RSM Newsletter

Agosto 12 / 2025 – Distribución Gratuita

N° 84

Cisco Hackeado – Atacantes Robaron Detalles de Perfiles de Usuarios Registrados en Cisco.com:

Cisco confirmó un ciberataque donde los atacantes robaron información básica de perfil de usuarios registrados en Cisco.com.

Como GPT-5:

LexisNexis está mejorando su juego de IA, añadiendo GPT-5 a su conjunto de herramientas legales.

Modelos GPT OSS de OpenAI disponibles en Amazon Bedrock y Amazon SageMaker:

AWS es ahora el orgulloso padre de los modelos de OpenAI, ofreciéndolos a millones de clientes.

CISA Publica Dos Avisos sobre Sistemas de Control Industrial:

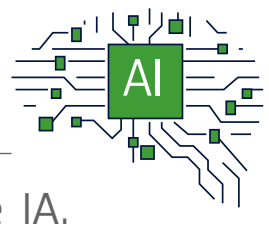
CISA publicó dos avisos sobre Sistemas de Control Industrial (ICS) el 5 de agosto de 2025.

Salesforce Obligado a Emitir Advertencia de Robo de Datos mientras Google Confirma que es una de las Víctimas:

Google anunció la semana pasada que han sido objetivo de un grupo de amenazas tras una serie de brechas de datos relacionadas con Salesforce.

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 las actualizaciones de IA de esta semana están más calientes que la última tecnología de Tony Stark! ¡Vamos a sumergirnos de lleno!

En el torbellino de eventos de IA de esta semana, Microsoft ha lanzado el tan esperado GPT-5 en su Copilot sin costo de suscripción, mientras que AWS está poniendo los modelos de OpenAI a disposición de su vasta base de clientes. El CEO de GitHub está agitando las aguas con un memorando sobre el uso de IA, y Anthropic está lanzando Claude Opus 4.1 con algunas mejoras impresionantes. Mientras tanto, LexisNexis está expandiendo sus capacidades de IA, y Xiaomi está mejorando su juego en los sectores de hogar inteligente y automotriz. En una nota más seria, el impacto de la IA en las perspectivas laborales para los graduados en ciencias de la computación está levantando cejas.

Gigantes Tecnológicos Desatados

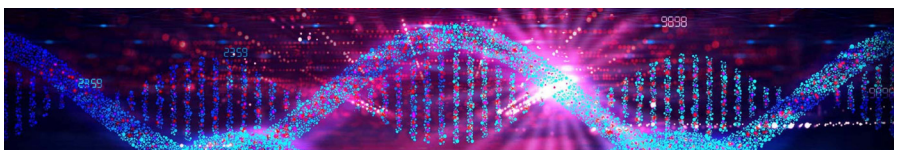
Microsoft Lanza GPT-5 en Copilot—No Se Necesita Suscripción: ¡Microsoft está regalando GPT-5 como Oprah regala autos—gratis para todos los usuarios de Copilot! Leer más

Modelos GPT OSS de OpenAI disponibles en Amazon Bedrock y Amazon SageMaker: AWS es ahora el orgulloso padre de los modelos de OpenAI, ofreciéndolos a millones de clientes. ¡Es como adoptar una mascota de IA súper inteligente! Leer más

CEO de GitHub: El Memorando de Microsoft Sobre Evaluar el Uso de IA es 'Juego Justo': El CEO de GitHub está jugando la carta de la IA, sugiriendo a los empleados que abracen la IA o consideren otras galaxias tecnológicas. ¡Que la fuerza de la IA los acompañe! Leer más

Lanzamiento de Claude Opus 4.1: Claude Opus 4.1 de Anthropic está aquí, con mejoras que lo convierten en el Iron Man de los modelos de IA. Leer más

LexisNexis Lanza Protégé General AI, Expandiendo las Capacidades Agénticas de su Asistente de IA a Modelos de IA General



Como GPT-5: LexisNexis está mejorando su juego de IA, añadiendo GPT-5 a su conjunto de herramientas legales. ¡Es como tener un superhéroe legal a disposición! Leer más

