



Informe diario de tecnología

Las tendencias tecnológicas de hoy

22 de octubre de 2026 (jueves)

En pocos sorbos

Hoy en día, las herramientas de auditoría centradas en la seguridad y los motores de inferencia de alta eficiencia están ganando protagonismo en el ecosistema de desarrollo. Especialmente, los estudios académicos sobre las capacidades de los modelos de lenguaje visual (VLM) para comprender escenas tridimensionales y realizar manipulaciones en el mundo físico están atrayendo mucha atención.

27 destacados · ~9 min de lectura

12 GitHub
Trending

5 Hacker
News

5 Hugging Face ·
modelos del día

5 Hugging Face ·
artículos del día

Datos recopilados el 22 de octubre de 2026 a las 12:25.

Los recuentos de las fuentes y los metadatos de los elementos de este informe quedan fijados en el momento de la recopilación. Las páginas de Descubrimiento pueden mostrar valores de fuentes en vivo más recientes.

Los resúmenes y las traducciones de este informe se preparan con inteligencia artificial. Antes de tomar decisiones importantes, le recomendamos verificar la fuente mediante el enlace que acompaña a cada elemento.

01 cloudflare/security-audit-skill

security-audit-skill, desarrollado por Cloudflare, es una capacidad de agente de codificación (coding-agent skill) diseñada para auditorías de seguridad de múltiples etapas. Su objetivo es estandarizar las auditorías de seguridad en los procesos de desarrollo de software proporcionando hallazgos legibles por máquina y verificados de forma independiente.

JavaScript · ★ 37.749 · +2.012 hoy <https://github.com/cloudflare/security-audit-skill>

[Informar un error](#)

02 vllm-project/vllm

vllm-project/vllm es un motor de inferencia y servicio para grandes modelos de lenguaje (LLM) que proporciona un alto rendimiento y eficiencia de memoria. Desarrollada en Python, esta herramienta tiene como objetivo optimizar los procesos de ejecución de modelos de inteligencia artificial.

Python · ★ 95.076 · +441 hoy <https://github.com/vllm-project/vllm>

[Informar un error](#)

03 stablyai/orca

stablyai/orca es una plataforma que le permite ejecutar varios agentes de codificación (coding agents), como Grok Bot y Claude Code, con sus propias suscripciones. Permite gestionar flotas de agentes en diferentes dispositivos con opciones de escritorio, móvil y tiempo de ejecución remoto (remote runtime).

TypeScript · ★ 101.961 · +1.541 hoy <https://github.com/stablyai/orca>

[Informar un error](#)

04 headroomlabs-ai/headroom

headroomlabs-ai/headroom es una herramienta que reduce el uso de tokens al comprimir datos como archivos de registro, salidas de código y fragmentos de RAG enviados a grandes modelos de lenguaje (LLM). Esta estructura, que puede utilizarse como biblioteca, proxy y servidor MCP, tiene como objetivo aumentar la eficiencia manteniendo la calidad de respuesta del modelo.

Python · ★ 77.462 · +474 hoy <https://github.com/headroomlabs-ai/headroom>

[Informar un error](#)

05 DietrichGebert/ponytail

DietrichGebert/ponytail es un proyecto de JavaScript que minimiza el proceso de escritura de código de los agentes de inteligencia artificial, guiándolos para que actúen como el desarrollador senior más perezoso. Adopta el principio de que el mejor código es el que no se escribe, con el objetivo de abordar la eficiencia en los procesos de desarrollo con un enfoque diferente.

JavaScript · ★ 172.377 · +2.079 hoy <https://github.com/DietrichGebert/ponytail>

[Informar un error](#)

06 Comfy-Org/ComfyUI

ComfyUI es una interfaz gráfica modular y una interfaz de programación de aplicaciones (API) que ofrece una interfaz basada en nodos para modelos de difusión (diffusion models). Este software, capaz de realizar inferencias rápidas en sistemas locales, permite a los usuarios configurar flujos de trabajo complejos a través de un editor visual.

Python · ★ 141.808 · +939 hoy <https://github.com/Comfy-Org/ComfyUI>

[Informar un error](#)

07 supabase/supabase

Supabase es una plataforma de desarrollo que ofrece una base de datos Postgres dedicada para crear aplicaciones web, móviles y de inteligencia artificial. Este proyecto, escrito en TypeScript, tiene como objetivo facilitar los procesos de gestión de bases de datos y desarrollo de aplicaciones.

