ZTC CYBER INTELLIGENCE

México & Latinoamérica

INTELIGENCIA SEMANAL DE CIBERSEGURIDAD

Las señales que importan

- IA asistiendo ataques contra controladores industriales
- SharePoint entra en explotación activa
- Google fija 2029 para su preparación post-cuántica
- El fraude financiero explota la identidad de marca

Edición 001

Lunes 24 de agosto de 2026

Las señales de ciberseguridad que importan esta semana

ZEROTRUST.CONSULTING

linkedin.com/company/zerotrustconsulting

00 / EDITORIAL

Editorial

Por qué nace ZTC CYBER INTELLIGENCE y cómo leer esta primera edición

DIRECCIÓN EDITORIAL / JUAN PABLO YBARRA LLAMAS

Antes de comenzar la semana

La ciberseguridad se volvió demasiado importante para consumirla como una secuencia de titulares. Una vulnerabilidad crítica puede ser irrelevante para una empresa sin el activo afectado; una alerta aparentemente local puede anticipar un riesgo operativo para toda una industria. ZTC CYBER INTELLIGENCE nace para separar ambas cosas: el volumen de información y las señales que merecen una decisión.

México recibe buena parte de sus señales de riesgo desde fuera de sus fronteras: estándares que cambian en Estados Unidos, obligaciones que maduran en Europa, campañas que aparecen primero en Brasil o Colombia y plataformas globales que modifican su arquitectura criptográfica. Interpretarlas a tiempo exige traducir tecnología en exposición, continuidad, cumplimiento y responsabilidad ejecutiva.

Cada lunes seleccionaremos pocos acontecimientos, verificaremos qué está confirmado y explicaremos qué significan para organizaciones mexicanas y latinoamericanas. El lector encontrará hechos, análisis, inferencias explícitas y una lista breve de acciones. La ambición editorial es sencilla: llegar al inicio de la semana con mejores preguntas y prioridades más claras.

El mapa de señales de esta edición

SEÑAL	EVIDENCIA DE LA SEMANA	DECISIÓN EJECUTIVA
Velocidad	IA aplicada a scripts de explotación industrial y revisión agentiva de código.	Medir la latencia para detectar, decidir y contener.
Identidad	Suplantación de financieras y reclutamiento falso como acceso inicial.	Proteger flujos de confianza, no sólo cuentas.
Criptografía	Google publica ruta PQC a 2029; ML-KEM ya aparece en defensa y ataque.	Iniciar inventario criptográfico y pruebas híbridas.
Cumplimiento	CISA aplica parcheo por riesgo; ENISA amplía el foco de evaluación.	Convertir obligación en evidencia operativa.

MÉTODO
Ventana principal: 17-23 de agosto de 2026. Se amplió hasta 14 días cuando una publicación seguía generando consecuencias esta semana. HECHO describe evidencia confirmada; ANÁLISIS interpreta; INFERENCIA identifica una conclusión razonable que la fuente no afirma de forma expresa. Corte editorial: 23 de agosto de 2026.

01 / LA NOTICIA DE LA SEMANA

La noticia de la semana

IA asistiendo ataques contra controladores que gobiernan procesos físicos

Controladores Siemens S7 bajo una amenaza activa

HECHO El 19 de agosto, CISA, NSA, FBI, el Departamento de Energía y la EPA de Estados Unidos publicaron una alerta conjunta sobre actividad activa contra controladores lógicos programables Siemens S7. Los actores usan servicios de escaneo para localizar PLC expuestos o mal segmentados y emplean scripts de explotación asistidos por IA, disfrazados como herramientas legítimas de monitoreo. [1]

Qué está confirmado

- La actividad se dirige a las series S7-200, S7-300, S7-400, S7-1200 y S7-1500.
- Los scripts combinan información pública con bibliotecas como snap7/python-snap7 para leer o escribir memoria, configuración y lógica de escalera mediante S7comm.
- Los sectores observados incluyen manufactura crítica, energía, agua, químicos, alimentos y agricultura, y edificios comerciales.
- Las agencias describen reconocimiento persistente y desarrollo de capacidad; advierten que la exposición a internet eleva materialmente la probabilidad de explotación.

