

ZTC CYBER INTELLIGENCE

México & Latinoamérica

IA · EXPLOTACIÓN · CITRIX · ZIMBRA · RMM · RESILIENCIA

LA VELOCIDAD YA ES EL RIESGO

Más vulnerabilidades · explotación más rápida · perímetro bajo ataque · herramientas legítimas convertidas en persistencia

Tesis editorial: priorizar por explotación, exposición, capacidad de propagación y evidencia de cierre.

6 señales · 4 capas de análisis

8 controles · 8 preguntas ejecutivas

[LECTURA EJECUTIVA >](#)

Edición 007 · 5 de octubre de 2026

MENOS TITULARES. MÁS CONTEXTO PARA DECIDIR.

La ventana de defensa se encoge.

Durante años, la gestión de vulnerabilidades se construyó alrededor de una secuencia razonable: descubrir, evaluar, priorizar y corregir. Esa secuencia sigue siendo válida. Lo que está cambiando es el tiempo disponible para ejecutarla.

Google Threat Intelligence Group reportó esta semana que las divulgaciones mensuales de vulnerabilidades se duplicaron durante 2026 y que la explotación observada pasó de un promedio de 10.5 vulnerabilidades mensuales en 2025 a 18 durante enero-agosto de 2026. Pero solo 0.23% de las vulnerabilidades divulgadas fue observado en explotación activa. El reto no es perseguir todo: es distinguir rápido qué importa.

ESTA SEMANA

GTIG mide más descubrimiento y explotación; Citrix NetScaler enfrenta zero-days activamente explotados; PeopleSoft vuelve a ser atacado tras un bypass simple de WAF; Microsoft documenta explotación de Zimbra sin autenticación ni interacción; campañas de phishing abusan RMM legítimo; y el Digital Defense Report 2026 describe un entorno más conectado y con timelines comprimidos.

LA PREGUNTA DE CADA LUNES

¿Cuánto tiempo necesita hoy nuestra organización para pasar de "existe una vulnerabilidad" a "sabemos si estamos expuestos, si fuimos comprometidos y si el riesgo quedó realmente cerrado"?

POR QUÉ AHORA

El cambio no es solo volumen.

Algunos actores convierten una divulgación o una ruta conocida en explotación antes de que inventario, dueño y remediación hayan terminado de alinearse.

CRITERIO ZTC

Cinco filtros antes de escalar.

1) ¿Está explotada? 2) ¿Estamos expuestos? 3) ¿Qué proceso sostiene? 4) ¿Qué autoridad hereda? 5) ¿Qué evidencia demostrará el cierre?

VENTANA EDITORIAL

28 de septiembre - 4 de octubre de 2026. La selección prioriza hechos que cambian una decisión operativa para organizaciones en México y Latinoamérica, no la novedad por sí misma.

Publicar más CVE no significa tener que perseguirlos todos

GTIG publicó el 30 de septiembre un análisis de la evolución de vulnerabilidades durante 2025 y 2026. Las divulgaciones mensuales pasaron de 5,045 en enero de 2026 a 10,740 en agosto. La explotación observada subió de 10.5 vulnerabilidades mensuales en 2025 a 18 durante enero-agosto de 2026.

10,740

vulnerabilidades divulgadas en agosto

18 / MES

promedio explotado en 2026

0.23%

de las divulgadas llegó a explotación observada

75

High-Risk explotadas entre enero y agosto

LA SEÑAL

El volumen dejó de ser una estrategia de priorización. Cuando miles de vulnerabilidades aparecen cada mes, CVSS por sí solo produce ruido. GTIG observa además que la explotación sigue concentrándose en appliances de borde y servicios empresariales expuestos.

REVISAR ESTA SEMANA

Cruzar vulnerabilidades con activos realmente desplegados. Identificar exposición a internet. Incorporar KEV e inteligencia de explotación. Separar "vulnerable" de "explotado". Definir SLA por riesgo operativo y no únicamente por severidad. La meta no es cerrar más tickets: es reducir primero el riesgo que un adversario puede convertir en acceso.

QUÉ CAMBIA

CVSS ya no puede decidir solo.

Una falla media expuesta y explotada puede exigir acción antes que una crítica sin superficie real. Contexto de activo, explotación y alcance deben viajar juntos.

MÉTRICA CLAVE

Tiempo a alcance.

