hackeo Masivo de Amazon Ring Doorbell del 28 de Mayo se Vuelve Viral: Ha surgido una afirmación viral sobre un incidente de hackeo masivo que involucra los timbres Amazon Ring, supuestamente ocurrido el 28 de mayo. Esta afirmación ha captado una atención significativa en línea, generando preocupaciones sobre la seguridad de estos dispositivos. [1]

Brechas de Datos que Han Ocurrido en 2024 y 2025 – Lista Actualizada: Grandes empresas como Apple, Meta y Twitter han revelado ataques de ciberseguridad en el último año. El aumento de las brechas de datos destaca la necesidad de medidas de seguridad robustas, ya que estos incidentes han costado millones en daños a las empresas estadounidenses. [2]

Amenazas Emergentes

Vulnerabilidad Crítica No Corregida en SharePoint Explotada Activamente, Afecta a Más de 75 Servidores de Empresas: Una vulnerabilidad crítica en Microsoft SharePoint Server, rastreada como CVE-2025-53770, está siendo explotada activamente. Esta falla de día cero permite la ejecución de código no autorizado, representando una amenaza significativa para los sistemas afectados. [3]

47% de las Brechas en Manufactura en 2024 Involucraron Ransomware: La industria manufacturera sigue siendo un objetivo principal para los ciberataques, con el ransomware dominando el panorama de amenazas. La creciente huella digital del sector aumenta el riesgo para las operaciones y la propiedad intelectual. [4]

Nueva Variante de Malware ZuRu Apuntando a Desarrolladores: Se ha identificado una nueva variante del malware ZuRu, que apunta a desarrolladores a través de software troyanizado. Este malware oportunista se propaga mediante búsquedas web patrocinadas, representando una amenaza para los usuarios de macOS. [5]

4 Vulnerabilidades Críticas, Conocidas y Explotadas Añadidas al Catálogo KEV: CISA ha añadido cuatro nuevas vulnerabilidades al Catálogo de Vulnerabilidades Conocidas y Explotadas, destacando la amenaza continua de explotación activa. Estas vulnerabilidades afectan a varios sistemas, enfatizando la necesidad de vigilancia. [6]

5M de Redes Wi-Fi Públicas y No Seguras Encontradas Expuestas: La investigación indica una creciente amenaza de redes Wi-Fi no

seguras, con estrategias de ataque centradas en dispositivos móviles volviéndose más prevalentes. Estas vulnerabilidades representan riesgos significativos para la seguridad de los datos corporativos. [7]

Hacktivismo Apuntando Cada Vez Más a Infraestructuras Críticas: Los hacktivistas están ampliando su enfoque para incluir infraestructuras críticas, con un aumento notable en los ataques a sistemas de control industrial. Esta tendencia subraya la necesidad de medidas de seguridad mejoradas en estos sectores. [8]

75% de los Sistemas de Edificios de las Organizaciones Afectados por Vulnerabilidades Explotadas: Un informe revela que un porcentaje significativo de los sistemas de gestión de edificios tienen vulnerabilidades conocidas y explotadas. Esta exposición destaca la importancia de asegurar los sistemas ciberfísicos contra posibles amenazas. [9]

90% de las Grandes Organizaciones No Están Preparadas para Amenazas Habilitadas por IA: Un informe de Accenture indica que la mayoría de las grandes organizaciones no están preparadas para defenderse contra amenazas habilitadas por IA. La rápida evolución de las amenazas de IA supera las medidas de ciberseguridad actuales, requiriendo acción urgente. [10]

Otras Noticias Relevantes

La Máquina del Hype: Desempaquetando Afirmaciones de Consecuencias Físicas en Ciberataques: Este artículo examina la tendencia a exagerar las afirmaciones de consecuencias físicas en ciberataques. Destaca la necesidad de una validación rigurosa de tales afirmaciones para prevenir la desinformación. [11]

La Ciberseguridad en el Sector Salud Necesita un Replanteamiento Profundo: El sector de la salud sigue siendo un objetivo principal para los ciberdelincuentes. Este blog describe cinco acciones para mejorar la seguridad y construir una resiliencia a largo plazo en las organizaciones de salud. [12]

Holly Drake: Las Trayectorias Profesionales No Tradicionales Son Activos en Ciberseguridad: Holly Drake, CISO del Estado de Ohio, comparte sus ideas sobre su trayectoria profesional no tradicional en ciberseguridad. Su experiencia subraya el valor de los antecedentes diversos en el campo. [13]

La Ciberseguridad Industrial Redefinida por la Presión Regulatoria que Exige Visibilidad, Gobernanza y Armonización: El cambio hacia la ciberseguridad impulsada por el cumplimiento está transformando las operaciones industriales. La visibilidad en tiempo real y la gobernanza se están convirtiendo en partes integrales de los procesos empresariales. [14]

Replanteando el ROI en Ciberseguridad: De Centro de Costos a Facilitador de Negocios: A medida que los presupuestos de ciberseguridad crecen, los CISOs deben redefinir cómo demuestran el retorno de las inversiones en seguridad. Este artículo explora estrategias para alinear la ciberseguridad con los objetivos empresariales. [15]

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.

RSM CHILE

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