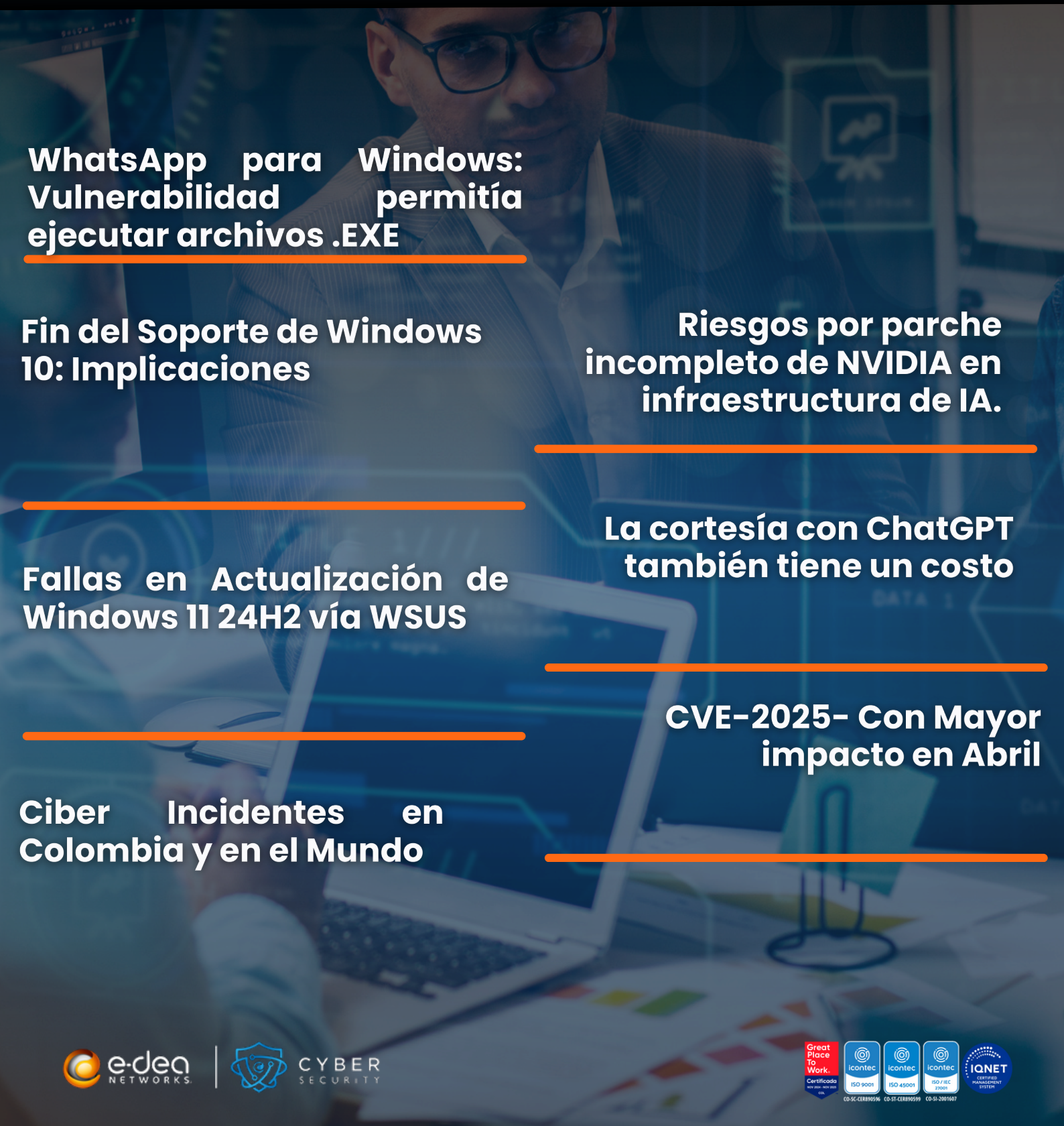
CIBER E-DEA

Boletín de Seguridad



WhatsApp para Windows: Vulnerabilidad permitía ejecutar archivos .EXE

Fin del Soporte de Windows 10: Implicaciones

Riesgos por parche incompleto de NVIDIA en infraestructura de IA.

