BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Campañas con IA atacan gobierno y finanzas en LATAM

TLP:CLEAR
20.05.2026

CLICK PARA EMPEZAR

CYBERSOCDTS

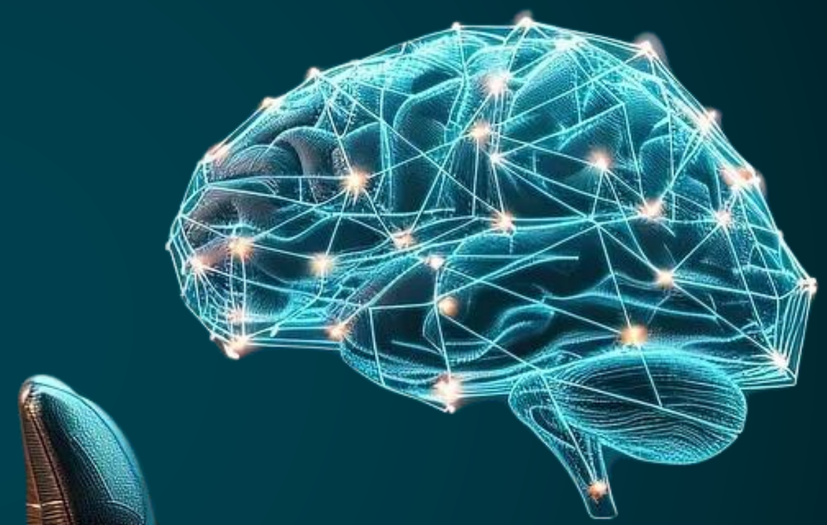
En esta edición:

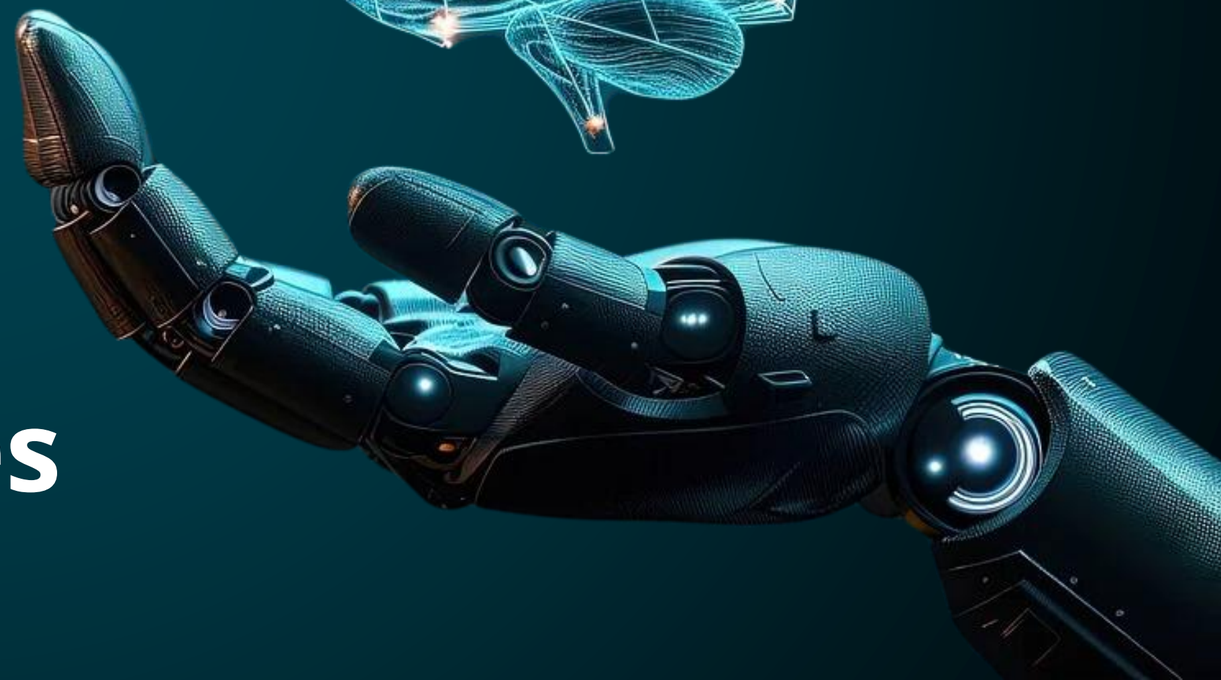
Vibe Hacking: Dos campañas potenciadas por IA se dirigen a los sectores gubernamental y financiero en América Latina

