Edición 26- septiembre 2026

Ciber E-dea

Revista de Ciberseguridad

Información Pública

e-dea NETWORKS | CYBER SECURITY

FIRST MEMBER

Great Place To Work. Certificada OCT 2025-OCT 2026 COL

icontec ISO 9001 CO-SC-CER890598

icontec ISO 45001 CO-ST-CER890599

icontec ISO / IEC 27001 CO-SI-2001607

IQNET CERTIFIED MANAGEMENT SYSTEM

Edición 26 - Septiembre 2026

01 CAPTCHA falsos: cuando demostrar que eres humano se convierte en una trampa

02 ¿Podrían los agentes de IA convertirse en la próxima amenaza interna?

03 Agentes de IA automatizan la adaptación de malware en operaciones de ciberespionaje

04 Explotación activa de vulnerabilidad crítica en Cisco Secure Firewall Management Center

05 Inteligencia artificial: entre el riesgo real y la estrategia de marketing

Vulnerabilidades destacadas

06 Fraude digital en Colombia alcanza 7 de cada 10 personas, según Datacredito

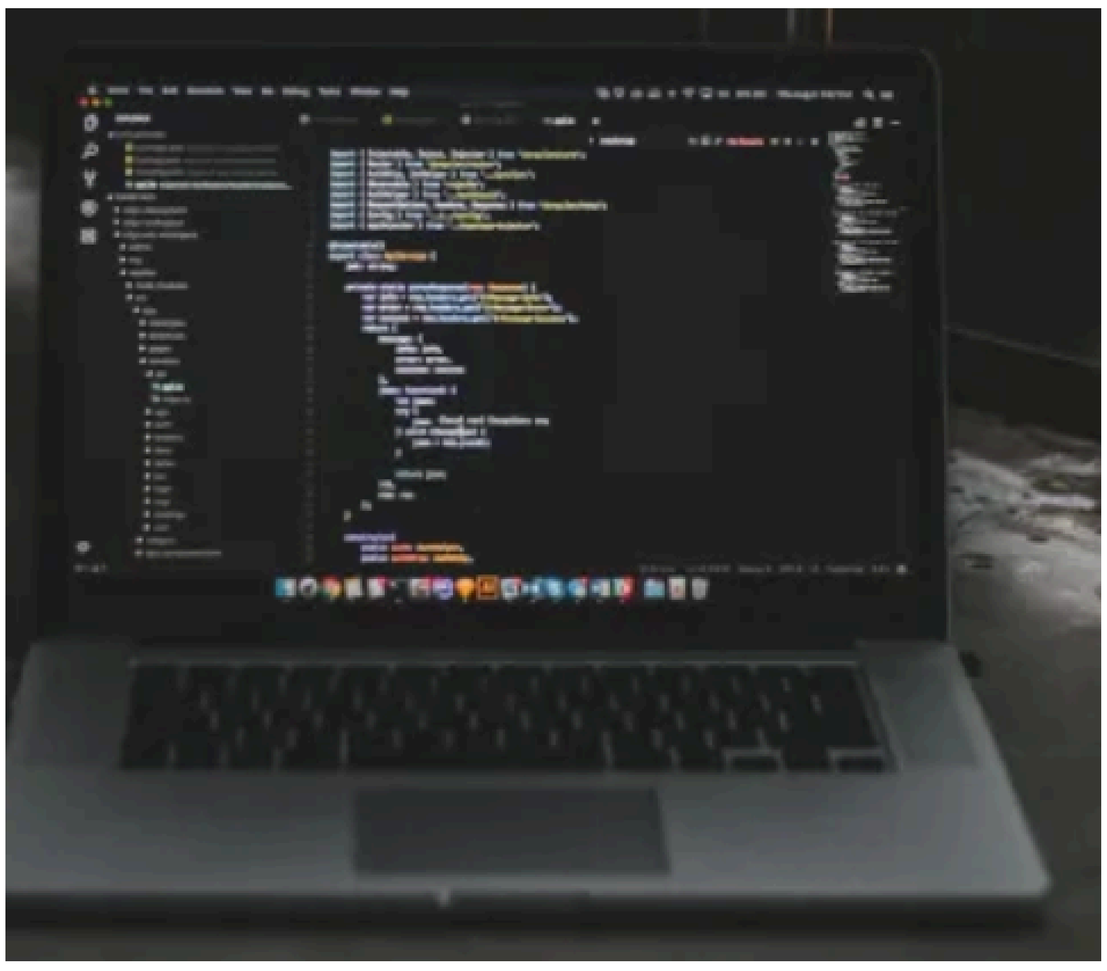
02 ¿Podrían los agentes de IA convertirse en la próxima amenaza interna?