POR QUÉ IMPORTA A MÉXICO

México es una plataforma manufacturera y logística profundamente conectada con cadenas norteamericanas. La alerta se refiere a actividad observada en Estados Unidos; la inferencia relevante es que el mismo patrón de exposición, integradores remotos, firmware rezagado y segmentación insuficiente puede existir en plantas mexicanas. El riesgo no termina en datos: puede alcanzar producción, seguridad física, calidad y continuidad.

Qué debería hacer un CISO o CEO

1	**Inventario**	Ubicar todos los PLC S7, firmware, estaciones TIA/STEP 7 y responsables.
2	**Exposición**	Confirmar que TCP/102 y los PLC no sean accesibles desde internet.
3	**Terceros**	Validar accesos de integradores, credenciales, ventanas y trazabilidad.
4	**Detección**	Buscar snap7 no autorizado, escrituras fuera de cambio y escaneo secuencial.
5	**Continuidad**	Probar recuperación de lógica y operación segura ante indisponibilidad.

02 / MÉXICO

México

La marca financiera se convierte en superficie de ataque

Once instituciones reportaron suplantación de identidad

HECHO La CONDUSEF informó que once instituciones financieras inscritas en SIPRES reportaron durante julio el uso indebido de su nombre, logotipo o datos institucionales. Los suplantadores ofrecían créditos o servicios para obtener anticipos, documentos personales o información sensible. La alerta fue publicada en agosto. [2]

DISTINCIÓN ESENCIAL
Suplantación de identidad corporativa no equivale a intrusión en los sistemas de las instituciones. La evidencia disponible describe fraude que explota confianza, canales digitales y parecido visual; no acredita una brecha tecnológica en las entidades afectadas.

Lo que la señal revela

ANÁLISIS La superficie de ataque de una financiera incluye sus dominios, números telefónicos, perfiles sociales, anuncios, documentos, distribuidores y procesos de originación. El atacante puede producir una pérdida para el cliente sin atravesar el firewall de la entidad. Para banca y fintech, la protección de marca debe conectarse con fraude, seguridad, atención a clientes, privacidad, jurídico y comunicación de crisis.

Controles que deben converger

CAPACIDAD	PREGUNTA DE CONTROL
Detección	¿Monitoreamos dominios parecidos, anuncios, perfiles, teléfonos y apps de mensajería?
Verificación	¿El cliente puede comprobar en segundos el canal, asesor y cuenta receptora?
Respuesta	¿Existe un flujo de takedown, preservación de evidencia y alerta pública?
Aprendizaje	¿Los casos de fraude retroalimentan diseño de producto, onboarding y soporte?

PARA EL CONSEJO
Solicitar una métrica que una abuso de marca, fraude evitado, tiempo de retiro de contenido y afectados atendidos. Lo que no se mide como riesgo digital suele quedarse dividido entre áreas.

NOTA DE VERIFICACIÓN Esta edición no eleva alegaciones públicas sobre incidentes en México cuando no existe confirmación suficiente de la organización afectada o de una autoridad competente.

03 / LATINOAMÉRICA

Latinoamérica

Dos alertas oficiales muestran cómo la región traduce riesgo global en acción local

Brasil: SharePoint pasa de vulnerabilidad a explotación activa

HECHO El 19 de agosto, el CTIR Gov de Brasil publicó la Alerta 69/2026 sobre CVE-2026-55040 en SharePoint Server. La falla permite eludir controles de autenticación; fue incorporada al catálogo KEV de CISA el 18 de agosto y tiene una calificación CVSS 3.1 de 9.1 aportada por Microsoft. El CTIR recomendó identificar versiones afectadas y aplicar de inmediato las correcciones del fabricante. [3][7]

SEÑAL REGIONAL
La alerta brasileña no sólo replica un CVE. Lo traduce a una obligación operativa para su red federal y comunica métricas de explotación. Esa capacidad de traducción es parte de la resiliencia nacional.