Medir cuánto tarda el equipo en saber cuántos activos están afectados, cuáles están expuestos y quién tiene la responsabilidad de cerrarlos.

DISCOVER

Alerta -> detección interna.

SCOPE

Identificar todos los activos.

CONTAIN

Mitigar o aislar de forma verificable.

CLOSE

Parche + hunting + residual.

Citrix NetScaler: el dispositivo que protege el perímetro también puede abrirlo

Mandiant y GTIG informaron el 29 de septiembre explotación activa de CVE-2026-88772 en Citrix NetScaler ADC y NetScaler Gateway. La actividad habría comenzado al menos a principios de septiembre. El exploit evade autenticación y permite establecer acceso inicial a nivel root. Citrix también reportó explotación activa de CVE-2026-88771.

2
zero-days bajo explotación activa

PRE-AUTH
acceso antes de autenticación

ROOT
nivel de privilegio inicial observado

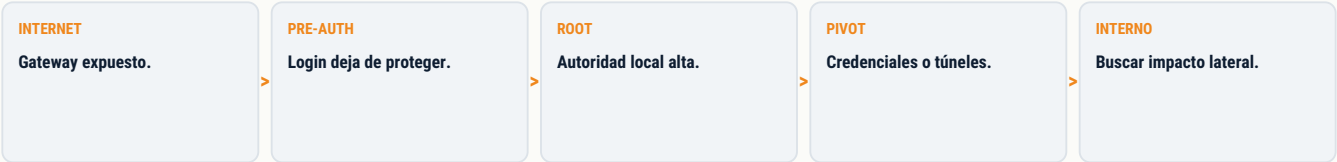
SEP
actividad desde principios de septiembre

POR QUÉ IMPORTA

VPN, ADC, gateways y appliances de seguridad suelen ubicarse exactamente donde un atacante quiere estar: entre internet y los sistemas internos. Estos componentes también pueden tener menor visibilidad EDR que un endpoint convencional.

REVISAR ESTA SEMANA

Confirmar versión y exposición. Aplicar actualizaciones del fabricante. Revisar indicadores y persistencia. Rotar credenciales potencialmente accesibles desde el appliance. Documentar desde cuándo estuvo expuesto y qué evidencia permite cerrar el riesgo. Cuando existió explotación activa, el parche no demuestra ausencia de compromiso previo.



ANTES DE CERRAR
La ventana de exposición importa.
Registrar versión, periodo vulnerable, IOCs revisados, credenciales rotadas y limitaciones de logging. Si falta evidencia, documentar el riesgo residual.

ARQUITECTURA
El edge no debe heredar todo.
Segmentación, cuentas dedicadas y administración separada reducen el radio de impacto si el appliance que protege el acceso resulta comprometido.

PeopleSoft: una regla de WAF no es una frontera de seguridad

Mandiant y GTIG reportaron una nueva ola de explotación masiva de CVE-2026-35273 contra Oracle PeopleSoft. El actor modificó su exploit para evadir reglas de WAF que bloqueaban literalmente la ruta vulnerable: bastó URL-encoding de un solo carácter para que la aplicación siguiera interpretando la solicitud mientras algunas defensas intermedias dejaban de bloquearla.

MASS
nueva ola de explotación

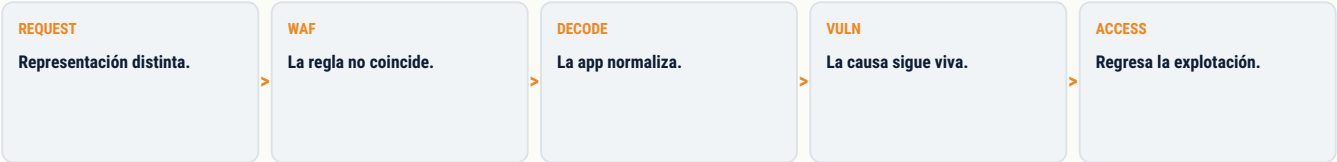
1 CHAR
variación suficiente para el bypass descrito

WAF
mitigación burlada por encoding

MULTI
targeting global y multisector

LA LECCIÓN
Una firma de WAF puede contener una técnica conocida sin eliminar la vulnerabilidad que existe detrás. Una mitigación externa puede transformarse inadvertidamente en control permanente aunque originalmente solo debía comprar tiempo.

