Edición 22 -Mayo 2026

# Ciber E-dea

## Revista de Ciberseguridad

e-dea NETWORKS | CYBER SECURITY

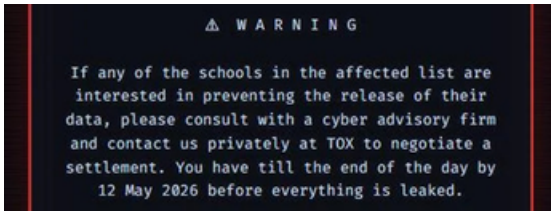
# 01 **Interrupción de Canvas,** afectaciones y filtraciones de datos advierte **ShinyHunters**

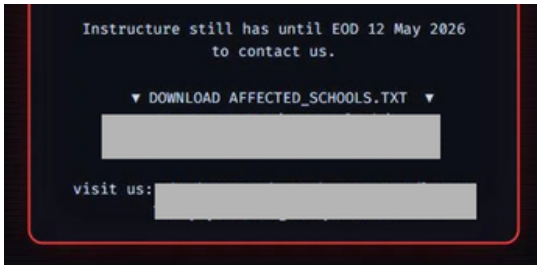
Recientemente la plataforma educativa Canvas, desarrollada por Instructure. Se encuentra en una creciente exposición a ciberataques. Dado que las universidades y centros educativos dependen de sistemas centralizados para gestionar clases, evaluaciones y comunicaciones, lo que los convierte atractivo a grupos de ciberdelincuencia.


## El grupo de hackers ShinyHunters

Se atribuyó el ataque a Canvas, siguiendo una línea de operaciones previas enfocadas en la exfiltración y extorsión de datos. Probocando una interrupción del servicio, generando fallos en el acceso y caídas del sistema en miles de instituciones alrededor del mundo, además de la aparición de mensajes en páginas de inicio de sesión donde los atacantes reclamaban la intrusión y amenazaban con filtrar información si no se iniciaban negociaciones.

La compañía confirmó posteriormente que logró restablecer el servicio y señaló que el origen del problema estaría relacionado con una vulnerabilidad en el entorno de soporte denominado "Free for Teacher". Como consecuencia, varias instituciones se vieron obligadas a suspender evaluaciones, extender plazos de entrega y recurrir a canales alternativos como el correo electrónico u otras plataformas digitales para mantener la continuidad académica.



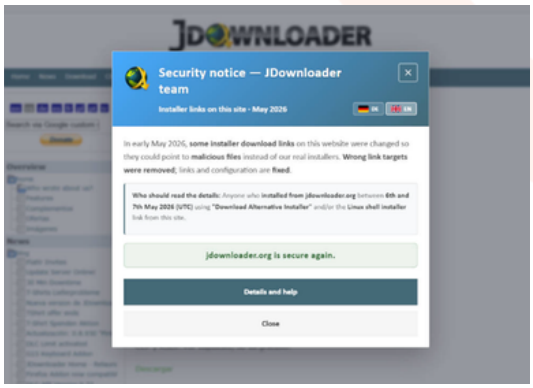




En cuanto a los datos potencialmente comprometidos, los reportes indican que podrían haberse expuesto nombres, direcciones de correo electrónico, identificadores de estudiantes y mensajes internos dentro de la plataforma.

No obstante, Instructure aseguró que no existe evidencia de que contraseñas, datos financieros o documentos de identificación gubernamental hayan sido afectados. Aun así, algunas de las cifras y afirmaciones difundidas por ShinyHunters no han sido verificadas, por lo que el alcance real del incidente continúa bajo evaluación.

¡Conoce más aquí!

# 02 **Alerta de Seguridad:** sitio oficial de JDownloader distribuía malware para **Windows y Linux**




El sitio oficial de JDownloader, uno de los gestores de descargas de código abierto más populares, fue comprometido para distribuir instaladores maliciosos entre el 6 y el 7 de mayo de 2026, atacantes lograron suplantar los archivos legítimos con troyanos de acceso remoto (RAT) diseñados para tomar el control total de los equipos infectados.

## ¿Qué sucedió exactamente?

Los atacantes explotaron una vulnerabilidad no parcheada en el Sistema de Gestión de Contenidos (CMS) del sitio web jdownloader.org. Aunque no lograron acceso total al servidor ni al sistema operativo subyacente, sí consiguieron modificar las Listas de Control de Acceso (ACL) y el contenido de las páginas de descarga.
Esto les permitió redirigir los enlaces de descarga hacia servidores externos controlados por ellos, donde alojaron versiones modificadas de los instaladores que incluían código malicioso.