Colombia: Remus Stealer se comercializa como servicio

HECHO El 20 de agosto, el CSIRT de la Policía Nacional de Colombia alertó sobre Remus Stealer, un malware de robo de información distribuido activamente bajo el modelo Malware-as-a-Service en foros y canales clandestinos. La autoridad publicó indicadores de compromiso para facilitar su detección. [4]

ANÁLISIS El modelo de servicio reduce la barrera de entrada para campañas que buscan credenciales, sesiones o información comercial. La defensa debe asumir variación continua de infraestructura y comportamiento, no depender únicamente de firmas estáticas.

Lectura conjunta

Brasil responde a una falla empresarial explotada; Colombia alerta sobre una capacidad criminal disponible para múltiples operadores. Ambas historias convergen en una necesidad: que los avisos de CSIRT lleguen al inventario real, al dueño del activo y a una decisión con fecha. Una suscripción sin enrutamiento interno sólo mejora la información, no la postura.

Tres preguntas para una organización regional

- ¿Qué equipo recibe alertas de cada país donde operamos y quién determina aplicabilidad?
- ¿Podemos mapear una alerta a activos, versiones, responsables y evidencia de corrección?
- ¿Compartimos indicadores y lecciones entre filiales sin depender de relaciones informales?

04 / EL MUNDO

El mundo

Acontecimientos globales con impacto directo en operación, proveedores y talento

Cisco ASA/FTD: explotación activa contra la disponibilidad de VPN

HECHO Cisco informó explotación activa en agosto de CVE-2026-20349, una falla de severidad alta (CVSS 8.6) en Remote Access SSL VPN de ASA y FTD. Un atacante remoto no autenticado puede provocar la recarga del dispositivo y una denegación de servicio. Cisco publicó actualizaciones y señaló que no existe workaround. La falla no se describe como ejecución remota ni como robo de datos. [5]

IMPLICACIÓN EMPRESARIAL
Una vulnerabilidad sin impacto en confidencialidad puede detener trabajo remoto, soporte, administración y acceso de proveedores. Disponibilidad también es ciberseguridad.

Lazarus convierte una oferta laboral en cadena de intrusión

HECHO Check Point Research documentó una nueva ola de Operation Dream Job vinculada con Lazarus. Los señuelos simulan vacantes en defensa, aeroespacial y aviación; entregan visores PDF alterados y malware. La cadena explotó CVE-2026-68820 en AFD.sys para elevar privilegios a SYSTEM y desplegar FudModule. Microsoft corrigió la falla el 11 de agosto. La investigación observó alcance global, incluida actividad en Brasil. [6][13]

Qué cambia para México y Latinoamérica

INFERENCIA Los sectores aeroespacial, defensa, software y manufactura avanzada de la región participan en cadenas internacionales y compiten por talento. Un flujo de reclutamiento externo puede convertirse en acceso inicial hacia equipos corporativos, repositorios o proveedores. La validación de reclutadores, archivos y herramientas debe integrarse al modelo de amenaza de talento y propiedad intelectual.

Acciones prioritarias

- Actualizar Windows y verificar cobertura específica de CVE-2026-68820.
- Revisar visores PDF no autorizados, carga lateral de libmupdf.dll y actividad anómala de AFD.sys.
- Separar la evaluación de ofertas externas de los equipos y credenciales corporativas.
- Probar continuidad del acceso remoto antes de actualizar appliances VPN críticos.

05 / AMENAZA DE LA SEMANA

Amenaza de la semana

SharePoint: el momento en que parchear deja de ser suficiente

CVE-2026-55040

QUÉ ES	Bypass de autenticación por red en Microsoft SharePoint Server. [7]
A QUIÉN AFECTA	SharePoint Enterprise Server 2016, SharePoint Server 2019 y Subscription Edition en versiones vulnerables identificadas por Microsoft.
GRAVEDAD	CVSS 9.1; explotación activa; añadida a CISA KEV el 18 de agosto. La fecha federal de remediación fue el 21 de agosto.
QUÉ REVISAR	Versiones y exposición, aplicación de actualizaciones, registros de autenticación, persistencia, cuentas y artefactos anómalos, y evidencia forense previa a la corrección.