CONTENIDO

DataSec

- Nuestra Esencia
- Vulnerabilidades
- Noticias
- Recomendaciones





NUESTRA ESENCIA

BOLETÍN CIBERSEGURIDAD

Este boletín está diseñado para mantener al lector informado y brindarle pautas de seguridad en un entorno digital en constante evolución. Incluye contenido sobre las últimas amenazas, vulnerabilidades y las mejores prácticas de protección.

EMPRESA

DataSec es una empresa colombiana líder en servicios tecnológicos, enfocada en la implementación, administración, soporte, monitoreo y gestión de plataformas de Seguridad Informática y Networking, con años de experiencia en proyectos de ciberseguridad y conectividad para diversos sectores.

SOC

DataSec cuenta con un Centro de Operaciones de Seguridad Cibernética (CSOC) especializado en la detección, análisis y respuesta a amenazas. Este centro opera de manera continua 24/7, contribuyendo a la prevención y mitigación de incidentes en tiempo real.

Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability

CVE-2026-20182

Critical (10)

Impacto: Elevación de privilegios.

Resumen: Una vulnerabilidad en Cisco Catalyst SD-WAN Controller y Cisco Catalyst SD-WAN Manager permitiría a un atacante remoto no autenticado evadir el proceso de autenticación y obtener acceso con privilegios administrativos. La falla se origina en un error durante el mecanismo de handshaking de las conexiones de control, lo que permite que solicitudes manipuladas sean aceptadas como válidas.

Producto Afectado

- Cisco Catalyst SD-WAN Controller (vSmart)
- Cisco Catalyst SD-WAN Manager (vManage)

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad publicadas por Cisco.
Restringir y monitorear conexiones de control SD-WAN.
Auditar accesos administrativos y uso de NETCONF.

Ver + INFO.

Fecha de Publicación: 08/MAY/2026 INFO

Cisco Catalyst SD-WAN Manager Multiple Vulnerabilities

CVE-2026-20209, CVE-2026-20210, CVE-2026-20224

High (8.6)

Impacto: Acceso no autorizado.

Resumen: Múltiples vulnerabilidades en Cisco Catalyst SD-WAN Manager permiten a un atacante remoto sin autenticación acceder a información sensible, escalar privilegios o lograr acceso no autorizado a la aplicación. Las fallas se deben a una validación insuficiente de entradas y controles de seguridad inadecuados en el manejo de ciertos procesos internos del sistema.

Producto Afectado

Cisco Catalyst SD-WAN Manager (vManage)

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad publicadas por Cisco.

Ver +INFO.

Fecha de Publicación: 14/MAY/2026 INFO

Incorrect global authorization

CVE-2026-26083

Critical (9.8)

Impacto: Ejecución de código o comandos no autorizados.

Resumen: Una vulnerabilidad de autorización faltante [CWE-862] en la interfaz web (WEB UI) de FortiSandbox, FortiSandbox Cloud y FortiSandbox PaaS podría permitir que un atacante no autenticado ejecute código o comandos no autorizados mediante solicitudes HTTP.

Producto Afectado

- FortiSandbox 4.4 y 5.0
- FortiSandbox Cloud 5.0, 23 y 24
- FortiSandbox PaaS 22.1 a 23.4.

Ver +INFO.

Solución:

Actualizar inmediatamente a las versiones corregidas publicadas por Fortinet y restringir temporalmente el acceso público a la interfaz administrativa GUI

Ver +INFO.

Fecha de Publicación: 13/MAY/2026

INFO

Vulnerabilidades críticas en Cisco Unity Connection permiten ejecución remota de código y ataques SSRF

CVE-2026-20034 / CVE-2026-20035

High (8.8)

Impacto: Ejecución remota de código, ataques SSRF y compromiso de sistemas.

