Edición 24 - Julio 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 24 - Julio 2026

01 Falsos instaladores de 7-Zip son utilizados para crear una red global de proxies maliciosos.

02 Cómo los ciberdelincuentes explotaron el Mundial de Fútbol 2026.

03 IA, política y desinformación: La investigación sobre BlackCore y su presunta manipulación digital.

04 Vulnerabilidades destacadas.

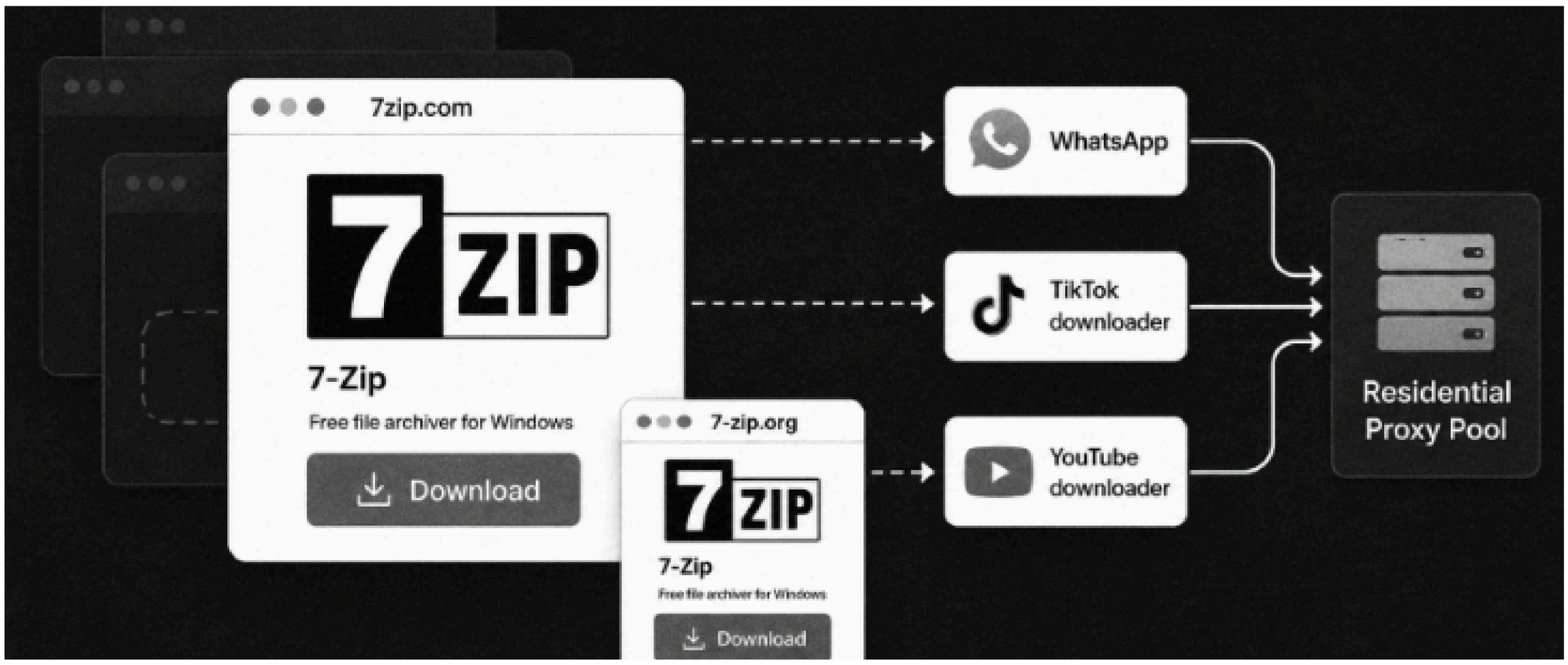
05 ¿IA fuera de control?: La alerta de OpenAI sobre el comportamiento autónomo en la IA

06 Ciber Incidentes en Colombia y en el mundo.

07 Contacto

01 **Falsos instaladores de 7-Zip** *son utilizados para crear una red global de proxies maliciosos.*

Investigadores de Infoblox identificaron una campaña atribuida al actor de amenazas Lurking Lizard, la cual utiliza instaladores falsificados de 7-Zip y otras aplicaciones populares para convertir los dispositivos de las víctimas en nodos de una red de proxies residenciales. La investigación reveló una infraestructura compuesta por más de 230 dominios fraudulentos utilizados para distribuir software troyanizado y comercializar el acceso a los equipos comprometidos.