## Medidas de respuesta y recomendaciones

JDownloader confirmaron la brecha y cerraron temporalmente el sitio para investigar y restaurar la seguridad. El portal ya ha sido asegurado, pero los usuarios que descargaron el software deben actuar de inmediato ya que el malware permite la ejecución de código arbitrario y tiene capacidades de persistencia.

Los expertos en ciberseguridad recomiendan:

- Reinstalar el sistema operativo: Es la única forma segura de garantizar que no queden restos del troyano.
- Cambiar contraseñas: Una vez limpio el sistema, cambia todas tus contraseñas, especialmente las de servicios bancarios, correos y redes sociales.
- Escanear con antivirus: Utiliza herramientas de seguridad actualizadas para detectar posibles copias del malware en otros discos

## Versiones afectadas

No todos los usuarios de JDownloader se vieron comprometidos.

El ataque fue selectivo y afectó específicamente a:

- Windows: Solo el enlace de "Alternative Installer" (Instalador Alternativo). El instalador estándar y las actualizaciones dentro de la aplicación se mantuvieron seguros.
- Linux: El instalador de shell (.sh) fue modificado para inyectar binarios maliciosos ofuscados que establecen persistencia en el sistema.

¡Conoce más aquí!

# 03 5 habilidades para alcanzar una carrera exitosa en Seguridad

Según Mary Gates que pasó décadas en el "top" de la seguridad corporativa en (JP Morgan) se dio cuenta que muchas empresas estaban perdidas, comprando cámaras y alarmas, sin dar importancia a la esencia de la seguridad. Su filosofía es simple: la seguridad debe facilitar el trabajo, no hacerlo más difícil. Además, manifiesta 5 habilidades que, según ella, harán a un crack en el mundo de la seguridad:

### 1. Saber dónde poner las fichas (Gestión de Riesgos)

En seguridad, intentar proteger todo es como no proteger nada. Si gastas el mismo presupuesto en cuidar la papelería que en proteger la base de datos de los clientes, estás mal

### 2. No perder la cabeza cuando todo explota (Liderazgo en Crisis)

Cualquiera es buen jefe cuando no pasa nada, pero el verdadero líder de seguridad se ve cuando hay un hackeo o una emergencia.

### 3. Hablar "negocio", no solo "cables" (Comunicación e Influencia)

A los directivos no les importan los tecnicismos; les importa la rentabilidad. Si no sabes explicar por qué una inversión es necesaria en un lenguaje que ellos entiendan, no te van a dar ni un centavo.

### 4. Ser parte del equipo, no el policía pesado (Alineación Empresarial)

Seguridad tiene que llevarse bien con todos: TI, Recursos Humanos, Legal y Ventas. Si pones protocolos que hacen que trabajar sea una tortura, los empleados van a buscar la forma de saltárselos.

### 5. Saber que lo más importante es la gente (Gestión de Personas)

Puede tener el mejor software del mundo, pero si su equipo está agotado, mal pagado o no sabe qué hacer, vas a fallar.

¡Conoce más aquí!

# Vulnerabilidades **destacadas**


## Microsoft

**CVE-2026-42834**

Una resolución incorrecta de enlaces antes del acceso a archivos, también conocida como seguimiento de enlaces, en el Centro de administración de Windows del portal de Azure. Esta debilidad permite que un usuario autorizado ejecute operaciones con privilegios superiores a los previstos


## Kernel de Linux

**CVE-2026-31417**

el subsistema de red X25 del kernel de Linux, es un desbordamiento de enteros que ocurre cuando el kernel acumula fragmentos de paquetes. un atacante podría forzar al kernel a interpretar erróneamente los tamaños o índices de los paquetes, lo que provocaría corrupción de memoria o una denegación de servicio


## GitHub

**CVE-2026-29783**

La herramienta de shell en las versiones de GitHub Copilot CLI anteriores a la 0.0.422 inclusive permite la ejecución de código arbitrario mediante patrones de expansión de parámetros bash manipulados. Un atacante que pueda influir en el texto del comando enviado a la herramienta de shell (por ejemplo, mediante la inyección de prompts a través de contenido malicioso del repositorio

**¡Conoce más aquí!**

# 05 **CiberIncidentes en Colombia** y en el mundo

## Colombia ocupa el tercer lugar en ciberataques

Colombia es el tercer país más ciberatacado de Latinoamérica con 10,9 billones de intentos de ciberataques registrados en 2025, según FortiGuard Labs. Los sectores críticos —energía, agua, salud, finanzas y telecomunicaciones— están bajo una presión sin precedentes. Los ciberdelincuentes atacan con precisión quirúrgica: escanean, identifican y explotan las vulnerabilidades. La inteligencia artificial juega en ambos bandos: los criminales atacan con mayor eficiencia (menos intentos, más daño), mientras que las organizaciones que la adoptan pueden anticipar y responder en tiempo real.