REVISAR ESTA SEMANA
Identificar PeopleSoft expuesto. Confirmar versión y corrección real. Verificar si el WAF está siendo tratado como mitigación temporal o como sustituto del parche. Buscar web shells, herramientas RMM y accesos privilegiados anómalos en sistemas que estuvieron expuestos.



MITIGACIÓN
Compra tiempo, no borra la causa.
Debe tener owner, alcance, fecha de expiración y condición de salida. Una excepción sin caducidad se convierte en arquitectura por accidente.

REMEDIACIÓN
Elimina la ruta de raíz.
La evidencia fuerte es que la vulnerabilidad desapareció o que la arquitectura ya no permite la ruta; no solo que una firma continúa bloqueando la forma conocida del exploit.

Zimbra: un correo puede convertirse en ejecución sin que nadie haga clic

Microsoft Threat Intelligence documentó explotación de CVE-2026-73570 en Zimbra Collaboration Suite. La vulnerabilidad afecta la ruta de notificaciones SNMP cuando está instalado el paquete opcional zimbra-snmp y las notificaciones están habilitadas. Puede activarse mediante un correo especialmente construido contra servidores expuestos a internet, sin autenticación ni interacción del usuario.

0

clics requeridos

0

autenticación del atacante

MAIL

servidor como superficie inicial

RCE

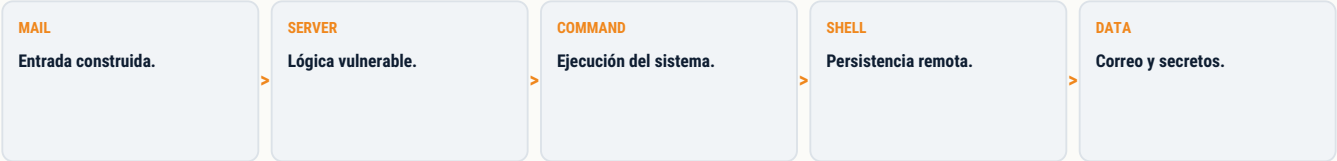
inyección de comandos del sistema

POR QUÉ CAMBIA LA PRIORIDAD

Durante años, muchas campañas de correo dependieron de que una persona abriera un archivo o siguiera un enlace. Aquí el usuario no es el control decisivo. La exposición reside en el propio servidor. Capacitación y filtros antiphishing no compensan una vulnerabilidad de ejecución en infraestructura expuesta.

REVISAR ESTA SEMANA

Identificar servidores Zimbra y configuración afectada. Confirmar actualización. Revisar exposición histórica. Buscar web shells, reverse shells, procesos anómalos y acceso inusual a buzones o credenciales. "Ya está parchado" y "nunca fue comprometido" son afirmaciones diferentes.



NO DEPENDE DEL USUARIO

El clic deja de ser el control.

Capacitación anti-phishing no detiene una ruta que se ejecuta en el servidor. El control principal se mueve a versión, hardening, exposición, telemetría y respuesta.

CIERRE MÍNIMO

Parchar y demostrar.

Versión corregida + configuración revisada + ventana histórica de exposición + hunting de shells/procesos + revisión de accesos a buzones y secretos.

Cuando el malware parece software de soporte técnico

Microsoft observó campañas de phishing que distribuían un instalador legítimo y firmado de MSP360 bajo nombres engañosos. Tras instalarse, MSP360 fue utilizado para descargar ConnectWise ScreenConnect, creando un segundo canal de acceso remoto. Microsoft no observó explotación de ScreenConnect: las herramientas funcionaban como fueron diseñadas.

SIGNED
software legítimo y firmado

2
canales de administración remota

RMM
persistencia y ejecución remota

TRUST
actividad mezclada con operación normal

LA SEÑAL

Allowlisting basado exclusivamente en firma digital o reputación del fabricante ya no responde toda la pregunta. Una herramienta puede ser legítima y la sesión que la controla no. El atacante aprovecha software administrativo precisamente porque ya tiene capacidades poderosas y apariencia operacional normal.

REVISAR ESTA SEMANA

Definir qué RMM está autorizado, quién puede instalarlo y desde dónde debe conectarse. Alertar instalaciones nuevas o poco frecuentes. Restringir herramientas no aprobadas. Correlacionar RMM con PowerShell, descargas, servicios y credenciales. La pregunta es: ¿esta herramienta debería estar aquí, ahora y bajo este operador?