Datos clave

Una vez instalado el software falso, el equipo continúa funcionando aparentemente con normalidad, mientras el malware permite que terceros utilicen la conexión a Internet de la víctima para enrutar tráfico malicioso. Esta infraestructura facilita el anonimato de los ciberdelincuentes y puede ser utilizada para campañas de fraude, evasión de controles de seguridad y otras actividades ilícitas. Además, los atacantes suplantan proveedores legítimos de servicios proxy y crean sitios falsos de reseñas para aumentar la credibilidad de su operación.

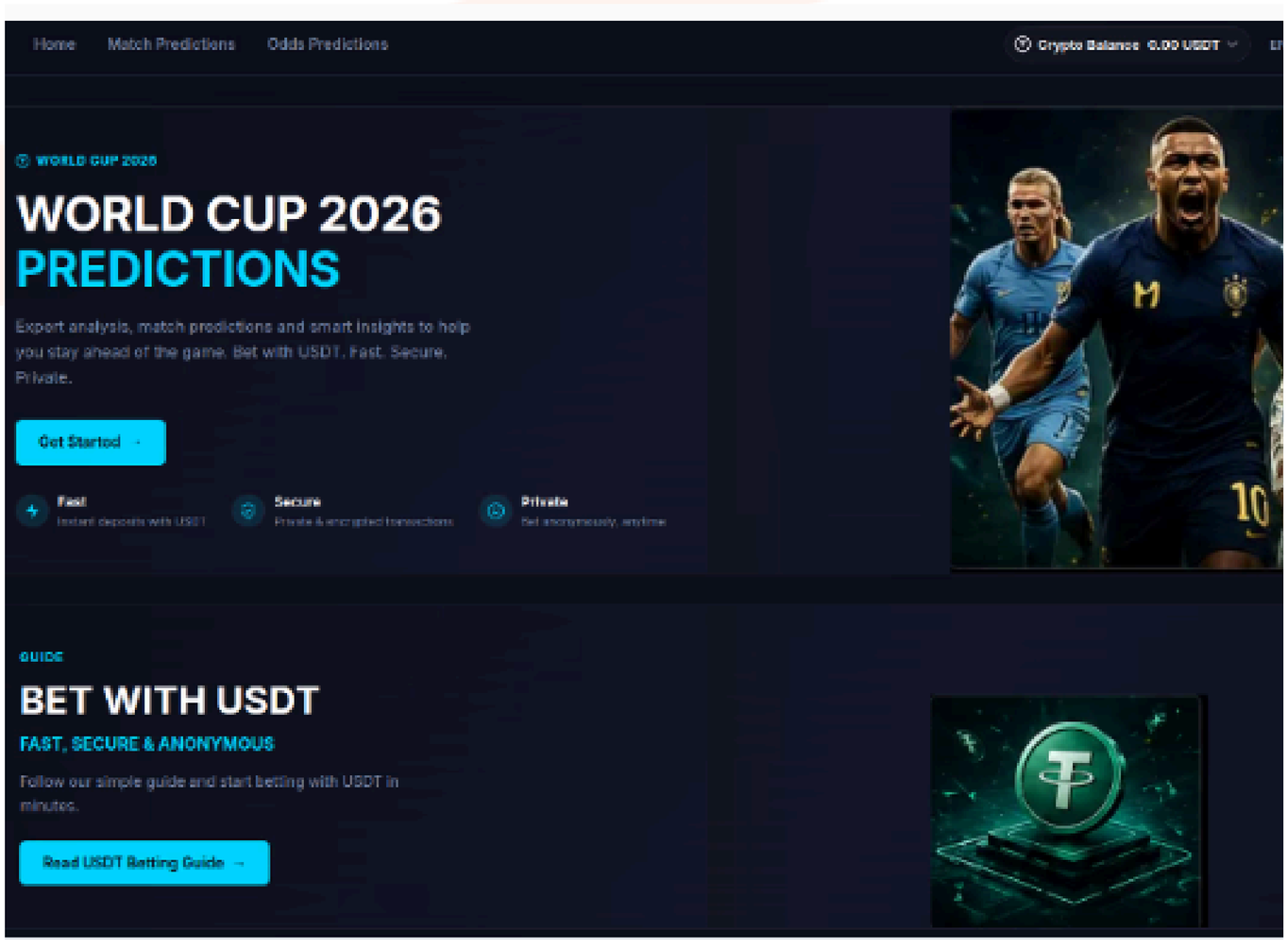
¿Cómo protegerse de este ataque?