Parchear corrige la puerta; investigar responde si ya fue atravesada

ANÁLISIS Cuando una vulnerabilidad entra al catálogo KEV, existe evidencia confiable de explotación real. La secuencia de respuesta debe incluir contención y búsqueda de compromiso, no sólo instalación de un KB. CISA vinculó esta remediación con su BOD 26-04 y requisitos de triage forense para activos federales. Aunque la directiva no obliga a empresas mexicanas, su lógica ofrece un benchmark útil: combinar explotación, exposición, automatización e impacto técnico para ordenar el trabajo. [7][12]

DECISIÓN EN 60 MINUTOS
1) identificar servidores y builds; 2) confirmar exposición; 3) aislar o limitar acceso si la corrección no puede aplicarse; 4) preservar registros y buscar señales de compromiso; 5) corregir; 6) validar y documentar. El orden exacto debe adaptarse al entorno y al plan de respuesta de la organización.

Evite tres errores

- Confundir disponibilidad de parche con remediación comprobada.
- Cerrar el ticket sin revisar posible acceso anterior.
- Aplicar una prioridad global sin considerar exposición y criticidad del activo.

06 / IA + CIBERSEGURIDAD

IA + ciberseguridad

La ventaja no está en tener un modelo, sino en gobernar el sistema que lo rodea

Mandiant abre su arquitectura de revisión agentiva de código

HECHO El 18 de agosto, Mandiant describió su Agentic Vulnerability Discovery Harness. En una investigación con repositorios corporativos robados, el sistema encontró más de 100 vulnerabilidades críticas verdaderamente positivas en dos días. La organización reporta doce CVE asignados y mantiene validación humana y pruebas dinámicas antes de formalizar hallazgos. [8]

La misma semana, la IA apareció del otro lado

La alerta conjunta sobre Siemens S7 atribuye a los actores el uso de IA para generar y adaptar scripts de explotación industrial. Google Cloud, por su parte, insistió el 21 de agosto en que la IA amplifica tanto ataque como defensa, y que MFA, Zero Trust, parcheo y detección siguen siendo la base que proporciona contexto a una defensa automatizada. [1][10]

LA SEÑAL

IA no sustituye el proceso de seguridad: amplifica la calidad -o la debilidad- del inventario, el modelo de amenazas, los datos, las reglas de validación y la supervisión humana que recibe.

Qué debería aprobar un CISO

CONTROL	CRITERIO
Alcance	Repositorios, datos, secretos y entornos donde el agente puede leer o ejecutar.
Pruebas	Benchmarks propios, reproducibilidad, falsos positivos y falsos negativos.
Validación	Revisión experta y prueba dinámica antes de tratar una hipótesis como vulnerabilidad.
Acción	Cambios en producción, divulgación y cierre sujetos a autorizaciones explícitas.
Trazabilidad	Modelo, versión, entradas, decisiones, evidencia y responsable humano.

07 / CRIPTOGRAFÍA Y PQC

Criptografía y PQC

La transición post-cuántica recibe un calendario operativo y una advertencia inesperada

Google Cloud fija 2029 como meta de preparación completa

HECHO El 11 de agosto, Google Cloud publicó una hoja de ruta para alcanzar preparación post-cuántica completa en 2029. La empresa informó que sus endpoints google.com y *.googleapis.com ya ofrecen intercambio híbrido con ML-KEM; que sus balanceadores soportan X25519MLKEM768 para TLS 1.3; y que Cloud KMS ofrece ML-KEM, ML-DSA y SLH-DSA con disponibilidad general. La ruta separa confidencialidad, integridad y fundamentos de gestión de claves. [9]

Una señal desde el adversario

HECHO Check Point observó que un módulo de Lazarus utilizaba Kyber/ML-KEM para negociar material de sesión antes de descargar y ejecutar su carga de escalamiento de privilegios. No significa que PQC sea insegura: significa que los algoritmos son capacidades neutrales y que los actores ofensivos también adoptan criptografía moderna. [6]

SIGNIFICADO PRÁCTICO
La disponibilidad de un algoritmo en el proveedor cloud no completa la migración de una empresa. Las aplicaciones, clientes, certificados, tokens, HSM, bibliotecas, integraciones, terceros y ciclos de vida de claves siguen bajo responsabilidad del cliente.