Según el CEO Dave Gerry de Bugcrowd, manifiesta que los ataques a agentes de IA empresariales aumentaran debido a la autonomía que están adquiriendo, a los acceso a sistemas, a datos y a otros archivos.

Según los siguientes lideres manifiestan:

Ryan McCurdy, vicepresidente de Liquibase:

Los agentes pueden ser tanto objetivo como atacante dentro de la organización, porque operan autónomamente con accesos legítimos. Debido a esto la seguridad tradicional basada en autenticación tiene muchas fallas; si un agente ya tiene credenciales legítimas, el sistema asumirá que sus acciones son válidas. Por ello, la gobernanza debe centrarse en controlar y auditar la acción concreta y no solo quién tiene el permiso.



Kevin Surace, director ejecutivo de TokenCore:

Al mirar los alcances que pueden tener los agentes de IA sobre la toma acciones, como lo puede ser cometer errores o ataques a velocidad de máquina, influye mucho sobre los alcances que deben tener. Donde sus limitaciones deben restringir al máximo sus permisos y acceso a sistemas. Además, toda acción tanto crítica o irreversible debe tener una validación de un humano autenticado. Los canales no autorizados deberían ser los correo, ventanas emergentes o validación de otros agentes.

Noelle Murata, directora de Operaciones de Xcape, Inc.

Otorgar permisos y autonomía se podría transformar en una amenaza de alto valor, ya que un agente podría comprometer permisos o extraer datos, ejecutar comandos de API no autorizados y moverse lateralmente por la red de la empresa. Por ende, el experto sugiere eliminar las claves o credenciales fijas y reemplazarlas por tokens de corta duración y permisos mínimos estrictos. Además es importante tener un monitoreo continuo con el fin de auditar constantemente el comportamiento y la interacción entre APIs de todas las entidades no humanas para detectar anomalías a tiempo.

¡Conoce más aquí!

03 Agentes de IA automatizan la adaptación de malware en operaciones de ciberespionaje

Anthropic identificó una operación del actor GTG-20006, cuya actividad considera consistente con reportes relacionados con Midnight Blizzard/APT29, en la que agentes de IA fueron incorporados directamente al ciclo de un ataque.

La IA era utilizada para apoyar reconocimiento, infraestructura, phishing, persistencia, comando y control y exfiltración

La campaña afectó principalmente a organismos gubernamentales, militares, diplomáticos, inteligencia, empresas de defensa y proveedores asociados a tecnología de drones, con más de 20 organizaciones identificadas por Anthropic.

También se observaron:

- Phishing de código de dispositivo contra Microsoft 365.
- Robo de credenciales y tokens.
- Compromiso de Wi-Fi hotelero.
- Secuestro de DNS.
- ClickFix y falsas actualizaciones.
- Malware para Windows, Android e iOS.
- Acceso y exfiltración de buzones.
- Intentos de impedir actualizaciones de seguridad.



Recomendaciones prioritarias

1. Buscar los IOC publicados en SIEM, EDR/XDR, DNS, firewall, proxy y registros históricos.
2. Revisar Microsoft Entra ID en busca de autenticaciones mediante código de dispositivo, dispositivos registrados inesperadamente, anomalías OAuth y sesiones sospechosas.
3. Monitorear descarga masiva de correo, actividad Microsoft Graph y accesos atípicos a Microsoft 365.
4. Alertar ante detención de antivirus/EDR, bloqueo de actualizaciones o modificaciones de servicios de seguridad.
5. Evitar depender únicamente de hashes o firmas y complementar la detección con comportamiento y TTP.