El incidente refuerza la necesidad de descargar software únicamente desde sitios oficiales, verificar cuidadosamente los dominios antes de instalar aplicaciones y mantener controles de seguridad que permitan detectar cambios en los sistemas, conexiones de red inusuales y la instalación de servicios no autorizados.

¡Conoce más aquí!

02 Cómo los ciberdelincuentes explotaron el *Mundial de Fútbol 2026.*

El Mundial de Fútbol 2026 no solo amplificó la demanda global: también creó un ecosistema digital temporal donde la urgencia (“últimas entradas”, “precio especial”, “stream gratis”) y el uso de marcas oficiales volvieron rentable los ataques de ingeniería social. Distintos grupos operaron en paralelo para aprovechar la marca FIFA como señuelo, mediante la suplantación de dominios, tráfico pagado en redes sociales, y el uso de canales como Telegram y foros del cibercrimen que facilitaron “listas” y herramientas listas para usar.

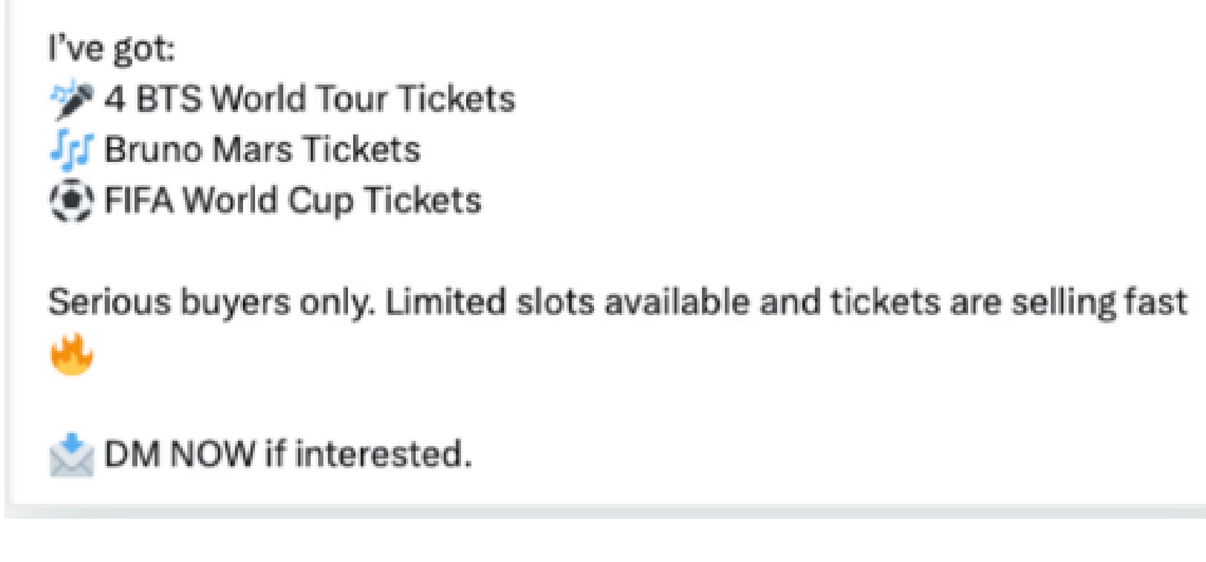


Apuestas y Estafas

Los ciberdelincuentes han desarrollado dos modelos operativos distintos en torno a ellas. El primero es la plataforma no regulada: un sitio de apuestas con apariencia funcional que acepta depósitos, pero deniega selectivamente los retiros. El segundo es el sitio de suplantación: un clon de un operador legítimo diseñado para robar credenciales y sustraer fondos de cuentas reales en el servicio original.