PQC es un programa de arquitectura

AHORA	2027	2028	2029
Inventario criptográfico, datos de larga vida y dependencias.	Validar tráfico híbrido, VPN, SDK y pipelines.	Firmas, PKI, identidad, HSM y cadena de software.	Convergencia operativa y evidencia de preparación.

ANÁLISIS El anuncio convierte 2029 en una fecha de planeación para clientes de Google Cloud, no en un permiso para esperar. Los sistemas con vida útil de varios años y los datos sensibles que deben permanecer confidenciales necesitan decisiones antes de que cambie la infraestructura subyacente.

08 / ZERO TRUST / CLOUD / IDENTIDAD

Zero Trust / cloud / identidad

El nuevo perímetro es el flujo de confianza

Las credenciales ya no son el único objetivo

Las historias de esta semana recorren distintos puntos del mismo problema. Los suplantadores financieros copian la identidad de una institución; Lazarus copia la identidad de un reclutador; los atacantes de OT disfrazan scripts como herramientas de monitoreo; y una falla en SharePoint permite eludir autenticación. El activo común es la confianza que rodea una acción aparentemente legítima. [1][2][3][6]

ANÁLISIS Zero Trust debe extenderse más allá del inicio de sesión. Verificar explícitamente significa confirmar identidad, dispositivo, origen, propósito, sensibilidad de la acción y contexto operativo durante todo el flujo. Una autenticación correcta no vuelve legítima una descarga masiva, un cambio de MFA, una escritura de PLC o una solicitud de pago anticipado.

PERSPECTIVA EJECUTIVA

El perímetro ya no es una red ni una cuenta: es cada flujo donde una persona o sistema confía en una identidad, una herramienta o una instrucción.

Cinco controles de flujo

FLUJO	CONTROL PRIORITARIO
Acceso SaaS	MFA resistente a phishing, dispositivo administrado y evaluación continua de sesión.
Soporte	Verificación fuera de banda para cambios de credenciales, MFA y recuperación.
Reclutamiento	Canales aprobados, sandboxing de archivos y separación de equipos corporativos.
OT / terceros	Acceso temporal, segmentado, registrado y ligado a una orden de trabajo.
Marca	Monitoreo, takedown, comunicación y verificación pública de canales.

Google Cloud resumió la postura defensiva el 21 de agosto: IA cambia la escala, pero MFA, Zero Trust, parcheo consistente y detección integral siguen creando la base y el contexto que la defensa automatizada necesita. [10]

09 / REGULACIÓN Y CUMPLIMIENTO

Regulación y cumplimiento

La regulación se está convirtiendo en una arquitectura de priorización y evidencia

CISA: parchear según riesgo observable

HECHO La aplicación de BOD 26-04 a la falla de SharePoint muestra un modelo que combina estado KEV, exposición del activo, automatización del exploit e impacto técnico. La directiva obliga a agencias federales estadounidenses; no a empresas mexicanas. Su valor para el mercado es metodológico: sustituye calendarios uniformes por decisiones justificadas con contexto y exige triage cuando pudo existir compromiso. [7][12]

ENISA amplía el mercado de evaluación

HECHO El 10 de agosto, ENISA actualizó su estudio del mercado de evaluaciones de ciberseguridad para 2021-2025. La nueva edición incorpora datos del primer esquema europeo de certificación, EUCC, y añade servicios de seguridad gestionados como categoría. [11]

IMPLICACIÓN PARA EMPRESAS MEXICANAS
Quien vende tecnología o servicios a clientes europeos puede enfrentar expectativas crecientes de evaluación, certificación y evidencia sobre productos, nube, sistemas de gestión y servicios administrados. Cumplir tenderá a requerir trazabilidad técnica, no sólo políticas.

La señal que cruza jurisdicciones

MODELO	CAMBIO	EVIDENCIA ESPERADA
CISA	Prioridad por riesgo.	Inventario, exposición, KEV, triage y cierre verificable.
ENISA	Evaluación y certificación.	Alcance, controles, organismo evaluador y resultado reproducible.
Finanzas MX	Abuso de identidad de marca.	Detección, atención, retiro, preservación y comunicación.