Resumen: Cisco publicó múltiples vulnerabilidades de alta severidad que afectan a Cisco Unity Connection. Las fallas identificadas podrían permitir a atacantes remotos ejecutar código arbitrario en dispositivos afectados o realizar ataques Server-Side Request Forgery (SSRF) mediante solicitudes HTTP especialmente manipuladas

Producto Afectado

Producto compatible afectado:

- Cisco Unity Connection
- Sistemas con Web Inbox habilitado
- Interfaces web de administración

Ver +INFO.

Solución:

Actualizar inmediatamente a las versiones corregidas publicadas por Cisco.
Restringir acceso administrativo.
Deshabilitar Web Inbox si no es necesario.

Ver +INFO.

Fecha de Publicación: 06/MAY/2026

INFO

Vulnerabilidad RCE en Windows DNS Client

CVE-2026-41096

Microsoft publicó una actualización de seguridad para corregir una vulnerabilidad crítica de ejecución remota de código (RCE) en Windows DNS Client. La falla podría permitir que un atacante remoto ejecute código arbitrario sobre sistemas vulnerables mediante tráfico DNS especialmente manipulado, comprometiendo la seguridad del sistema y facilitando movimientos laterales dentro de redes empresariales.

Recomendación:
Aplicar inmediatamente las actualizaciones de seguridad publicadas por Microsoft correspondientes al Patch Tuesday de mayo de 2026.

Productos Afectados

Los productos afectados son:

Windows DNS ClientSistemas Windows compatibles afectados por CVE-2026-41096

Ver +INFO

Fecha de Publicación: 12/MAY/2026 INFO

Vulnerabilidad crítica en Windows Netlogon

CVE-2026-41089

Microsoft corrigió una vulnerabilidad crítica de desbordamiento de búfer basado en pila en Windows Netlogon. Un atacante remoto podría explotar la falla sin requerir autenticación ni interacción del usuario, obteniendo privilegios SYSTEM sobre controladores de dominio afectados. Especialistas de Rapid7 advirtieron que la complejidad de explotación es baja y que el impacto podría comprometer completamente entornos Active Directory empresariales.

Recomendación:
Actualizar inmediatamente controladores de dominio y sistemas Windows afectados.

Productos Afectados:

Productos Afectados:

Windows NetlogonActive DirectoryWindows Server

Ver +INFO

Fecha de Publicación: 12/MAY/2026 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
12/05/2026	CVE-2025-67604	Fortinet	5.2	Vulnerabilidad de desbordamiento de memoria (Out-of-Bounds Write) en el daemon CAPWAP de FortiOS que puede permitir a un atacante con control de dispositivos autenticados (FortiAP, FortiExtender o FortiSwitch) ejecutar código o comandos con privilegios elevados en el dispositivo FortiGate.
06/05/2026	CVE-2026-20167	Cisco	7.7	Vulnerabilidad de denegación de servicio (DoS) en Cisco IoT Field Network Director que puede permitir a un atacante remoto provocar la interrupción del servicio mediante solicitudes maliciosas, afectando la disponibilidad de la plataforma de gestión.
18/05/2026	CVE-2026-8181	WordPress plugin	9.8	Vulnerabilidad crítica de bypass de autenticación en el plugin Burst Statistics para WordPress que permite a atacantes no autenticados obtener privilegios administrativos mediante solicitudes manipuladas a la API REST, comprometiendo la integridad del sitio.
12/05/2026	CVE-2025-53844	Fortinet	8.3	Vulnerabilidad de escritura fuera de límites (Out-of-Bounds Write) en el daemon CAPWAP de FortiOS que puede permitir a un atacante autenticado ejecutar código arbitrario en dispositivos FortiGate a través de dispositivos gestionados como FortiAP o FortiSwitch.

Campañas con IA atacan gobierno y finanzas en LATAM

Investigadores de Trend Micro identificaron dos campañas de ciberataques denominadas SHADOW-AETHER-040 y SHADOW-AETHER-064, dirigidas contra entidades gubernamentales y organizaciones financieras en Latinoamérica. Los atacantes emplearon inteligencia artificial “agentic AI” para automatizar gran parte de las operaciones ofensivas, desde el acceso inicial hasta la exfiltración de información, convirtiéndose en uno de los primeros casos documentados de uso de IA para ejecutar ataques completos de forma autónoma. Las campañas afectaron principalmente entidades gubernamentales en México y organizaciones financieras en Brasil, utilizando herramientas avanzadas para movimiento lateral, túneles SOCKS5 y despliegue de webshells. Los investigadores resaltan que el uso de IA permitió generar scripts y malware personalizados en tiempo real, dificultando la detección mediante herramientas tradicionales basadas en firmas.