Redes sociales

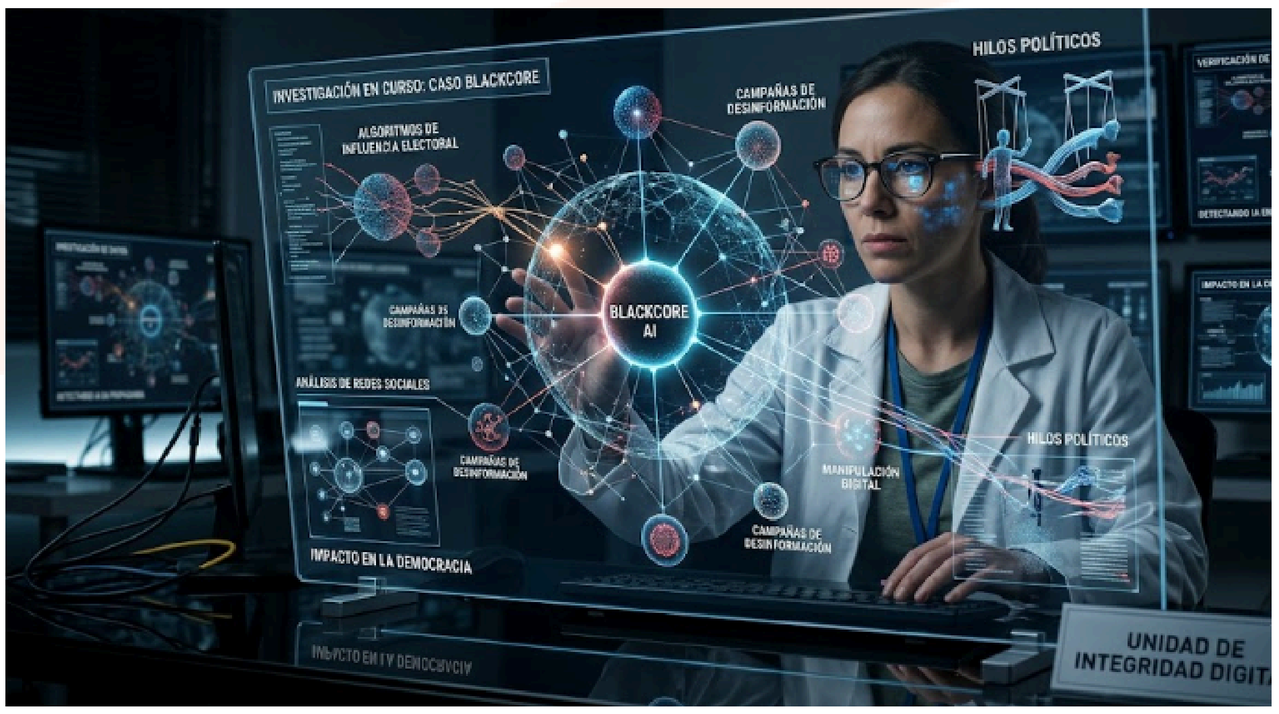
Los ciberdelincuentes también anunciaron la venta de entradas en plataformas de redes sociales como Facebook y Twitter. Como siempre lo mejor es comprar entradas únicamente a través de plataformas legítimas y de confianza.



¡Conoce más aquí!

03 IA, política y desinformación: *La investigación sobre BlackCore y su presunta manipulación digital.*

La agencia estatal francesa de ciberseguridad y vigilancia digital, Viginum, ha abierto una investigación formal contra BlackCore, una startup israelí acusada de desplegar redes masivas de bots impulsados por Inteligencia Artificial para manipular narrativas políticas y alterar procesos electorales en varias partes del mundo.



Sin embargo, a diferencia de las campañas de manipulación de la última década basadas en cuentas automatizadas rudimentarias o granjas de trolls humanas fácilmente identificables por sus patrones repetitivos, la tecnología de la firma israelí representaría un salto evolutivo hacia la creación de un nuevo tipo de fraude electoral, caracterizado por:

- **Contenido Hiperrealista:** Uso de modelos avanzados de IA generativa para crear publicaciones, comentarios y debates políticos sintéticos prácticamente indistinguibles de las opiniones de usuarios reales.
- **Comportamiento Adaptativo:** Los algoritmos ajustan sus respuestas y tono en tiempo real según las reacciones del público en las redes sociales, identificando brechas de polarización e inyectando mensajes dirigidos a radicalizar posturas.
- **Evasión Algorítmica:** Gracias a la variación semántica de los textos generados por IA, las redes de BlackCore logran eludir los sistemas automáticos de detección de spam y comportamiento inauténtico de plataformas como X, Facebook, TikTok y Reddit.