TypeScript · ★ 113.222 · +504 hoy <https://github.com/supabase/supabase>

[Informar un error](#)

08 twentyhq/twenty

Twenty ofrece una alternativa de código abierto al software de gestión de relaciones con clientes Salesforce. Esta plataforma se está desarrollando centrándose en la integración de la inteligencia artificial.

TypeScript · ★ 59.448 · +112 hoy <https://github.com/twentyhq/twenty>

[Informar un error](#)

09 shiyu-coder/Kronos

Kronos, un modelo base (foundation model) entrenado en el lenguaje de los mercados financieros, ha sido desarrollado para el procesamiento y análisis de datos financieros. Este proyecto, preparado en lenguaje Python, es un modelo de inteligencia artificial diseñado para dar sentido a los datos del mercado.

Python · ★ 43.035 · +575 hoy <https://github.com/shiyu-coder/Kronos>

[Informar un error](#)

10 strelov1/freehire

freehire, desarrollado en lenguaje Go, es un motor de búsqueda de código abierto (cuyo código fuente está abierto al acceso y desarrollo de todos) diseñado para quienes buscan empleo. Ofrece una plataforma que permite a los usuarios buscar y encontrar ofertas de trabajo.

Go · ★ 2.643 · +360 hoy <https://github.com/strelov1/freehire>

[Informar un error](#)

11 akitaonrails/ai-memory

akitaonrails/ai-memory ofrece una solución de memoria a largo plazo (long term memory) para interfaces de línea de comandos (CLI) centradas en la codificación. El proyecto, que tiene como objetivo facilitar la transferencia de datos entre diferentes proveedores de agentes de inteligencia artificial, se está desarrollando en lenguaje Rust.

Rust · ★ 12.583 · +286 hoy <https://github.com/akitaonrails/ai-memory>

[Informar un error](#)

12 Graphify-Labs/graphify

Graphify es un proyecto de Python que convierte bases de código y documentos en un grafo de conocimiento (knowledge graph) consultable. Al utilizar el análisis de árbol de sintaxis abstracta (AST) local en lugar de almacenamiento basado en vectores, esta herramienta funciona como una habilidad (skill) para entornos de desarrollo como Claude Code, Cursor, Codex y Gemini CLI.

Python · ★ 132.135 · +1.433 hoy <https://github.com/Graphify-Labs/graphify>

[Informar un error](#)

01 PHP 8.2.35

PHP 8.2.35 es una nueva actualización de seguridad lanzada para PHP, un lenguaje de script del lado del servidor. Esta versión se ha puesto a disposición de los usuarios como parte de los esfuerzos continuos para mejorar la seguridad general del software.

1.029 puntos · 545 comentarios <https://github.com/php/php-src/releases/tag/php-8.2.35>

[Informar un error](#)

Discusión: news.ycombinator.com/item?id=50180873 (1029 puntos · 545 comentarios)

02 Today's PHP security release, and how we're strengthening security

La PHP Foundation anunció la actualización de seguridad que viene con la versión PHP 8.2.35 y compartió sus nuevas estrategias para mejorar la seguridad general del software. Este trabajo tiene como objetivo solucionar las vulnerabilidades y fortalecer los mecanismos de defensa para PHP, un lenguaje de script del lado del servidor.

731 puntos · 362 comentarios <https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-we-re-strengthening-php-security/>

[Informar un error](#)

Discusión: news.ycombinator.com/item?id=50182987 (731 puntos · 362 comentarios)

03 Meta ordered to pay \$25B penalty in New Mexico Cambridge Analytica case

El estado de Nuevo México dictaminó que la empresa de redes sociales Meta debe pagar una multa de 25 mil millones de dólares en el marco del caso Cambridge Analytica. La decisión surgió como resultado del proceso legal relacionado con las prácticas de la empresa sobre la privacidad y seguridad de los datos de los usuarios.

543 puntos · 325 comentarios <https://www.cnn.com/2026/10/21/meta-new-mexico-cambridge-analytica-penalty.html>

[Informar un error](#)

Discusión: news.ycombinator.com/item?id=50184820 (543 puntos · 325 comentarios)

04 There isn't an easy exploit for this PHP vulnerability

Se señala que una vulnerabilidad de seguridad en PHP, contrariamente a la creencia popular, no tiene una estructura que sea fácil de explotar. Al examinar los detalles técnicos de dicha vulnerabilidad, se explica por qué es difícil para los atacantes aprovecharla.