Fallas en Actualización de Windows 11 24H2 vía WSUS

La cortesía con ChatGPT también tiene un costo

Ciber Incidentes en Colombia y en el Mundo

CVE-2025- Con Mayor impacto en Abril

WhatsApp para Windows: una vulnerabilidad permitía ejecutar archivos .EXE disfrazados de imágenes

Una reciente vulnerabilidad de seguridad descubierta en WhatsApp para Windows ha encendido las alarmas sobre la posibilidad de que los usuarios ejecuten código malicioso sin saberlo.

El fallo, identificado como CVE-2025-30401, afecta a todas las versiones del cliente de escritorio anteriores a la 2.2450.6, y podría haber sido explotado por atacantes para disfrazar archivos ejecutables como imágenes aparentemente inofensivas.

El problema radica en la discrepancia entre el tipo MIME —los metadatos que definen el tipo de archivo que se muestra al usuario— y la extensión real del archivo, que es la que la aplicación usa finalmente al abrirlo. Así, un archivo con tipo MIME "imagen/jpeg" pero extensión .EXE podría abrirse y ejecutarse como un programa si el usuario hace clic sobre él dentro de la aplicación de escritorio.

A diferencia de otros vectores de ataque más complejos, esta vulnerabilidad depende de la acción del usuario: requiere que la víctima abra manualmente el archivo. Sin embargo, la interfaz de WhatsApp no mostraba ninguna señal de alerta, ya que el archivo aparecía como si fuera una imagen legítima.

Recomendación: actualizar de inmediato

El fallo, identificado como CVE-2025-30401, afecta a todas las versiones del cliente de escritorio anteriores a la 2.2450.6, y podría haber sido explotado por atacantes para disfrazar archivos ejecutables como imágenes aparentemente inofensivas.

Último Capítulo de Windows 10: Fin del Soporte y sus Implicaciones

Desde el 14 de octubre de 2025, el soporte para Windows 10 dejará de existir.
El fin del soporte de Windows 10 significa que Microsoft dejará de proporcionar cualquier tipo de actualización para este sistema operativo. Actualmente, aunque Windows 10 no recibe nuevas características, sí obtiene actualizaciones de seguridad. Al terminar el soporte, ya no se tendrá:

- Riesgo incrementado: Los cibercriminales podrían aprovechar vulnerabilidades no corregidas.
- Compatibilidad con aplicaciones y hardware: Con el tiempo, las nuevas aplicaciones y el hardware dejarán de ser compatibles lo que hará su uso cada vez más limitado y problemático.
- Actualizaciones de seguridad: Cualquier vulnerabilidad descubierta después de la fecha final no será corregida, dejando el sistema operativo expuesto a posibles ataques.

Alternativas disponibles si aún utilizas Windows 10

La primera opción es actualizar a Windows 11, siempre y cuando se disponga de un equipo compatible a esta versión.

No obstante, existen otras alternativas, tales como:
Migrar a Linux
Migrar a macOS
Utilizar Windows IoT LTSC.

La excepción: versiones con soporte extendido

No todas las versiones de Windows 10 perderán soporte al mismo tiempo. Existen ediciones específicas diseñadas para sectores con necesidades particulares, como las versiones Long-Term Servicing Channel (LTSC).

Para los usuarios que ya cuentan con una licencia LTSC, no hay costos adicionales asociados al soporte extendido, ya que esto forma parte del paquete original.

Más información

Riesgos por parche incompleto de NVIDIA en infraestructura de IA

ETrend Micro descubrió que un parche de seguridad de NVIDIA lanzado en septiembre de 2024 para la vulnerabilidad CVE-2024-0132 es incompleto, lo que deja expuestos a los sistemas que usan el NVIDIA Container Toolkit a ataques de escape de contenedores. Además, se identificó una vulnerabilidad de denegación de servicio (DoS) en Docker sobre Linux.