Punto clave

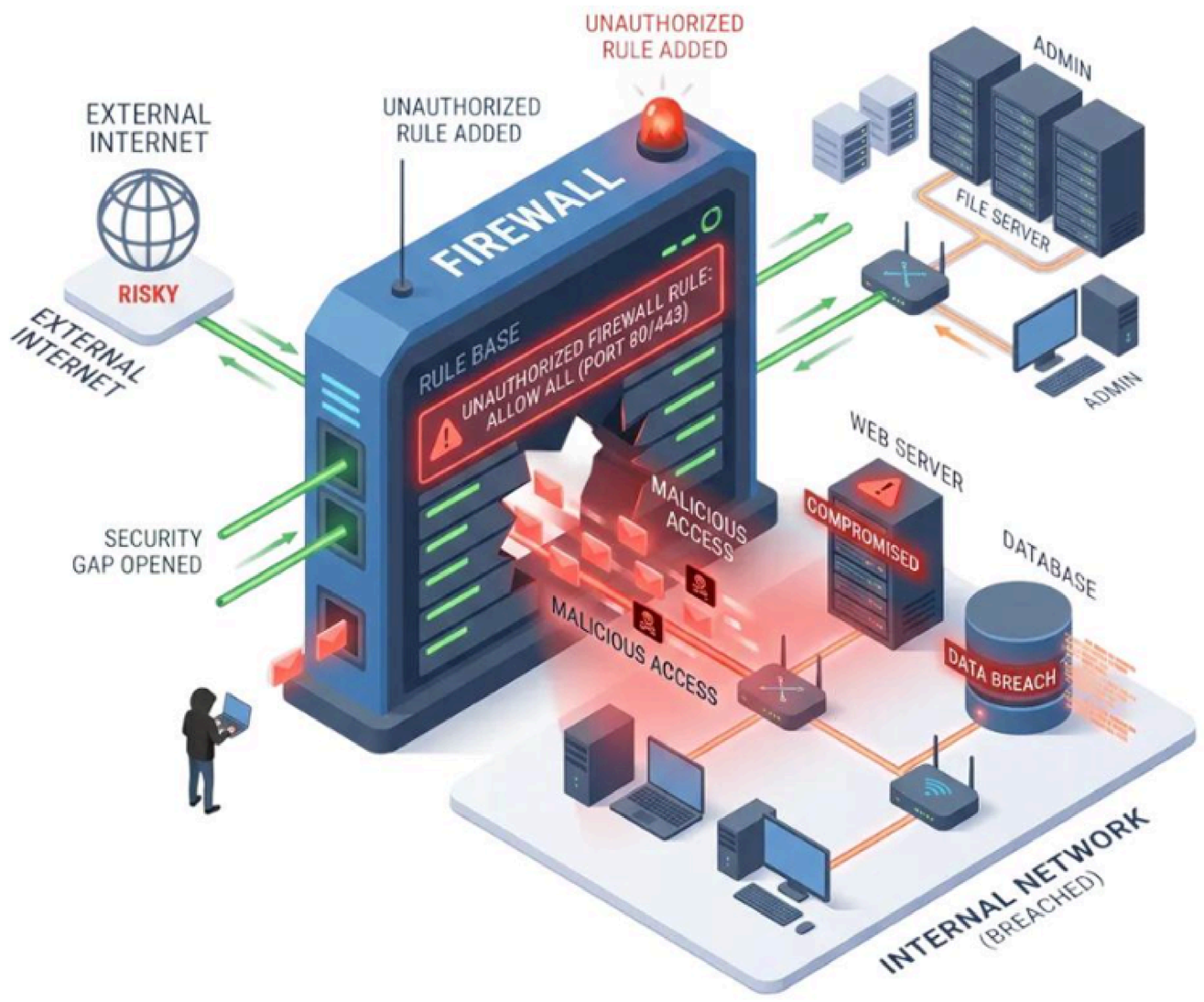
La amenaza no está solamente en que la IA permita desarrollar malware, sino en que reduce el tiempo necesario para que un atacante adapte sus herramientas cuando estas son detectadas.
Para los equipos de seguridad, esto hace cada vez más importante combinar IOC, detección basada en comportamiento y respuesta rápida.