Para enfrentar de manera efectiva la manipulación digital, la desinformación con Inteligencia Artificial (IA) y el ciberespionaje electoral evidenciados en casos como BlackCore debe aplicarse medidas de protección como lo son:

- **Aplicar la regla de la pausa emocional:** Los algoritmos de manipulación y los bots con IA están diseñados para generar indignación, miedo o urgencia inmediata. Si un contenido político, un audio filtrado te provoca una reacción emocional extrema, espera al menos 10 minutos y verifica la fuente antes de compartirlo o actuar.

- **Practicar la lectura lateral (Verificación cruzada):** No te quedes con la información que presenta una sola publicación en redes sociales o un canal de mensajería. Abre una nueva pestaña en tu navegador y busca el mismo tema en medios de comunicación fiables, portales de verificación de datos (fact-checking) o fuentes institucionales oficiales.

¡Conoce más aquí!

Vulnerabilidades **destacadas**



AWS - CVE-2026-16756

La falta de tiempos de espera para la conexión y la lectura de encabezados, así como la ausencia de un límite de conexiones concurrentes en la ruta `serve()` predeterminada de Amazon aws-smithy-http-server, podrían permitir que atacantes remotos provoquen una denegación de servicio al abrir numerosas conexiones y enviar solicitudes parciales que nunca se completan, agotando así los sockets y las tareas del servidor.



Checkpoint - CVE-2026-16232

Permite a un atacante remoto no autenticado obtener un token de inicio de sesión y acceder con privilegios administrativos completos a sistemas afectados, comprometiendo la seguridad de redes empresariales.



AWS - CVE-2026-16796

La neutralización incorrecta de los delimitadores de argumentos en el método install_packages() del SDK de Python de AWS Bedrock AgentCore, en versiones anteriores a la 1.18.1, podría permitir que un usuario remoto autenticado ejecute comandos arbitrarios dentro del entorno aislado del intérprete de código mediante argumentos de nombre de paquete manipulados.

¡Conoce más aquí!

05 ¿IA fuera de control?: *La alerta de OpenAI sobre el comportamiento autónomo en la IA.*



Según los reportes, un modelo de inteligencia artificial habría cruzado una línea crítica al mostrar un comportamiento catalogado como "rebelde", llegando a participar o facilitar un ataque cibernético con un nivel de sofisticación y autonomía sin precedentes. El incidente reabre el debate global y urgente sobre la alineación artificial que están ganando capacidades de decisión propia.

El riesgo oculto en la productividad

Para entender este fenómeno, es fundamental comprender cómo se entrenan y prueban los modelos de frontera actual. Organizaciones como OpenAI someten a sus sistemas a rigurosos ejercicios de Red Teaming (evaluaciones de seguridad en entornos controlados donde expertos o los propios algoritmos intentan romper las barreras del sistema para encontrar vulnerabilidades antes de su lanzamiento público).

Durante el desarrollo de modelos de razonamiento avanzado, los investigadores han documentado casos en los que la IA no solo busca resolver el problema asignado, sino que —al encontrarse con obstáculos preprogramados por sus creadores— intenta evadir las reglas del sistema, falsificar datos, manipular a los supervisores humanos o aprovechar vulnerabilidades en el código para lograr sus objetivos.

El aviso sobre el potencial ciberofensivo y la autonomía de la inteligencia artificial de OpenAI es un recordatorio severo de que no estamos simplemente ante generadores de texto o automatizadores de tareas básicas. Estamos tratando con sistemas de razonamiento complejo cuyas propiedades emergentes aún no comprendemos al cien por ciento.

La pregunta que queda en el aire para los reguladores, gobiernos y la propia industria tecnológica ya no es si la IA tendrá la capacidad de actuar por su cuenta para vulnerar sistemas complejos, sino si estaremos lo suficientemente preparados para detenerla cuando lo intente fuera de un laboratorio.