Identificación CVE	Vector	Puntuación base	Gravedad	CWE
CVE-2024-0132	AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	9	Critico	CWE 367
Descripcion				
NVIDIA Container Toolkit 1.16.1 o versiones anteriores contiene una vulnerabilidad de tiempo de verificación y tiempo de uso (TOCTOU) al usarse con la configuración predeterminada, donde una imagen de contenedor diseñada específicamente puede acceder al sistema de archivos del host. Esto no afecta los casos de uso donde se utiliza CDI. Una explotación exitosa de esta vulnerabilidad puede provocar ejecución de código, denegación de servicio, escalada de privilegios, divulgación de información y manipulación de datos.				
Impactos				
Ejecución de código, denegación de servicio, escalada de privilegios, divulgación de información, manipulación de datos				

Estas fallas podrían permitir a atacantes acceder a datos confidenciales, causar pérdidas de modelos de IA o generar interrupciones operativas. Se advierte que organizaciones con cargas de trabajo de IA, contenedores o entornos en la nube están especialmente en riesgo.

Identificación CVE	Vector	Puntuación base	Gravedad	CWE
CVE-2024-0133	AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:N	4.1	Medio	CWE 367
Impactos				
NVIDIA Container Toolkit 1.16.1 o versiones anteriores contiene una vulnerabilidad en el modo de operación predeterminado que permite que una imagen de contenedor especialmente diseñada cree archivos vacíos en el sistema de archivos del host. Esto no afecta a los casos de uso donde se utiliza CDI. Una explotación exitosa de esta vulnerabilidad podría provocar la manipulación de datos.				
Impactos				
Manipulación de datos				

Expertos como Thomas Richards y Jason Soroko advierten sobre la necesidad urgente de:

- Aplicar parches adecuados,
- Verificar la integridad de las mitigaciones,
- Reforzar la segmentación de sistemas y la detección de intrusos,
- Y mantener comunicación activa con proveedores.

La situación subraya la importancia de adoptar una postura de ciberseguridad proactiva, especialmente en sectores que dependen de la infraestructura NVIDIA para IA.

Más información

Fallas en la Actualización de Windows 11 24H2 a través de WSUS tras parches de Abril

Microsoft ha reconocido un problema que afecta a entornos empresariales que utilizan Windows Server Update Services (WSUS) para distribuir actualizaciones.

Luego de aplicar las actualizaciones de seguridad publicadas el 8 de abril de 2025 (como la KB5055528), los dispositivos con Windows 11 22H2 o 23H2 no logran actualizar a la versión 24H2, generando el error 0x80240069.

El Impacto que se evidenciaría

Este fallo impide que se inicie o complete la descarga de la nueva versión, y los registros pueden reflejar mensajes como "El servicio wuauserv se ha detenido inesperadamente".

Microsoft confirmó el incidente tras numerosos reportes en foros comunitarios y aclaró que los usuarios domésticos no se ven afectados, dado que WSUS es una herramienta utilizada principalmente en entornos corporativos. Se recomienda a los administradores de TI mantenerse atentos a futuras actualizaciones correctivas por parte de Microsoft

Más información

La cortesía con ChatGPT también tiene un costo

Decir “por favor” o “gracias” a ChatGPT puede parecer un gesto inofensivo, pero según Sam Altman, CEO de OpenAI, estas amables palabras cuestan millones en electricidad.

Cada consulta enviada a la IA consume energía.

Se estima que una sola pregunta usa 0,3 vatios-hora. Multiplicado por cientos de millones de usuarios semanales, el gasto energético anual supera los 1.000 gigavatios-hora, similar al consumo de ciudades enteras. Además, también se requiere agua para refrigerar los servidores: hasta 2 litros por cada 10 a 50 consultas.

Aunque Altman lo comentó en tono ligero, el mensaje es claro: la tecnología no es gratuita para el planeta.

Aun así, los expertos recomiendan mantener mensajes claros y bien redactados —incluso con cortesía— ya que suelen generar mejores respuestas. En un mundo cada vez más digital, ser consciente del impacto de cada interacción también es parte de nuestra responsabilidad.

Más información

Vulnerabilidades críticas (CVE)

CVE, al ser gestionadas adecuadamente, contribuyeron significativamente a la protección de sistemas y datos frente a amenazas cibernéticas. A continuación, se destacan cinco de las más relevantes:

1. CVE-2025-29824 (Windows CLFS)

Elevación de privilegios explotada en campañas de ransomware.
Recomendación: Aplicar parche de seguridad de Microsoft.

2. CVE-2025-24054 (NTLM – Windows)

Suplantación de identidad mediante archivos .library-ms.
Recomendación: Deshabilitar NTLM y actualizar sistemas

3. CVE-2025-26670 / CVE-2025-26663 (LDAP – Windows:

Ejecución remota de código sin autenticación.
Recomendación: Actualizar sistemas afectados.