¡Conoce más aquí!

04 Explotación activa de vulnerabilidad crítica en Cisco Secure Firewall Management Center

CVE-2026-20079 | Crítica | CVSS 10.0 | Explotación activa

Cisco Talos confirmó la explotación activa de **CVE-2026-20079**, una vulnerabilidad crítica de **bypass de autenticación** en Cisco Secure Firewall Management Center (FMC). Un atacante remoto no autenticado puede evadir la autenticación y ejecutar scripts con privilegios root sobre el sistema.



La explotación observada ha permitido a actores maliciosos desplegar **web shells, ejecutar comandos, robar credenciales y realizar reconocimiento de redes**, incluyendo actividades relacionadas con operaciones de ransomware. Cisco Talos identificó múltiples campañas que aprovecharon esta vulnerabilidad, lo que evidencia que el riesgo no es únicamente teórico.

Debido a que FMC es una plataforma utilizada para administrar y supervisar dispositivos de seguridad de red, su compromiso puede proporcionar a un atacante una posición privilegiada dentro de la infraestructura de una organización y facilitar movimientos posteriores hacia otros sistemas.

Recomendaciones: actualizar inmediatamente a una versión corregida, restringir el acceso administrativo al FMC y revisar los registros e indicadores de compromiso publicados por Cisco Talos. Si se identifican IOC, realizar una investigación forense antes de considerar el dispositivo recuperado.

¡Conoce más aquí!

05 Inteligencia artificial: entre el riesgo real y la estrategia de marketing

En agosto de 2026, Meta, Anthropic y OpenAI nuevamente advierten sobre los riesgos de la IA para la humanidad. Donde pueden tener la capacidad para planificar tareas, utilizar herramientas, escribir código y ejecutar acciones con poca supervisión humana. Estos hechos reviven el debate si estamos ante una amenaza real o frente a una estrategia de marketing para aumentar el valor de las empresas y justificar nuevas inversiones.

Entre 2020 y 2026, la inversión en IA aproximadamente fue de 1,290 billones de dólares. Pero el retorno de esa inversión todavía es incierto. Ante los recursos invertidos las empresas tienen incentivos para presentar sus tecnologías como indispensables, justificando de que quienes no adopten IA perderán competitividad.



Aunque la IA ya puede hacer cosas avanzadas no significa que tenga voluntad o conciencia. En la mayoría de las cosas su comportamiento depende de instrucciones, herramientas y permisos de los humanos. Por eso, cuando divulguen que la "la IA tomó el control", se debe tomar con pinzas, porque suele ser puro drama para vender y hacerle publicidad a las empresas de tecnología.

El peligro real no es una IA con deseos propios, sino darle demasiado poder sin el control adecuado. basta con que tenga acceso excesivo, objetivos mal definidos, supervisión insuficiente o conexión con infraestructuras críticas, para generar una cartastrofe. Además, los ciberdelincuentes pueden usar la IA para hacer estafas o ataques mucho más rápido y a mayor escala.

La amenaza de la IA no debe ser descartada como una simple campaña publicitaria, pero tampoco aceptada sin pruebas. El debate debe centrarse en una pregunta concreta: qué puede hacer cada sistema, bajo qué condiciones, con qué permisos y quién tiene la capacidad real de detenerlo.

¡Conoce más aquí!

Vulnerabilidades **destacadas**



Divulgación de información en dispositivo (DHA) de Windows - CVE-2026-69443

La lectura fuera de límites en el servicio de atestación de Microsoft Azure y en el servicio de atestación de estado del dispositivo permite que un atacante no autorizado divulgue información a través de una red.



