Edición 25 - Agosto 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 25 - Agosto 2026

01 SharePoint bajo ataque: múltiples vulnerabilidades y una nueva amenaza crítica

02 La IA avanza más rápido que la regulación.

03 Vulnerabilidad crítica en VMware vCenter Server explotada activamente

04 Vulnerabilidades destacadas.

05 IA impulsa el riesgo cibernético y se convierte en una amenaza para la estabilidad financiera mundial

06 Ciber Incidentes en Colombia y en el mundo.

07 Contacto

01 SharePoint bajo ataque: múltiples vulnerabilidades y una nueva amenaza crítica

Panorama de la amenaza

Los servidores Microsoft SharePoint Server on-premises han sido objetivo de múltiples vulnerabilidades que han incrementado el riesgo de acceso no autorizado y compromiso de organizaciones a nivel global. Las fallas afectan principalmente a SharePoint Server 2016, 2019 y Subscription Edition, especialmente cuando los servidores están expuestos directamente a Internet.

Nueva amenaza: CVE-2026-55040

Una de las vulnerabilidades más relevantes es **CVE-2026-55040**, con una puntuación **CVSS de 9.1**, relacionada con un bypass de autenticación en el proceso de validación de **tokens JWT.**
Su explotación podría permitir a un atacante remoto evadir controles de seguridad, suplantar identidades y realizar acciones con privilegios elevados, sin necesidad de utilizar credenciales válidas.
La publicación de un Proof of Concept (PoC) incrementa el riesgo de explotación, especialmente para organizaciones que mantienen servidores vulnerables o expuestos a Internet.

Versiones afectadas

Vendor	Product	Default status	Versions		
Microsoft	Microsoft SharePoint Enterprise Server 2016	affected	**Version**	**Status**	**Constraints**
			16.0.0	affected	< 16.0.5561.1001
Microsoft	Microsoft SharePoint Server 2019	affected	**Version**	**Status**	**Constraints**
			16.0.0	affected	< 16.0.10417.20175
Microsoft	Microsoft SharePoint Server Subscription Edition	affected	**Version**	**Status**	**Constraints**
			16.0.0	affected	< 16.0.19725.20434

Acciones recomendadas

- Actualizar: Aplicar inmediatamente los parches de seguridad.
- Investigar: Revisar accesos anómalos y posibles compromisos previos.
- Reducir exposición: Evitar la exposición directa a Internet.
- Monitorear: Vigilar actividades administrativas sospechosas.

¡Conoce más aquí!