A continuación, compartimos IoC para ser agregados a las herramientas de seguridad perimetral. Ver *+INFO*.

El ATAQUE

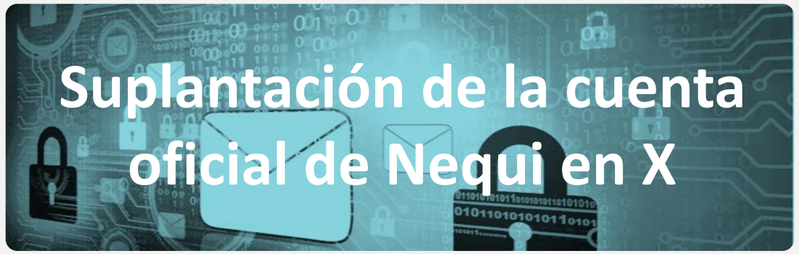
Los atacantes comprometieron servidores y aplicaciones expuestas para desplegar webshells y herramientas de tunneling como Chisel y Neo-reGeorg, permitiéndoles mantener acceso persistente dentro de las redes afectadas y ocultar el tráfico malicioso mediante conexiones SOCKS5 y ProxyChains.

Posteriormente, utilizaron inteligencia artificial para generar scripts y malware personalizados en tiempo real, facilitando actividades de movimiento lateral, robo de credenciales y exfiltración de información sensible. Estas campañas estuvieron dirigidas principalmente a entidades gubernamentales y organizaciones financieras de Latinoamérica, dificultando la detección mediante controles tradicionales basados en firmas.

+ INFO

CONTEXT	INDICATOR	(MD5)
IPv4	62[.]171[.]185[.]97	N/A
IPv4	209[.]99[.]185[.]223	N/A
IPv4	209[.]99[.]185[.]221	N/A
IPv4	167[.]148[.]195[.]53	N/A
IPv4	159[.]65[.]202[.]204	N/A
Dominio	cloudservbr[.]com	N/A
Dominio	infra-telemetry[.]com	N/A

ÚLTIMAS NOTICIAS

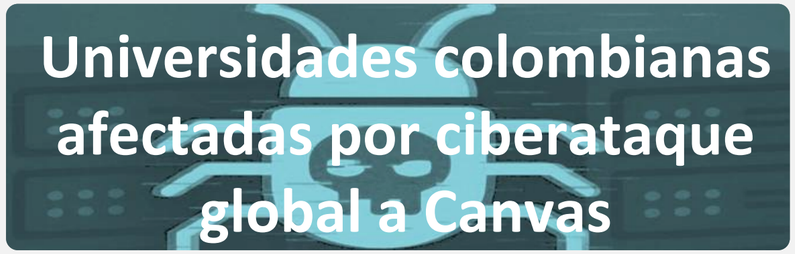


Suplantación de la cuenta oficial de Nequi en X

La cuenta oficial de Nequi en la red social X fue comprometida temporalmente por atacantes, quienes modificaron la imagen del perfil y publicaron mensajes relacionados con criptomonedas y posibles esquemas fraudulentos. Debido a que se trataba de una cuenta verificada, el incidente representó un riesgo significativo de phishing y estafas dirigidas a usuarios de la plataforma.

Durante el compromiso, se difundieron publicaciones promocionando activos como TRON y USDT, una táctica común utilizada para aprovechar la confianza de los seguidores y redirigir tráfico hacia enlaces maliciosos o campañas de fraude financiero.

INFO

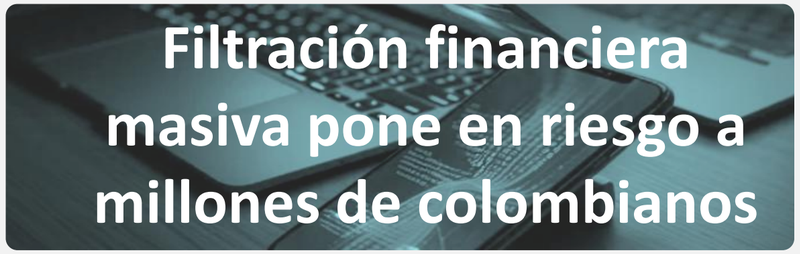


Universidades colombianas afectadas por ciberataque global a Canvas

Varias universidades colombianas aparecieron en la lista de instituciones potencialmente afectadas por el ciberataque masivo contra la plataforma educativa Canvas, atribuido al grupo ShinyHunters. El incidente habría comprometido datos académicos y personales de millones de estudiantes y docentes a nivel mundial.