NOTA En la ventana editorial no se confirmó un cambio regulatorio mexicano de alcance comparable. La ausencia de novedad normativa no reduce la urgencia operativa de las señales observadas.

10 / PERSPECTIVA ZTC

Perspectiva ZTC

Lo que el mercado quizá todavía no está midiendo

El riesgo que todavía no se mide: la latencia de decisión

ANÁLISIS EDITORIAL

Esta semana parece reunir temas distintos: controladores industriales, SharePoint, ofertas laborales falsas, agentes de IA, suplantación financiera y criptografía post-cuántica. La señal transversal es otra. El riesgo está cambiando de velocidad, pero muchas organizaciones siguen decidiendo con el mismo ritmo.

Las agencias estadounidenses describen actores que usan IA para convertir información pública en scripts contra PLC. Mandiant reporta más de cien vulnerabilidades críticas verificadas en dos días mediante una arquitectura agentiva. CISA incorpora una falla de SharePoint a su catálogo de explotación activa y fija una remediación federal de tres días. Google publica una ruta post-cuántica que obliga a mirar 2027, 2028 y 2029 como hitos de arquitectura. En todos los casos, el dato decisivo no es sólo la severidad. Es el tiempo disponible para convertir conocimiento en control.

Ese desfase puede llamarse latencia de decisión: el intervalo entre una señal confiable y una acción autorizada, ejecutada y verificada. Una empresa puede tener buenas herramientas y aun así quedar expuesta porque tarda días en saber quién es dueño del activo, semanas en aprobar una ventana de cambio o meses en resolver una dependencia contractual. La vulnerabilidad técnica y la demora organizacional se multiplican.

Conviene distinguir cuatro relojes. El primero es el de descubrimiento: cuánto tarda la organización en saber que un activo, clave, proveedor o flujo existe. El segundo es el de exposición: cuánto tiempo permanece vulnerable o accesible. El tercero es el organizacional: cuánto tarda en decidir entre parchear, aislar, aceptar, recuperar o comunicar. El cuarto es el de migración: cuánto tarda en transformar una arquitectura, como ocurrirá con PQC, identidad o segmentación industrial.

La consecuencia para el consejo es concreta. Ya no basta preguntar cuántos incidentes hubo o qué porcentaje de parches se instaló. Debe preguntar cuánto tiempo tomó determinar aplicabilidad, quién pudo autorizar una contención, qué evidencia cerró el riesgo y qué dependencias impidieron actuar antes. La velocidad sin control genera errores; el control sin velocidad genera exposición. La resiliencia aparece cuando ambos se diseñan juntos.

La oportunidad para México y Latinoamérica es evitar copiar únicamente herramientas. Podemos adoptar directamente una disciplina basada en tiempos: inventarios que responden, responsables explícitos, umbrales de decisión, alternativas de continuidad, evidencia de cierre y migraciones con hitos. En un entorno donde atacantes, proveedores y reguladores aceleran, reducir la latencia de decisión puede producir más resiliencia que añadir otra capa tecnológica sin integración.

LA PREGUNTA PARA EL CONSEJO

¿Cuánto tiempo transcurre, en nuestra organización, entre una señal confiable y una reducción verificable de exposición?

11 / RADAR EJECUTIVO

Radar ejecutivo

Cinco revisiones concretas para comenzar la semana

☐ OT: inventariar PLC Siemens S7, firmware, TCP/102, estaciones de ingeniería y accesos de integradores.

☐ SharePoint: confirmar builds, exposición, actualización y búsqueda de compromiso para CVE-2026-55040.

☐ Acceso remoto: validar versiones corregidas de Cisco ASA/FTD y continuidad ante indisponibilidad de VPN.

☐ Identidad: revisar flujos de reclutamiento, cambios de MFA, suplantación de marca y verificación fuera de banda.

☐ PQC: iniciar inventario criptográfico, clasificar datos de larga vida y definir pruebas híbridas 2026-2027.