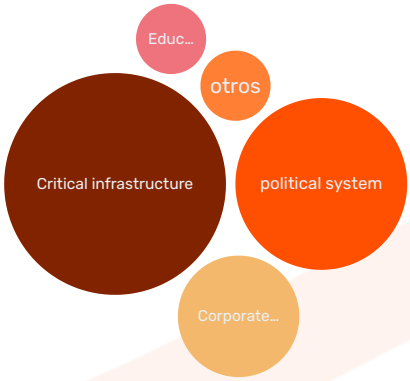
## están estafando con el álbum del Mundial 2026 en Colombia


Las estafas con el álbum del Mundial 2026 en Colombia están en aumento. Un informe reciente de Kaspersky advierte que delincuentes están utilizando WhatsApp e Instagram para ofrecer álbumes y stickers falsos, engañando a compradores en el país.

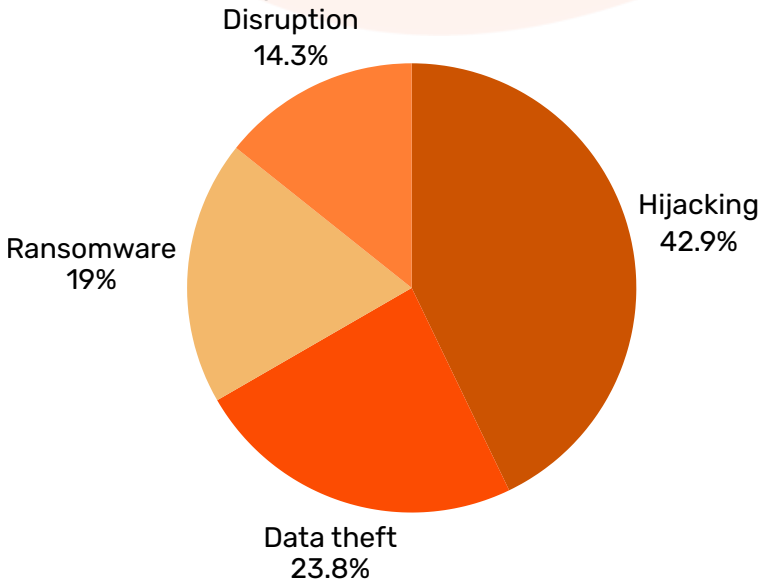
El proceso de compra es similar al de cualquier tienda real, lo que reduce las sospechas. Una vez se realiza el pago, los recursos se transfieren a cuentas intermediarias, muchas veces vinculadas a plataformas fintech, y luego se distribuyen entre varias cuentas para evitar rastreo.

# El mundo

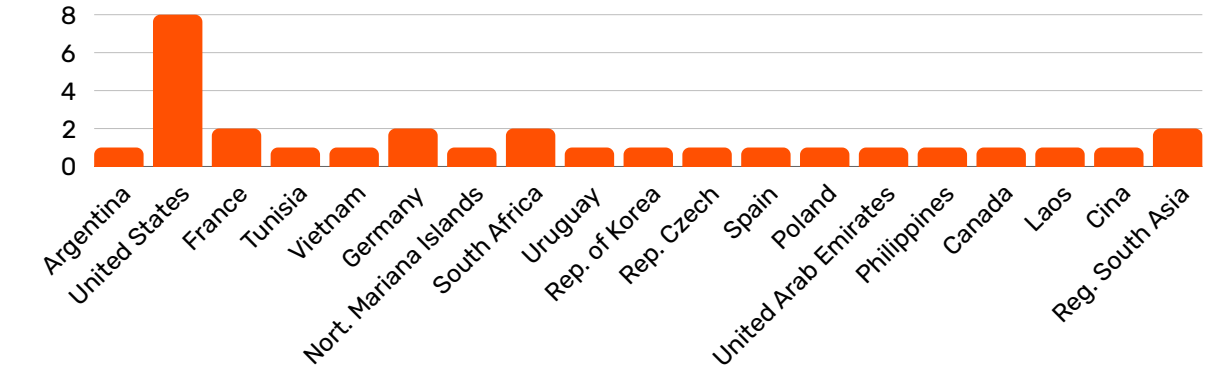

## Sectores afectados




## Tipo de incidente




## Países destacados




¡Conoce más aquí!

# 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