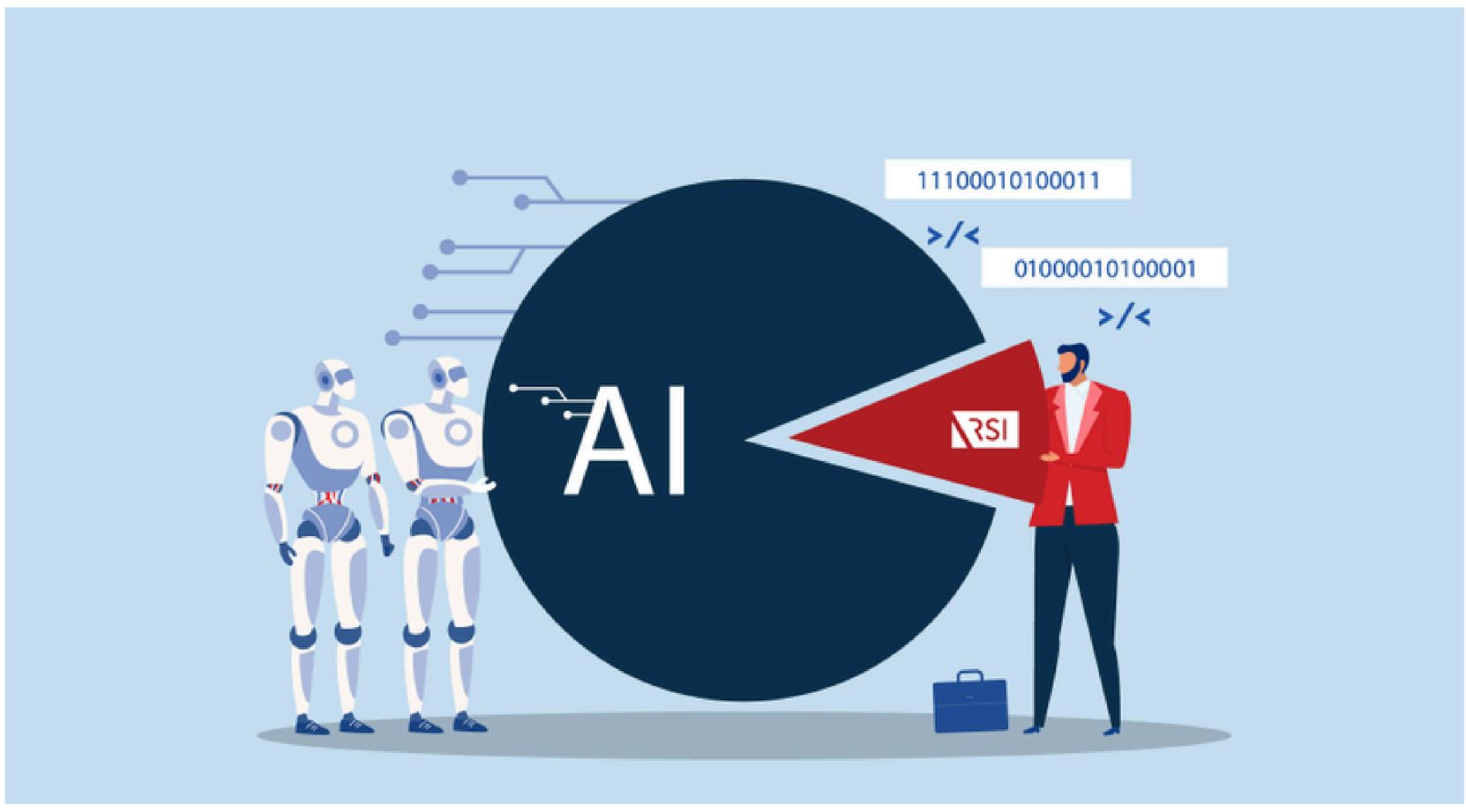
02 La IA avanza más rápido que la regulación.

Panorama de la amenaza

La rápida evolución de la Inteligencia Artificial está superando la capacidad de respuesta de los marcos regulatorios, generando una brecha de gobernanza que puede afectar la confianza entre empresas, clientes, socios y reguladores.
Aunque existen iniciativas como la Ley de IA de la Unión Europea e ISO/IEC 42001, el desafío va más allá del cumplimiento normativo. Un uso inadecuado de la IA puede afectar directamente la credibilidad, reputación y confianza en una organización.

La brecha entre innovación y confianza

El desafío no consiste únicamente en regular la Inteligencia Artificial, sino en garantizar que las organizaciones puedan demostrar que sus sistemas son seguros, transparentes y responsables.



La confianza como ventaja competitiva

La gobernanza y la seguridad no deben considerarse obstáculos para la innovación. Implementar una IA segura y responsable desde el diseño permite integrar principios como gobernanza, explicabilidad, trazabilidad y control de accesos desde las primeras etapas.
Las organizaciones capaces de demostrar un uso ético, seguro y transparente de la IA podrán fortalecer la confianza y convertir la responsabilidad en una ventaja competitiva.

¡Conoce más aquí!

03 Vulnerabilidad crítica en VMware vCenter Server explotada activamente

Los equipos de seguridad e infraestructura deben prestar especial atención a CVE-2026-59310, una vulnerabilidad crítica en VMware vCenter Server, plataforma utilizada para administrar entornos de virtualización.

Con una puntuación CVSS de 9.8/10 y reportes de explotación activa, la vulnerabilidad podría permitir la ejecución remota de código y facilitar el compromiso del servidor y otros componentes de la infraestructura virtualizada.

Impacto potencial

Un compromiso exitoso de vCenter Server podría permitir a un atacante:

- Ejecutar código o comandos no autorizados.
- Modificar configuraciones críticas.
- Establecer mecanismos de persistencia.
- Acceder a recursos de la infraestructura virtual.
- Realizar movimiento lateral hacia otros sistemas.
- Interrumpir servicios o desplegar malware y ransomware.

Debido a su función central dentro de los entornos virtualizados, el impacto de un compromiso puede extenderse más allá de un único servidor.