513 puntos · 308 comentarios <https://eliastaylor.com/noexploit/>

[Informar un error](#)

Discusión: news.ycombinator.com/item?id=50188948 (513 puntos · 308 comentarios)

05 Compromised LiteLLM 1.107.0 on PyPI Installs a Credential Stealer and Backdoor

La versión 1.107.0 de LiteLLM fue reemplazada en el índice de paquetes de Python (PyPI) por un código malicioso que contenía una puerta trasera (backdoor) y realizaba robo de credenciales. LiteLLM, la biblioteca que los desarrolladores de software utilizan para integrar modelos de lenguaje, puso en peligro los datos de los usuarios con esta brecha de seguridad.

508 puntos · 168 comentarios <https://safedep.io/litellm-pypi-compromise-credential-stealer-backdoor/>

[Informar un error](#)

Discusión: news.ycombinator.com/item?id=50181114 (508 puntos · 168 comentarios)

01 deepseek-ai/DeepSeek-V4.1-Flash-1017

DeepSeek-V4.1-Flash-1017 es un modelo de generación de texto basado en imagen-texto (image-text-to-text) compartido en Hugging Face. Dicho modelo tiene la capacidad de procesar datos obtenidos de imágenes para generar resultados de texto.

♥ 2.240 · 42.122 descargas <https://huggingface.co/deepseek-ai/DeepSeek-V4.1-Flash-1017>

[Informar un error](#)

02 black-forest-labs/flux-3-image-klein-comfy

Desarrollado por Black Forest Labs, black-forest-labs/flux-3-image-klein-comfy es un modelo de inteligencia artificial diseñado para operaciones de conversión de imagen a imagen (image-to-image). Este modelo, compartido en la plataforma Hugging Face, está configurado para funcionar de manera compatible con herramientas de flujo de trabajo basadas en imágenes como ComfyUI.

♥ 1.225 · 490.447 descargas <https://huggingface.co/black-forest-labs/flux-3-image-klein-comfy>

[Informar un error](#)

03 meta-models/Muse-Spark-Open-816B-A42B

meta-models/Muse-Spark-Open-816B-A42B, compartido en Hugging Face, es un modelo de inteligencia artificial que genera resultados de texto procesando entradas de imagen y texto. El modelo destaca por sus capacidades de procesamiento de datos multimodales.

♥ 645 · 2.891 descargas <https://huggingface.co/meta-models/Muse-Spark-Open-816B-A42B>

[Informar un error](#)

04 black-forest-labs/flux-3-image-klein

Desarrollado por Black Forest Labs, black-forest-labs/flux-3-image-klein es un modelo de inteligencia artificial diseñado para operaciones de conversión de imagen a imagen (image-to-image). Este modelo, disponible en la plataforma Hugging Face, permite generar nuevos resultados basados en imágenes existentes.

♥ 615 · 92.604 descargas <https://huggingface.co/black-forest-labs/flux-3-image-klein>

[Informar un error](#)

05 OpenMOSS-Team/MOSS-Image-SFT

OpenMOSS-Team/MOSS-Image-SFT es un modelo de inteligencia artificial con capacidad de generación de imágenes a partir de texto (text-to-image). Este modelo, compartido en la plataforma Hugging Face, ha sido desarrollado para convertir comandos basados en texto en resultados visuales.

♥ 545 · 5.840 descargas <https://huggingface.co/OpenMOSS-Team/MOSS-Image-SFT>

[Informar un error](#)

01 SpatialScout: Can VLM Agents Actively Explore and Map 3D Scenes?

SpatialScout es una herramienta de evaluación (benchmark) que mide las habilidades de los modelos de lenguaje visual (vision-language models) para mapear escenas tridimensionales y exhibir inteligencia espacial a nivel de objeto a través de la exploración activa. Este estudio, que incluye ochenta escenas interiores diferentes, tiene como objetivo evaluar si los modelos pueden crear una representación coherente del mundo en procesos de exploración autónoma.

50 me gusta · 2 comentarios <https://huggingface.co/papers/2610.26659>

[Informar un error](#)

02 From VLM Planners to Robotic Agents: Self-Evolving Harnesses for History-Dependent Manipulation

Los modelos de visión-lenguaje-acción (vision-language-action) ofrecen resultados exitosos al combinar los procesos de comprensión visual y generación de acciones en tareas de manipulación robótica. Este artículo propone sistemas de automejora para gestionar dependencias basadas en interacciones pasadas en tareas a largo plazo y reducir los errores de ejecución.