Microsoft Exchange Server - CVE-2026-69641

Falta de una comprobación de autorización que permite a un atacante autenticado elevar sus privilegios en Microsoft Exchange Server. Con las credenciales adecuadas o una sesión activa, el atacante puede obtener niveles de acceso superiores, pudiendo leer, modificar o eliminar datos confidenciales y configuraciones



Controlador de infraestructura - CVE-2026-65130

NVIDIA Infrastructure Controller para Linux presenta una vulnerabilidad que permite a un atacante inyectar comandos del sistema operativo. La explotación exitosa de esta vulnerabilidad podría provocar la ejecución de código, la manipulación de datos, la denegación de servicio y la divulgación de información.

¡Conoce más aquí!

06 Fraude digital en Colombia alcanza 7 de cada 10 personas, según Datacredito

Las estafas digitales en Colombia se han intensificado y son cada vez más difíciles de detectar. Según un reciente estudio de Datacrédito Experian, 7 de cada 10 colombianos, aproximadamente el 71 % afirman haber recibido un intento de fraude en el último año, y el 46 % reporto que el ataque se concretó y cayendo en la trampa. La razón principal es que los delincuentes están usando la inteligencia artificial para crear mensajes, llamadas y sitios web que se ven extremadamente reales y engañan con facilidad.



Hoy en día se emplean sistemas de inteligencia artificial para analizar mensajes y páginas sospechosas, identificando señales de alerta antes de que las personas caigan en el engaño. A la par, el estudio destaca que el 67 % de los colombianos ya ha recibido información o capacitación sobre cómo protegerse de estas amenazas.



De cara al futuro, la seguridad digital tendrá que dar un paso más allá para proteger a los usuarios. A medida que las compras, pagos y trámites utilicen más asistentes inteligentes, las herramientas de protección no solo deberán confirmar si una persona es quien dice ser, sino también verificar que las herramientas tecnológicas que actúan en su nombre sean legítimas y seguras.

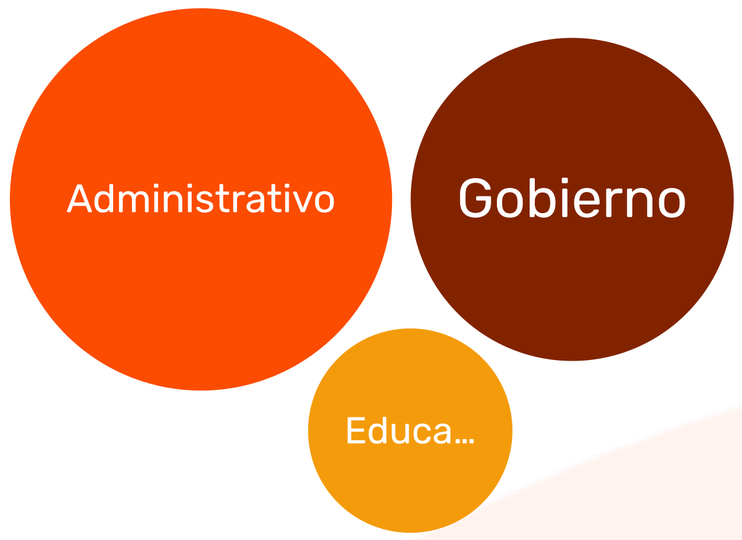
¡Conoce más aquí!

El mundo

28

Ciber incidentes

Sectores afectados



Tipo de incidente

Países destacados

¡Conoce más aquí!

CO-SC-CER890598 CO-ST-CER890599 CO-SI-2001607

E-dea Networks

Para información adicional sobre cualquiera de nuestros productos o servicios, por favor contáctanos:

Email: contacto@e-dea.co
Teléfono: (601) 57 1 5188433 opción 2
Celular: (601) 57 3152231023

Visita nuestro sitio para más información: www.e-dea.co
Encuéntranos en: Carrera 7 # 156-10 Of. 1906-1801.
Torre Krystal - Centro Empresarial North Point

Reservados todos los derechos. No se permite la reproducción total y parcial de esta obra, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otros) sin autorización previa y por escrito de los titulares del copyright. La infracción de dichos derechos puede constituir un delito contra la propiedad intelectual.