Acciones recomendadas

- Verificar: Identificar las versiones de vCenter Server.
- Validar: Confirmar la exposición a CVE-2026-59310.
- Actualizar: Aplicar prioritariamente las correcciones.
- Investigar: Revisar actividad anómala y cambios no autorizados.
- Monitorear: Reforzar la vigilancia desde el SOC/SIEM.

¡Conoce más aquí!

Vulnerabilidades **destacadas**



Linux Kernel- CVE-2026-53362

Esta vulnerabilidad afecta al kernel de Linux y está relacionada con un error en el manejo de datos dentro de la funcionalidad IPv6. El fallo puede permitir la corrupción de memoria y ser aprovechado para obtener privilegios elevados en el sistema. CISA la ha tratado como una vulnerabilidad de interés por existir evidencia de explotación.



Microsoft SharePoint - CVE-2026-63520

Esta vulnerabilidad está relacionada con Microsoft SharePoint Server y, dentro de los escenarios reportados, puede formar parte de una cadena de ataque utilizada para comprometer servidores empresariales. Por tratarse de infraestructura que normalmente almacena documentos e información corporativa, su impacto puede ser significativo.



Windows AFD.sys — CVE-2026-68820

Esta vulnerabilidad afecta al componente Windows Ancillary Function Driver for WinSock (AFD.sys) y corresponde a un fallo de tipo Use-After-Free. Un atacante autorizado con acceso local puede aprovecharla para realizar un escalamiento de privilegios y obtener mayor control sobre el sistema. CISA registra la explotación como activa.

¡Conoce más aquí!

05 IA impulsa el riesgo cibernético y se convierte en **una amenaza para la estabilidad financiera mundial**

El Financial Stability Board (FSB) advirtió que el uso de inteligencia artificial (IA) está incrementando de forma significativa el riesgo cibernético para el sistema financiero mundial. Según el organismo, la IA permite a los actores maliciosos automatizar y acelerar diferentes fases de un ataque, incluyendo reconocimiento, desarrollo de herramientas, explotación de vulnerabilidades y campañas de phishing, aumentando la velocidad y escala de las operaciones ofensivas.

El informe señala que la evolución de modelos de IA más avanzados puede reducir las barreras técnicas para ejecutar ataques sofisticados y facilitar campañas dirigidas contra bancos, proveedores tecnológicos, infraestructuras críticas y organizaciones que administran información sensible. Como consecuencia, el riesgo deja de ser únicamente operativo y pasa a considerarse un factor que podría afectar la estabilidad y confianza del sistema financiero globa



Impacto para las organizaciones

Las organizaciones deben considerar la IA como un multiplicador de capacidad ofensiva, más que como una amenaza aislada. Esto implica fortalecer la gestión de vulnerabilidades, reducir la superficie de exposición de servicios críticos, implementar autenticación multifactor resistente al phishing, proteger credenciales y secretos utilizados por agentes de IA, y mejorar las capacidades de detección y respuesta automatizada frente a amenazas impulsadas por IA.

06 Ataque de ransomware al Ministerio de Justicia de Colombia



Justicia

Comunicado del Ministerio de Justicia a la opinión pública

Bogotá, D. C., 3 de agosto de 2026.

El Ministerio de Justicia y del Derecho fue víctima de un ataque cibernético mediante un virus tipo ransomware, que comprometió parte de su infraestructura tecnológica y afectó la disponibilidad de algunos de sus servicios.

"Rechazo de manera categórica este ataque contra la infraestructura tecnológica del Estado y hago un llamado a la Fiscalía General de la Nación, a la Policía Nacional y a las demás autoridades competentes para que adelanten con la mayor celeridad las investigaciones que permitan esclarecer los hechos, identificar a los responsables y llevarlos ante la justicia" aseguró la ministra de Justicia (e) Cielo Rusinque.

Desde que se detectó el ataque, se activaron de manera inmediata los protocolos de ciberseguridad y contención, incluyendo el aislamiento preventivo de los sistemas comprometidos para evitar su propagación.

Actualmente, el Ministerio trabaja de manera articulada con el equipo especializado del Ministerio TIC y las demás autoridades competentes para contener el incidente, determinar su alcance, avanzar en la recuperación segura de los sistemas y restablecer gradualmente los servicios afectados.