POR QUÉ CUESTA VERLO

Se parece a operación normal.

El binario puede estar firmado, usar infraestructura legítima del proveedor y comportarse como una herramienta de soporte. La reputación del ejecutable ya no basta.

QUÉ GOBERNAR

No solo el producto.

Producto aprobado, tenant o consola autorizada, instalador permitido, grupo de operadores, ventana de uso y destinos. El contexto administrativo es parte del control.

ALLOWLIST

RMM aprobado por nombre y versión.

OPERATOR

Quién controla la sesión.

INSTALL

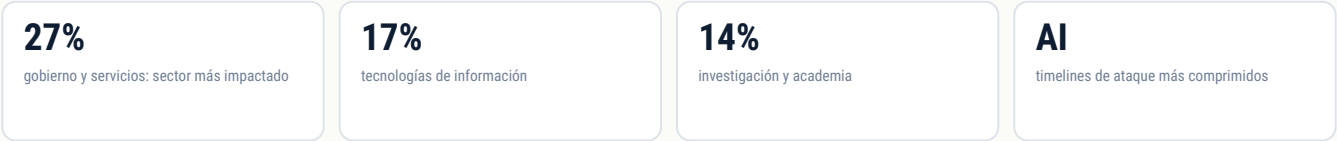
Alta nueva debe generar revisión.

BEHAVIOR

Correlacionar scripts, descargas y credenciales.

Microsoft: las amenazas ya no respetan las fronteras del organigrama

El Microsoft Digital Defense Report 2026 describe un entorno donde infraestructura, identidades, aplicaciones, nube y cadena de suministro deben analizarse como sistemas conectados. El reporte también sostiene que la IA está cambiando la física de la ciberseguridad al comprimir tiempos de ataque y ampliar el acceso a capacidades sofisticadas.

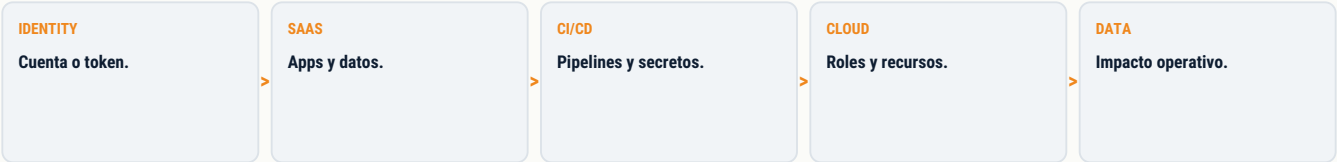


LA SEÑAL

Los incidentes rara vez permanecen en la tecnología donde comenzaron. Una identidad comprometida alcanza SaaS; SaaS alcanza pipelines; pipelines alcanzan nube; un appliance alcanza credenciales; una herramienta administrativa alcanza endpoints. El riesgo real vive en las conexiones.

REVISAR ESTA SEMANA

Seleccionar tres procesos críticos y mapear la cadena completa que los hace posibles: identidad, terceros, aplicaciones, infraestructura, secretos, datos y recuperación. Identificar qué control único puede producir una falla en cascada. Resiliencia también significa impedir que el compromiso de un componente herede automáticamente la autoridad de los demás.



PRUEBA EJECUTIVA Seguir una cadena completa. Elegir un proceso crítico y preguntar: si cae identidad, ¿qué falla después? Si cae SaaS, ¿qué secreto se hereda? Si cae cloud, ¿recovery permanece independiente?	OBJETIVO Romper herencias de confianza. La madurez no exige eliminar dependencias; exige conocerlas, limitar qué autoridad transmiten y probar una ruta alternativa cuando fallen.
--	---

Las seis señales convergen en cuatro planos de control

La superficie cambia, pero el patrón es consistente: cuando el tiempo de explotación se comprime, la organización necesita saber antes qué importa, dónde está expuesta y cómo demuestra que el riesgo dejó de estar abierto.

PLANO 01 / VELOCIDAD Y PRIORIZACIÓN

La decisión empieza antes del parche.

Inventario, exposición, inteligencia de amenazas y criticidad deben convertirse en una sola decisión operacional. La velocidad empieza en saber qué importa.

PLANO 02 / PERÍMETRO Y SUPERFICIE

El perímetro no desapareció: se volvió software.