Anthropic nombra a Hidetoshi Tojo como Jefe de Japón y anuncia planes de contratación: Anthropic está expandiendo su imperio a Japón con Hidetoshi Tojo al mando. ¡Es como la versión de IA de una historia de origen de Marvel! Leer más

Xiaomi Presenta Nuevo Modelo de Voz de IA para Automóviles y Hogares Inteligentes: El nuevo modelo de voz de IA de Xiaomi está aquí para hacer que tu auto y hogar sean más inteligentes que Jarvis. ¡Cuidado, Tony Stark! Leer más

Ética de la IA

Cómo la IA podría estar dejando fuera a los graduados de ciencias de la computación de EE.UU. de trabajos de nivel inicial: La IA está jugando al villano en el mercado laboral, haciendo difícil que los nuevos graduados encuentren trabajo. ¡Es como si Thanos estuviera chasqueando oportunidades laborales! Leer más

Y ahí lo tienen, amigos. Otra semana de noticias de IA envuelta con un lazo. Recuerden, este informe fue elaborado por un modelo de IA, así que no solo tomen mi palabra—¡vayan y verifiquen, humanos! Hasta la próxima, ¡que sus algoritmos siempre estén a su favor!

INFORME SEMANAL DE

Noticias de Ciberseguridad

Bienvenido al informe de noticias de ciberseguridad de esta semana, donde profundizamos en los últimos desarrollos y perspectivas del mundo de las amenazas y defensas cibernéticas. Como profesional en el campo, mantenerse informado sobre los últimos incidentes, amenazas emergentes y avances estratégicos es crucial. Este informe tiene como objetivo proporcionarle una visión concisa pero completa de los eventos y tendencias más significativos en ciberseguridad.

Esta semana, exploramos una variedad de temas, incluyendo importantes violaciones de datos que afectan a empresas prominentes, nuevas vulnerabilidades y amenazas emergentes en el panorama digital, y perspectivas estratégicas para mejorar las prácticas de ciberseguridad. Desde la disrupción de grupos de ransomware hasta el endurecimiento de regulaciones sobre cables submarinos, estas historias destacan la naturaleza dinámica y en constante evolución de la ciberseguridad.

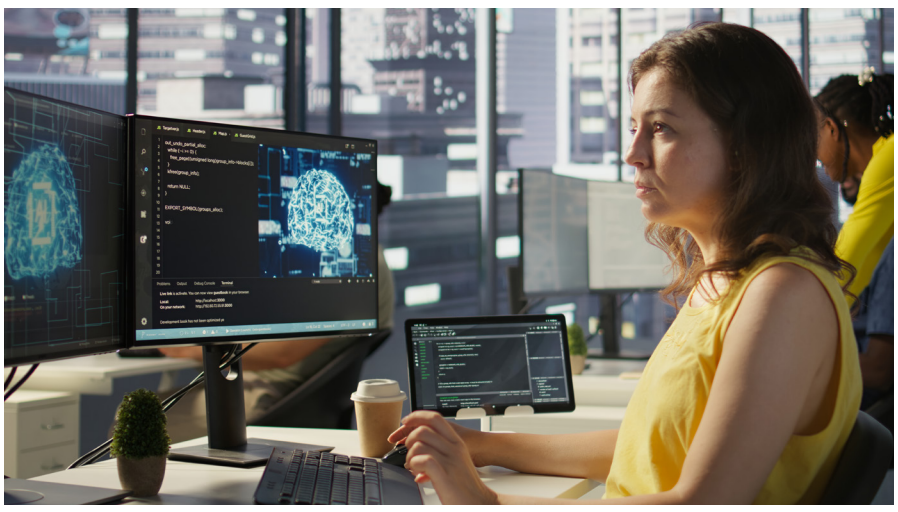
Incidentes y Brechas

Cisco Hackeado – Atacantes Robaron Detalles de Perfiles de Usuarios Registrados en Cisco.com: Cisco confirmó un ciberataque donde los atacantes robaron información básica de perfil de usuarios registrados en Cisco.com. La brecha ocurrió después de que un empleado fuera engañado por un ataque de phishing por voz, lo que llevó a un acceso no autorizado a un sistema CRM de terceros. Los datos comprometidos incluían nombres, nombres de organizaciones, direcciones físicas, IDs de usuario, direcciones de correo electrónico y números de teléfono. El equipo de seguridad de Cisco terminó el acceso del atacante e inició una investigación. [1]