Si bien ninguna organización está exenta de enfrentar este tipo de amenazas, el Ministerio contaba con mecanismos de seguridad y respuesta que fueron activados de manera inmediata para contener la situación y proteger la infraestructura tecnológica de la entidad.

"No cederemos ante este tipo de ataques y continuaremos fortaleciendo nuestras capacidades de ciberseguridad para proteger la información institucional, garantizar la continuidad de los servicios y reforzar nuestra infraestructura tecnológica", enfatizó la ministra Rusinque.

Mantendremos informada a la ciudadanía sobre la evolución de la situación a través de los canales oficiales del Ministerio.

El Ministerio de Justicia y del Derecho informó que fue víctima de un ataque cibernético mediante un virus tipo ransomware, ocurrido el 2 de agosto de 2026. De acuerdo con los hallazgos preliminares de COLCERT, el incidente afectó parte de la infraestructura tecnológica de la entidad y generó indisponibilidad de algunos servicios institucionales.

Tras detectar el incidente, el Ministerio activó sus protocolos de respuesta y contención, incluyendo el aislamiento preventivo de sistemas comprometidos para evitar la propagación de la amenaza y preservar evidencia digital.

COLCERT realizó una inspección del datacenter, aseguró registros y evidencias para el análisis forense y apoyó las labores de remediación. La investigación también cuenta con la participación de la Fiscalía General de la Nación.

Como consecuencia del incidente, algunos sistemas permanecieron temporalmente indisponibles, entre ellos SGDEA, SICAAC, SICJ, MICC y SUIN-JURISCOL, mientras que otros servicios continuaron operativos o con restricciones. El Ministerio implementó canales alternativos para garantizar la atención ciudadana y posteriormente activó un plan integral de recuperación tecnológica, con acompañamiento de COLCERT, Fiscalía, expertos DART de Microsoft y otros aliados.

El mundo

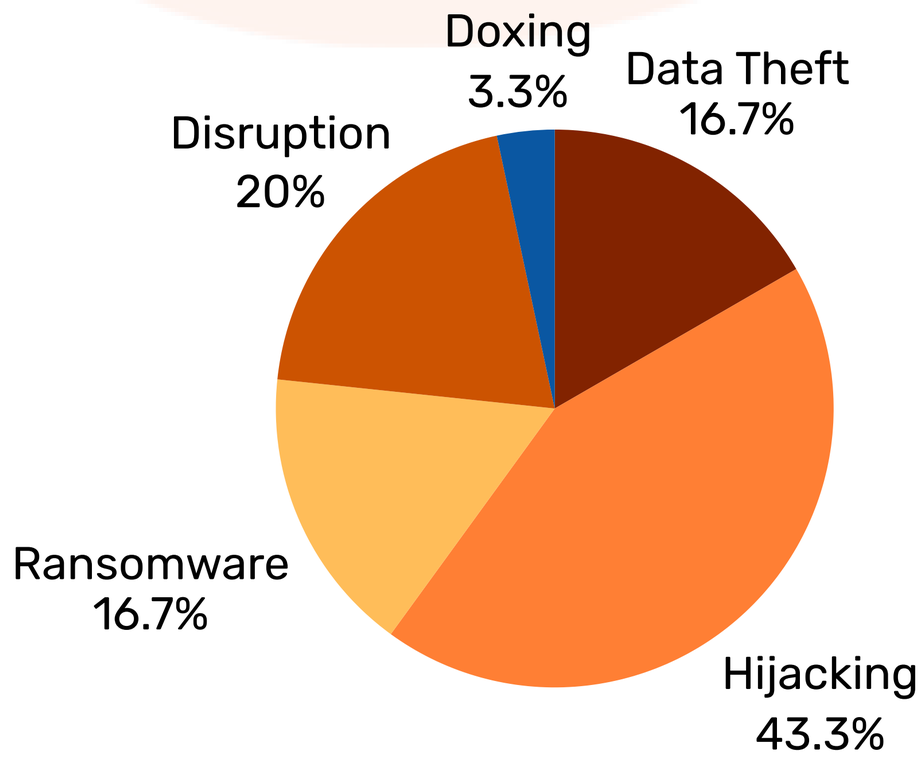
32

Ciber incidentes

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

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.