Citrix y Zimbra muestran que appliances y servicios directamente expuestos pueden convertirse en acceso inicial sin depender de un endpoint tradicional.

PLANO 03 / CONTROLES COMPENSATORIOS

Comprar tiempo no es eliminar la causa.

PeopleSoft recuerda que WAF, firmas y mitigaciones pueden contener una técnica sin corregir la vulnerabilidad. Todo control temporal necesita caducidad.

PLANO 04 / CONFIANZA OPERACIONAL

Legítimo no significa autorizado.

RMM firmado y herramientas conocidas pueden formar parte de una intrusión. La confianza depende de identidad, contexto, intención y comportamiento.

LECTURA ZTC

La ventaja del atacante no siempre proviene de una técnica más sofisticada. Puede provenir de moverse antes de que la organización haya terminado de clasificar el problema. Cuando el tiempo se comprime, inventario, telemetría, segmentación, hunting, recuperación y evidencia forman un mismo mecanismo para comprar tiempo.

SCOPE TIME

Horas para identificar todo activo afectado.

EXPOSED

Superficie internet con owner y versión.

PATCH + HUNT

Cierres con búsqueda de compromiso previo.

EXCEPTION AGE

Antigüedad de mitigaciones temporales.

LECTURA OPERACIONAL

Cuanto más corto es el ciclo del atacante, menos puede depender la defensa de procesos manuales separados. Inventario, threat intelligence, dueño del activo y evidencia de cierre deben encontrarse en el mismo flujo de decisión.

Seis señales, seis estados y respuestas distintas

Responder igual a crecimiento estadístico, explotación activa, una mitigación burlada y una tendencia estratégica produce decisiones deficientes. El estado de la evidencia debe decidir el tipo de acción.

SEÑAL	ESTADO	DECISIÓN CORRECTA
GTIG CVE	TENDENCIA MEDIDA	Sustituir priorización masiva por triage basado en exposición, explotación y criticidad.
CITRIX	EXPLOTACIÓN ACTIVA	Actualizar, contener, buscar compromiso previo y revisar credenciales potencialmente expuestas.
PEOPLESOFT	EXPLOTACIÓN RENOVADA + BYPASS	Corregir la vulnerabilidad real y verificar que el WAF no sea la única barrera.
ZIMBRA	EXPLOTACIÓN OBSERVADA	Actualizar y ejecutar hunting sobre servidores previamente expuestos y configuraciones afectadas.
RMM	ABUSO DE SOFTWARE LEGÍTIMO	Gobernar herramientas administrativas por autorización y comportamiento, no por reputación.
MDDR 2026	INTELIGENCIA ESTRATÉGICA	Mapear interdependencias y rutas de propagación entre identidad, aplicaciones, nube y terceros.

REGLA OPERATIVA

La severidad técnica ayuda a estimar impacto. La explotación demuestra intención adversaria. La exposición determina posibilidad. La criticidad determina consecuencia. La evidencia de cierre demuestra que el riesgo dejó de estar abierto.

LO QUE NO BASTA / 01

Severidad y parche no cierran solos.
CVSS alto no demuestra explotación; parche aplicado no demuestra ausencia de compromiso previo. El estado de evidencia define qué debe probarse.

LO QUE NO BASTA / 02

Confianza y mitigación no equivalen a seguridad.
Firma digital no demuestra uso autorizado; WAF activo no demuestra que la causa raíz haya desaparecido.

DISCIPLINA DE EVIDENCIA

Cada estado exige una acción distinta y una prueba distinta. Si cambia la naturaleza de la evidencia, también debe cambiar el estándar de cierre.

09 / MAPA DE CONTROLES

Ocho controles que conectan la edición 007

No son ocho productos. Son capacidades para reducir el tiempo entre señal, decisión, contención y cierre verificable.

1 / INVENTARIO EXPUESTO

Conocer qué servicios, appliances y aplicaciones están realmente accesibles desde internet.

EXPOSICIÓN · EDGE

2 / PRIORIZACIÓN POR AMENAZA

Combinar CVE, KEV, inteligencia de explotación, criticidad y exposición.

GTIG · VULN MGMT

3 / PATCH + HUNT

En fallas activamente explotadas, corregir y buscar evidencia de compromiso previo.

CITRIX · ZIMBRA

4 / GOBIERNO DE RMM

Inventario permitido, instalación controlada, operador identificado y alertas por herramientas no aprobadas.