Líderes de Seguridad Comparten Opiniones sobre la Brecha de Datos de DaVita: El 5 de agosto, la firma de diálisis DaVita confirmó una brecha de datos que afecta a más de 900,000 individuos. La brecha potencialmente expuso Números de Seguridad Social e información de salud personal. Rebecca Moody, Jefa de Investigación de Datos en Comparitech, señaló que este ataque es una de las mayores brechas de datos a través de ransomware este año, clasificándose como la séptima más grande en general, la tercera más grande en EE.UU., y la tercera más grande en un proveedor de atención médica. [2]

Salesforce Obligado a Emitir Advertencia de Robo de Datos mientras Google Confirma que es una de las Víctimas: Google anunció la semana pasada que han sido objetivo de un grupo de amenazas tras una serie de brechas de datos relacionadas con Salesforce. El actor ha afirmado estar afiliado al conocido grupo de hackers, ShinyHunters (también conocido como UNC6240), probablemente como un método para aumentar la presión sobre sus víctimas. Esta brecha se produce en medio de una ola continua de incidentes de hacking relacionados con Salesforce durante la última semana, con Chanel, Qantas, Adidas, Victoria's Secret, y muchos otros enfrentando ataques de ingeniería social. [3]

Incidentes y Vulnerabilidades de Ciberseguridad el 11 de agosto de 2025: El artículo discute varios incidentes y vulnerabilidades de ciberseguridad, incluyendo una vulnerabilidad de día cero en WinRAR explotada por el grupo de hackers Paper Werewolf, vulnerabilidades en webcams de Lenovo que podrían ser utilizadas para ataques BadUSB, y malware temático de Tesla propagado a través de anuncios falsos de Google. Además, las brechas de datos afectaron a Connex Credit Union, Google Ads CRM, y la Universidad de Australia Occidental. [4]



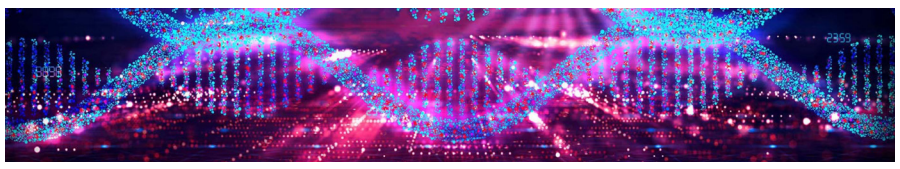
Amenazas Emergentes

El DOJ anuncia la disrupción del grupo de ransomware BlackSuit: El Departamento de Justicia (DOJ) ha anunciado la disrupción del grupo de ransomware BlackSuit, un movimiento significativo en la lucha contra el cibercrimen. Esta acción es parte de los esfuerzos continuos para combatir los ataques de ransomware que han tenido como objetivo varios sectores, incluyendo el de la salud. [5]

Microsoft Publica Guía sobre Vulnerabilidad de Alta Severidad (CVE-2025-53786) en Despliegues Híbridos de Exchange: Microsoft ha publicado una guía sobre una vulnerabilidad de alta severidad identificada como CVE-2025-53786, que afecta a los Despliegues Híbridos de Exchange. La guía tiene como objetivo abordar y mitigar los riesgos asociados con esta vulnerabilidad. [6]

CISA Publica Dos Avisos sobre Sistemas de Control Industrial: CISA publicó dos avisos sobre Sistemas de Control Industrial (ICS) el 5 de agosto de 2025. Estos avisos proporcionan información oportuna sobre problemas de seguridad actuales, vulnerabilidades y exploits relacionados con ICS. [7]