El ataque incluyó amenazas de filtración de información y afectaciones operativas en plena temporada de exámenes, evidenciando los riesgos de dependencia en plataformas SaaS educativas y la importancia de fortalecer controles de acceso y monitoreo de proveedores externos.

INFO



Filtración financiera masiva pone en riesgo a millones de colombianos

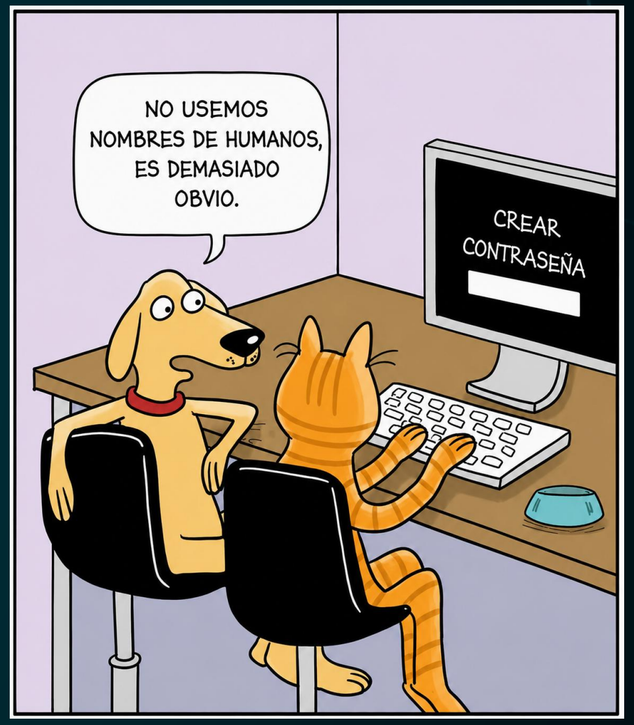
Una presunta filtración masiva de datos financieros expuso información sensible de millones de colombianos, incluyendo datos personales y bancarios que podrían ser utilizados en campañas de fraude, phishing y suplantación de identidad. El incidente es considerado uno de los mayores leaks financieros documentados en el país.

La exposición de este tipo de información incrementa el riesgo de estafas digitales, toma de cuentas y ataques dirigidos contra usuarios y entidades financieras, especialmente en un contexto donde los fraudes digitales continúan en aumento en Colombia.

INFO

Las mejores contraseñas no cuentan historias personales.

En ciberseguridad, uno de los errores más comunes continúa siendo el uso de contraseñas predecibles o relacionadas con información personal. Muchas personas creen estar creando claves “seguras”, pero terminan utilizando nombres, fechas o datos fáciles de descubrir mediante ataques de fuerza bruta, ingeniería social o filtraciones de datos. Una contraseña débil puede convertirse en la puerta de entrada a cuentas personales, correos corporativos o información sensible. La seguridad digital no depende solo de tener una contraseña, sino de crear una que realmente sea difícil de adivinar..



🔐 Evita usar nombres de personas, mascotas, fechas de nacimiento o palabras comunes en tus contraseñas.
🧠 Crea claves largas y complejas combinando mayúsculas, minúsculas, números y símbolos.
📱 Activa autenticación multifactor (MFA) para añadir una capa extra de protección.
⚠️ No reutilices la misma contraseña en diferentes plataformas o servicios.
🔑 Utiliza gestores de contraseñas para almacenar credenciales de forma segura.
🛡️ Cambia inmediatamente cualquier contraseña que haya podido verse comprometida.
🔍 Verifica regularmente si tus cuentas han sido expuestas en filtraciones de datos.
💻 Mantén una cultura de seguridad digital tanto en entornos personales como corporativos.

En ciberseguridad, no se trata de crear cualquier contraseña... sino de construir una que nadie pueda adivinar.

ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4