4. CVE-2025-22457 (Ivanti Connect Secure)

Ataques activos APT con ejecución remota de código.
Recomendación: Actualizar firmware y verificar integridad.

5. CVE-2025-21204 (Windows Update):

Escalada de privilegios a través de enlaces simbólicos.
Recomendación: No eliminar carpeta inetpub y aplicar parche KB5055523

Recomendación general: Manténga tus sistemas actualizados, aplica principios de mínimo privilegio y monitorea continuamente posibles amenazas

Ciber incidentes en Colombia y en el mundo

Informe de inteligencia sobre amenazas - Aumento de Ransomware

Se observó un incremento del 126% en ataques de ransomware en comparación con el primer trimestre de 2024, con 2,289 víctimas identificadas por 74 grupos de ransomware. El grupo Cl0p lideró la actividad explotando vulnerabilidades de día cero en productos de transferencia de archivos Cleo, principalmente dirigidos a empresas de bienes de consumo en América del Norte .

Estos incidentes subrayan la importancia de fortalecer las estrategias de ciberseguridad, tanto a nivel organizacional como nacional, para enfrentar las amenazas emergentes en el entorno digital.

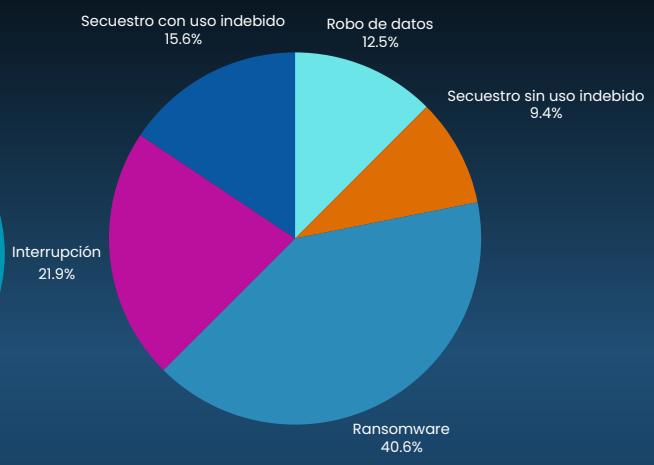
Más información

El mundo

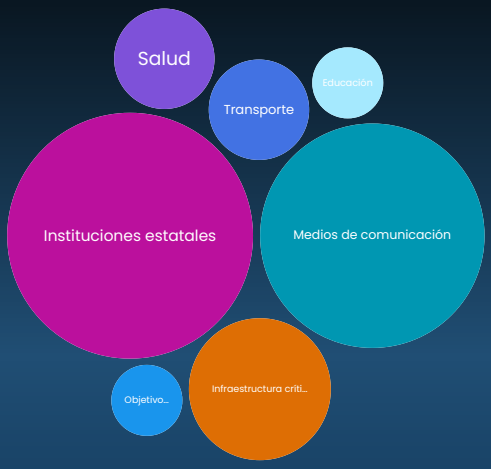
32

Ciber incidentes

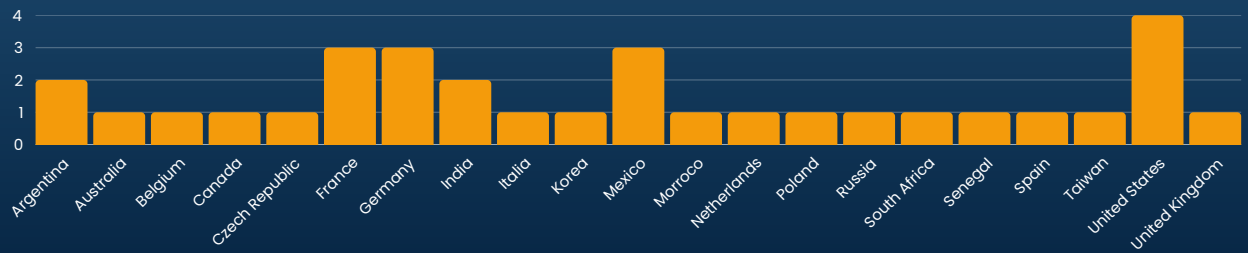
TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS



Más información

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

e-dea.co