Informe de Brecha de Datos de IBM Expone Brechas en la Gobernanza de IA: El nuevo informe de IBM "Costo de una Brecha de Datos" revela que, aunque la adopción de IA está aumentando, la seguridad y gobernanza de la IA están significativamente rezagadas. Suja Viswesan, Vicepresidente de Productos de Seguridad y Runtime en IBM, explica que hay una brecha entre la adopción de IA y la supervisión, que los actores de amenazas están comenzando a explotar. [8]



Trabajos Múltiples Exponen a los Trabajadores a Mayores Riesgos de Ciberseguridad: La investigación de Kaspersky revela que los profesionales involucrados en múltiples trabajos, particularmente los trabajadores de la Generación Z, están en mayor riesgo de ciberataques debido a la amplia gama de aplicaciones corporativas que deben usar. Cuantas más aplicaciones usen los trabajadores, más puntos de exposición potenciales para que los actores de amenazas exploten. [9]

Estudios de Caso e Historias de Éxito

La Alianza CISO–CMO: Por qué el Mensaje de Ciberseguridad Necesita un Frente Unificado: Cada ejecutivo hoy en día entiende que una sola brecha de datos puede amenazar no solo la continuidad operativa, sino la misma confianza que sustenta una marca. Las consecuencias de un incidente mal gestionado pueden eclipsar el daño técnico en sí, como se vio tras las brechas de SolarWinds y Equifax. Ambas organizaciones enfrentaron no solo la remediación técnica, sino una prolongada batalla para recuperar la confianza pública. [10]

Otras noticias relevantes

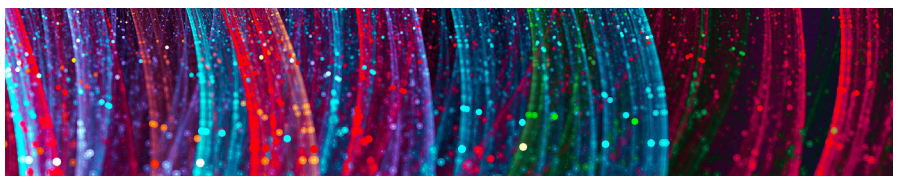
Amenazas Ocultas de Ciberseguridad: 20 Consejos de Expertos para Fortalecer la Estrategia: El artículo proporciona consejos de expertos para mejorar las estrategias de ciberseguridad identificando amenazas ocultas. [11]

La FCC endurece las reglas sobre empresas extranjeras que construyen cables submarinos, citando seguridad: La Comisión Federal de Comunicaciones ha adoptado nuevas reglas para dificultar que las empresas extranjeras soliciten licencias para construir cables submarinos, citando la necesidad de proteger la construcción continua de cables submarinos críticos que sustentan el internet y las comunicaciones transcontinentales. [12]

CISA Lanza una Plataforma de Análisis de Malware y Forense: La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) ha anunciado el lanzamiento de una plataforma automatizada y escalable de análisis de malware y forense llamada Thorium, creada en asociación con los Laboratorios Nacionales Sandia. [13]

Las Pruebas de Penetración ahora son Centrales en la Estrategia del CISO: Los líderes de seguridad están repensando su enfoque hacia la ciberseguridad a medida que las cadenas de suministro digitales se expanden y la IA generativa se incrusta en sistemas críticos. Una encuesta reciente de 225 líderes de seguridad realizada por Emerald Research encontró que el 68% está preocupado por los riesgos que plantean el software y los componentes de terceros. [14]

Seguridad en K–12 vs. Educación Superior: Lo que Escuelas y Universidades Necesitan Saber: Conozca las diferencias clave entre asegurar campus de K–12 y educación superior. El artículo discute la importancia de entender las necesidades y amenazas de seguridad específicas de diferentes entornos educativos, enfatizando la necesidad de estrategias de seguridad adaptadas para campus de K–12 y universidades. [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.

© 2025 RSM Chile Technology.

RSM CHILE

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