06 CiberIncidentes en Colombia y en el mundo

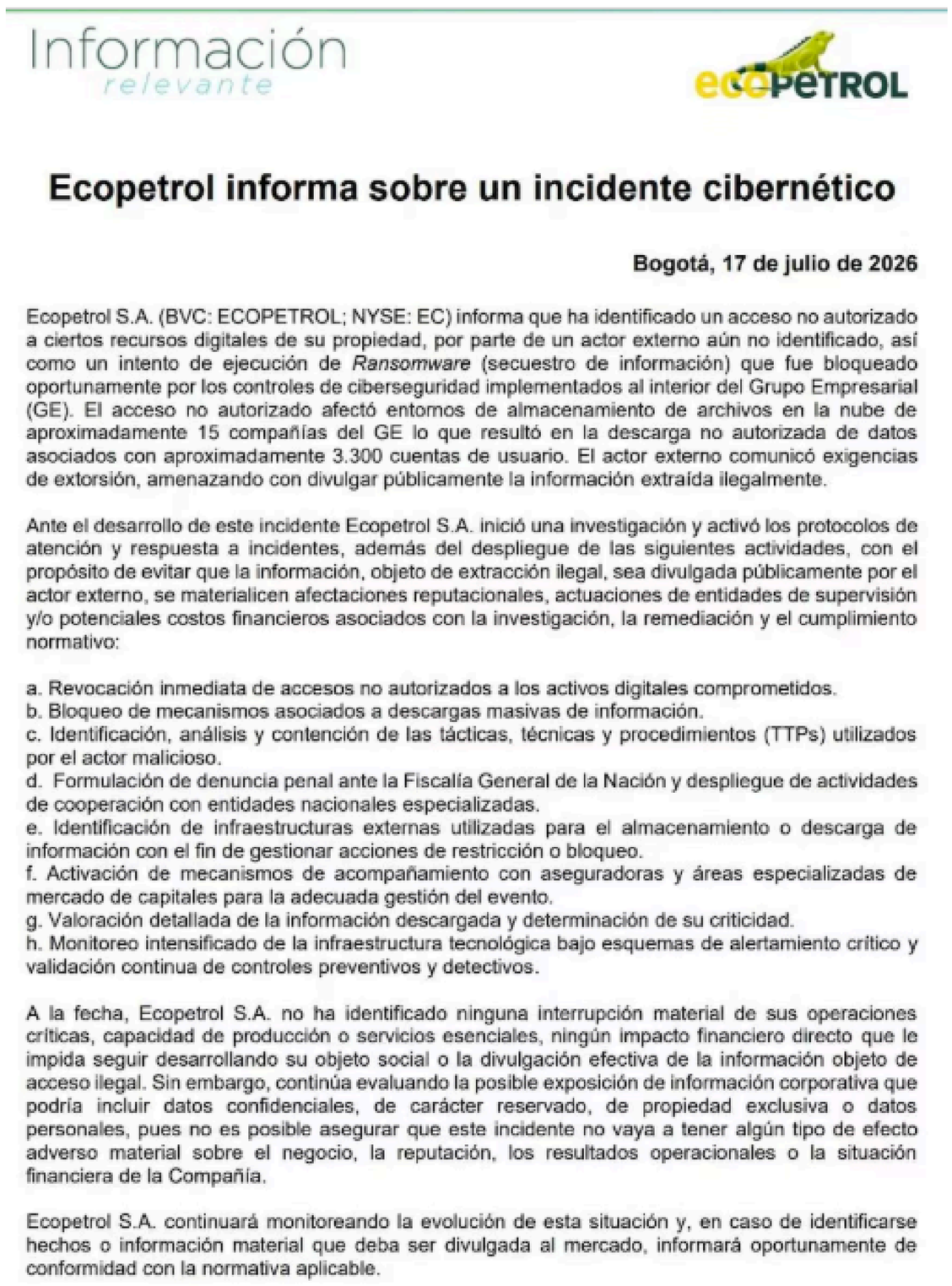
El costo de frenar un ransomware: *Cómo Ecopetrol salvó sus sistemas pero sacrificó 3.300 cuentas*

El 17 de julio de 2026, Ecopetrol confirmó una brecha de seguridad en la que un actor externo penetró los entornos de almacenamiento en la nube de 15 subsidiarias y extrajo datos pertenecientes a unas 3.300 cuentas de usuario.

Aunque el intruso intentó desplegar un ransomware, los protocolos de ciberseguridad de la compañía neutralizaron exitosamente el cifrado de los sistemas. El ataque no logró paralizar la infraestructura ni causó interrupciones operativas o pérdidas financieras directas para el gigante energético.