5 me gusta · 1 comentarios <https://huggingface.co/papers/2610.29560>

[Informar un error](#)

03 CompactSplat: Spatially Adaptive Gaussian Distribution for Feedforward Scene Reconstruction

CompactSplat es un método que reconstruye escenas tridimensionales a partir de imágenes dispersas y utiliza una distribución gaussiana espacialmente adaptativa (spatially adaptive Gaussian distribution) en lugar de realizar una distribución uniforme por píxel. Este enfoque tiene como objetivo aumentar la precisión geométrica y los detalles de textura sin necesidad de optimización basada en la escena.

1 me gusta · 1 comentarios <https://huggingface.co/papers/2610.13177>

[Informar un error](#)

04 Right Screen, Wrong Transition: World Models as Verifiers for GUI Agents

El artículo publicado en Hugging Face sostiene que la auditoría de seguridad para agentes de interfaz gráfica de usuario (GUI) no debe centrarse únicamente en la captura de pantalla, sino también en el proceso de transición esperado tras la acción realizada. Su objetivo es detectar vulnerabilidades en las interacciones de la interfaz integrando las salidas de los modelos mundiales (world models) actuales en procesos de verificación a partir de formatos como texto o código.

1 me gusta · 1 comentarios <https://huggingface.co/papers/2610.11942>

[Informar un error](#)

05 PACE: Periodic and Channel-Aligned Encoding of Four-Bit Recurrent States

PACE, compartido en Hugging Face, es un método que codifica los estados recurrentes (recurrent states) utilizados en modelos de lenguaje basados en atención lineal (linear-attention) con una precisión de cuatro bits. Esta técnica permite procesar más secuencias simultáneamente al reducir el uso de memoria durante la inferencia.

9 me gusta · 3 comentarios <https://huggingface.co/papers/2610.29545>

[Informar un error](#)



coding-agent skill

Es un módulo de capacidad especializado desarrollado por Cloudflare, utilizado para realizar auditorías de seguridad de software de forma automática.

LLM

Son modelos de inteligencia artificial entrenados con volúmenes masivos de datos, capaces de comprender el lenguaje humano y generar texto.

inference

Es el proceso mediante el cual un modelo de inteligencia artificial entrenado genera predicciones o resultados utilizando los nuevos datos que se le proporcionan.

coding agents

Son herramientas de inteligencia artificial que realizan de forma autónoma tareas como escribir, depurar y editar código en los procesos de desarrollo de software.

remote runtime

Es el entorno que permite que el software o los agentes de inteligencia artificial se ejecuten en un servidor remoto en lugar de en una computadora local.

diffusion models

Es un tipo de modelo de inteligencia artificial capaz de generar imágenes de alta calidad a partir de datos ruidosos.

API

Es el puente que permite que diferentes programas de software intercambien datos y se comuniquen entre sí.

foundation model

Es un modelo integral que constituye la base de los sistemas de inteligencia artificial, entrenado con conjuntos de datos amplios para ser utilizado en una gran variedad de tareas.

CLI

Es una interfaz basada en texto que ejecuta programas mediante comandos escritos en lugar de usar el ratón.

long term memory

Es un método de almacenamiento que permite a los sistemas de inteligencia artificial guardar y utilizar posteriormente sus interacciones y datos pasados sin olvidarlos.

knowledge graph

Es un modelo de datos que organiza la información y las relaciones entre ella en forma de una estructura de red interconectada.

AST

Es un método que convierte la estructura del código de un lenguaje de programación en un árbol jerárquico que el ordenador puede entender.

skill

Es una habilidad o complemento especializado que utilizan los agentes de inteligencia artificial para realizar una tarea específica.

exploit

Es un método utilizado para tomar el control de un software o sistema, o para hacerlo funcionar incorrectamente, aprovechando una vulnerabilidad de seguridad.

backdoor

Es un código malicioso insertado secretamente en un software que permite el acceso no autorizado al eludir las medidas de seguridad del sistema.

image-text-to-text

Es un modelo de inteligencia artificial capaz de procesar entradas visuales y de texto simultáneamente para generar salidas de texto adecuadas.

trescout.com · TreScout rastrea y resume, a usted solo le queda leer.