Una agenda de 30 minutos

MIN	PREGUNTA	SALIDA
0-10	¿Cuáles de las diez señales aplican a nuestros activos?	Lista de aplicabilidad y responsables.
10-20	¿Qué exposición requiere contención o verificación hoy?	Prioridades y fecha de decisión.
20-30	¿Qué dependencia estructural impedirá responder igual la próxima vez?	Una acción de arquitectura o gobierno.

PRÓXIMA EDICIÓN

ZTC CYBER INTELLIGENCE regresará el lunes 31 de agosto de 2026 con las señales que los responsables de seguridad, riesgo y tecnología en México deberían entender antes de comenzar la semana.

Conoce cómo ZTC diseña seguridad para entornos de misión crítica: zerotrust.consulting

12 / FUENTES

Fuentes

Fuentes consultadas y verificadas para la Edición 001

[1] CISA, NSA, FBI, DOE y EPA. Defending Against an Active Threat to Siemens S7 Series PLCs. 19 ago 2026.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-231a

[2] CONDUSEF. La CONDUSEF informa que durante julio de 2026 once instituciones financieras informaron suplantación de identidad.
https://www.gob.mx/condusef/prensa/la-condusef-informa-que-durante-el-mes-de-julio-de-2026-11-instituciones-financieras-han-informado-suplantacion-de-su-identidad

[3] CTIR Gov Brasil. Alerta 69/2026: vulnerabilidade crítica no SharePoint. 19 ago 2026.
https://www.gov.br/gsi/pt-br/assuntos/ctir/alertas/2026/alerta-69-2026

[4] CSIRT Policía Nacional de Colombia. Boletín 048: Remus Stealer. 20 ago 2026.
https://cc-csirt.policia.gov.co/alertas-tips/2026/iii-trimestre/boletin-informativo-nro-048-alerta-remus-stealer-m

[5] Cisco. ASA/FTD Remote Access SSL VPN Denial of Service Vulnerability, CVE-2026-20349. 11 ago 2026.
https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-asaftd-vpn-dos-dzv4mQFF.html

[6] Check Point Research. Shattering the Dream: When a Job Offer Becomes a Zero-Day Attack. 11 ago 2026.
https://research.checkpoint.com/2026/shattering-the-dream-when-a-job-offer-becomes-a-zero-day-attack/

[7] NIST NVD. CVE-2026-55040: Microsoft SharePoint weak authentication vulnerability.
https://nvd.nist.gov/vuln/detail/CVE-2026-55040

[8] Google Threat Intelligence / Mandiant. Staying Ahead of Adversarial AI Through Agentic Source Code Review. 18 ago 2026.
https://cloud.google.com/blog/topics/threat-intelligence/staying-ahead-of-adversarial-ai-through-agentic-source-code-review/

[9] Google Cloud. PQC in Plaintext: Google Cloud's post-quantum cryptography roadmap. 11 ago 2026.
https://cloud.google.com/blog/products/identity-security/pqc-in-plaintext-google-clouds-post-quantum-cryptography-roadmap

[10] Google Cloud. Cloud CISO Perspectives: Sticking to security fundamentals in the AI era. 21 ago 2026.
https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-sticking-to-security-fundamentals-in-the-ai-era/

[11] ENISA. How is the market of cybersecurity assessments doing? 10 ago 2026.
https://certification.enisa.europa.eu/news/how-market-cybersecurity-assessments-doing-2026-08-10_en

[12] CISA. BOD 26-04: Prioritizing Security Updates Based on Risk. 10 jun 2026.
https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk

[13] Microsoft Security Response Center. CVE-2026-68820 Security Update Guide.
https://msrc.microsoft.com/update-guide/advisory/CVE-2026-68820

Criterio editorial: se priorizaron fuentes gubernamentales, regulatorias, de fabricantes y de investigación técnica directa. Las fechas, nombres, CVE, alcance y estado de explotación fueron revisados por segunda vez antes del cierre. Cuando una conclusión corresponde a análisis o inferencia, se identifica expresamente.

ZTC CYBER INTELLIGENCE México & Latinoamérica. Edición 001.
Dirección editorial: Juan Pablo Ybarra Llamas | zerotrust.consulting | LinkedIn de Zero Trust Consulting