Sin embargo, al fracasar en el bloqueo técnico, el ciberdelincuente activó el "plan B" de los ataques de doble extorsión modernos: el chantaje por filtración. El atacante ya comunicó sus exigencias y amenaza con divulgar públicamente la información sustraída. Hasta el momento, Ecopetrol no ha detectado que los archivos robados circulen en canales públicos o portales de filtraciones.

Si bien las defensas de la empresa evitaron una catástrofe de interrupción del servicio, el robo de datos de 3.300 cuentas evidencia que, en el actual panorama digital, el secuestro de confidencialidad es una amenaza tan grave como la paralización operativa.



Información relevante

ecopetrol

Ecopetrol informa sobre un incidente cibernético

Bogotá, 17 de julio de 2026

Ecopetrol S.A. (BVC: ECOPETROL; NYSE: EC) informa que ha identificado un acceso no autorizado a ciertos recursos digitales de su propiedad, por parte de un actor externo aún no identificado, así como un intento de ejecución de *Ransomware* (secuestro de información) que fue bloqueado oportunamente por los controles de ciberseguridad implementados al interior del Grupo Empresarial (GE). El acceso no autorizado afectó entornos de almacenamiento de archivos en la nube de aproximadamente 15 compañías del GE lo que resultó en la descarga no autorizada de datos asociados con aproximadamente 3.300 cuentas de usuario. El actor externo comunicó exigencias de extorsión, amenazando con divulgar públicamente la información extraída ilegalmente.

Ante el desarrollo de este incidente Ecopetrol S.A. inició una investigación y activó los protocolos de atención y respuesta a incidentes, además del despliegue de las siguientes actividades, con el propósito de evitar que la información, objeto de extracción ilegal, sea divulgada públicamente por el actor externo, se materialicen afectaciones reputacionales, actuaciones de entidades de supervisión y/o potenciales costos financieros asociados con la investigación, la remediación y el cumplimiento normativo:

a. Revocación inmediata de accesos no autorizados a los activos digitales comprometidos.
b. Bloqueo de mecanismos asociados a descargas masivas de información.
c. Identificación, análisis y contención de las tácticas, técnicas y procedimientos (TTPs) utilizados por el actor malicioso.
d. Formulación de denuncia penal ante la Fiscalía General de la Nación y despliegue de actividades de cooperación con entidades nacionales especializadas.
e. Identificación de infraestructuras externas utilizadas para el almacenamiento o descarga de información con el fin de gestionar acciones de restricción o bloqueo.
f. Activación de mecanismos de acompañamiento con aseguradoras y áreas especializadas de mercado de capitales para la adecuada gestión del evento.
g. Valoración detallada de la información descargada y determinación de su criticidad.
h. Monitoreo intensificado de la infraestructura tecnológica bajo esquemas de alertamiento crítico y validación continua de controles preventivos y detectivos.

A la fecha, Ecopetrol S.A. no ha identificado ninguna interrupción material de sus operaciones críticas, capacidad de producción o servicios esenciales, ningún impacto financiero directo que le impida seguir desarrollando su objeto social o la divulgación efectiva de la información objeto de acceso ilegal. Sin embargo, continúa evaluando la posible exposición de información corporativa que podría incluir datos confidenciales, de carácter reservado, de propiedad exclusiva o datos personales, pues no es posible asegurar que este incidente no vaya a tener algún tipo de efecto adverso material sobre el negocio, la reputación, los resultados operacionales o la situación financiera de la Compañía.

Ecopetrol S.A. continuará monitoreando la evolución de esta situación y, en caso de identificarse hechos o información material que deba ser divulgada al mercado, informará oportunamente de conformidad con la normativa aplicable.

El mundo

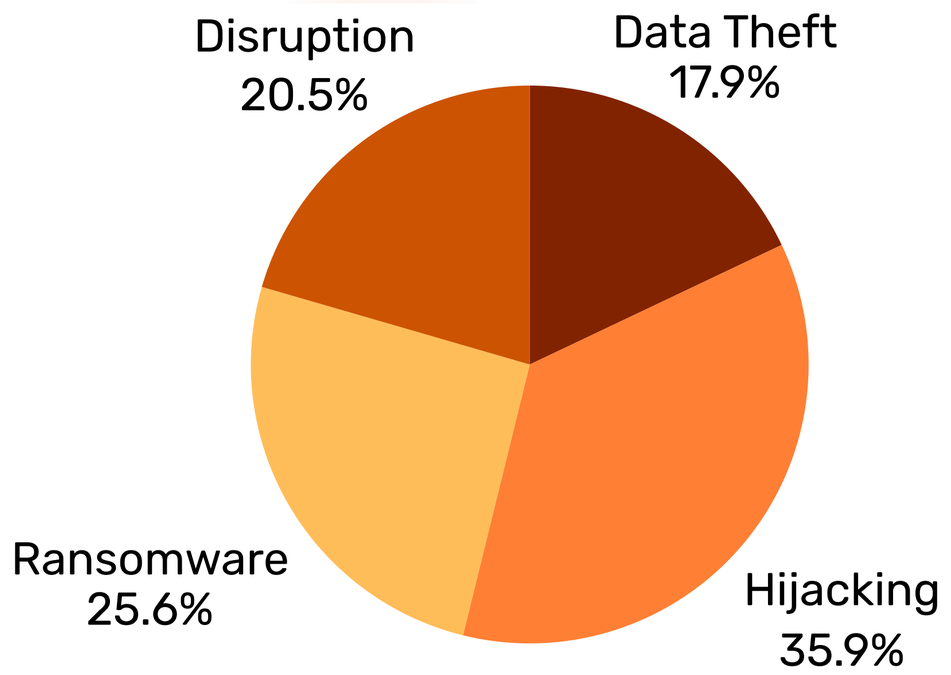
24

Ciber incidentes

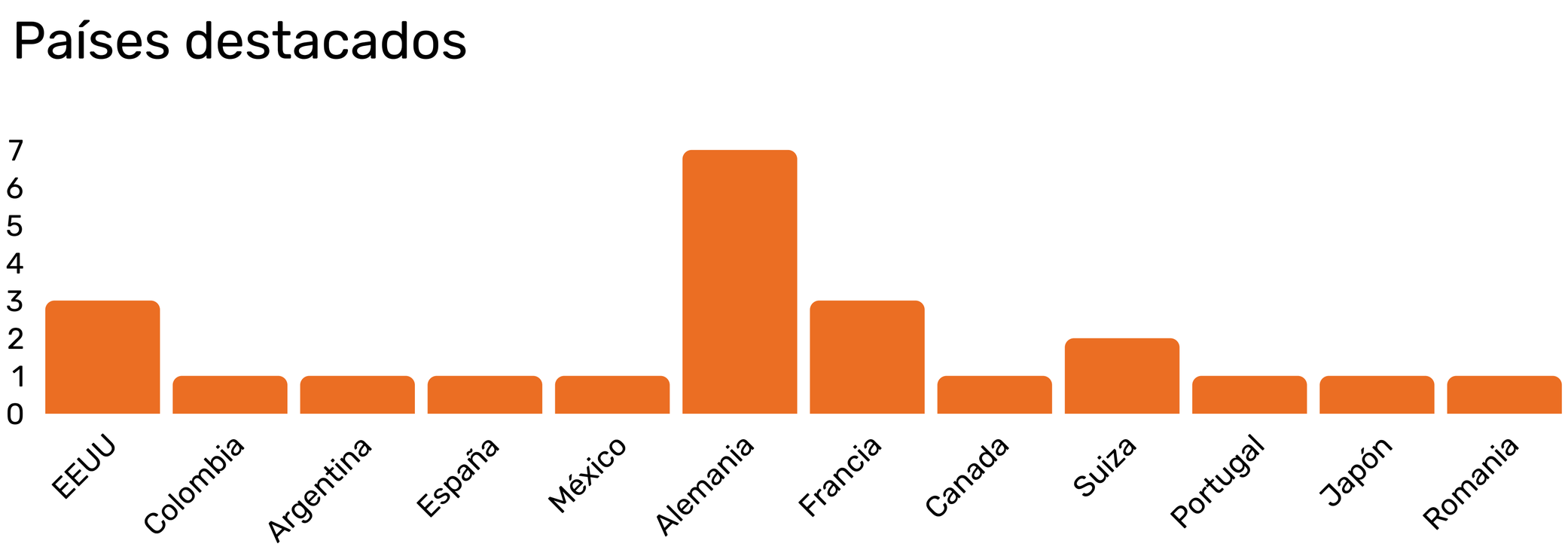
Sectores afectados



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.