RMM · ENDPOINT

5 / DEFENSA DEL EDGE

Appliances, VPN, gateways, correo y portales administrativos con hardening, telemetría y mínimo privilegio.

EDGE · ACCESS

6 / MITIGACIONES CON CADUCIDAD

Todo control temporal debe tener owner, alcance, evidencia, condición de salida y fecha límite.

WAF · EXCEPTIONS

7 / SEGMENTACIÓN DE AUTORIDAD

El acceso inicial a un componente no debe heredar automáticamente credenciales o rutas críticas.

ZERO TRUST · BLAST RADIUS

8 / EVIDENCIA DE CIERRE

Versión corregida, exposición revisada, hunting ejecutado, resultado, owner y riesgo residual.

TODAS LAS SEÑALES

COBERTURA

% de activos internet con owner, versión y criticidad.

SLA REAL

Alerta -> alcance -> contención -> cierre.

EXCEPCIONES

Edad, owner y fecha de salida.

EVIDENCIA

Prueba, hunting y riesgo residual.

DISEÑO DEL CONTROL

Un control maduro debe decir qué evita, quién responde, qué telemetría genera, cómo falla y qué artefacto demuestra que funcionó.

FUENTE / Controles derivados de las fuentes y de principios Zero Trust, exposición, resiliencia y respuesta
zerotrust.consulting

11 / 14

10 / CHECKPOINT EJECUTIVO

Ocho preguntas que dirección debería poder contestar con evidencia

Cada respuesta debe venir acompañada de un artefacto verificable y un responsable. "Sí, lo tenemos" no es evidencia.

01

¿Qué activos expuestos presentan vulnerabilidades bajo explotación activa?

Evidencia: inventario, versión, exposición y fuente de threat intelligence.

02

¿Cuánto tarda una alerta crítica en convertirse en lista completa de activos afectados?

Evidencia: último caso real, timestamps y responsable.

03

Cuando parchamos un activo expuesto, ¿investigamos si fue comprometido antes?

Evidencia: hunting, IOCs, logs y criterio de cierre.

04

¿Qué controles temporales llevan meses funcionando como permanentes?

Evidencia: excepción, owner, riesgo y fecha de retiro.

05

¿Qué herramientas de administración remota están autorizadas?

Evidencia: catálogo, instalación, operador y telemetría.

06

¿Un appliance de borde comprometido puede alcanzar credenciales o redes críticas?

Evidencia: arquitectura, segmentación, cuentas y rutas permitidas.

07

¿Qué proceso crítico depende de una cadena cuya falla conjunta nunca hemos probado?

Evidencia: mapa de dependencias y último ejercicio de recuperación.

08

¿Podemos demostrar cuándo un riesgo dejó realmente de estar abierto?

Evidencia: cambio, prueba, hunting, resultado, aprobación y residual.

SALIDA DEL VIERNES

Ocho respuestas. Ocho responsables. Evidencia verificable. Lo que no puede demostrarse permanece abierto.

FORMATO DE RESPUESTA

ALCANCE + TIMESTAMP + RESPONSABLE + ARTEFACTO + RESULTADO + RIESGO RESIDUAL. Si una respuesta no puede expresarse así, todavía es una opinión o una tarea pendiente; no evidencia de control.

Seis decisiones para comenzar la semana

01	EXPOSICIÓN	Cruzar inventario externo con Citrix, Zimbra, PeopleSoft y vulnerabilidades explotadas relevantes para la organización.
02	PATCH + HUNT	No cerrar activos explotables únicamente con evidencia de parche. Revisar compromiso previo.
03	WAF	Identificar vulnerabilidades cuyo principal control sea una regla compensatoria y establecer plan para eliminar el riesgo raíz.
04	RMM	Descubrir herramientas de administración remota existentes y bloquear o retirar las no autorizadas.
05	VELOCIDAD	Medir tiempo real desde publicación de una alerta hasta identificación, decisión, remediación y cierre.
06	DEPENDENCIAS	Seleccionar un proceso crítico y mapear identidad, aplicaciones, terceros, infraestructura y recuperación end to end.

RADAR MÉXICO / COOPERACIÓN

México y Canadá: inteligencia y ciberseguridad

El 29 de septiembre se anunció intención de fortalecer cooperación e intercambio de experiencias y mejores prácticas, particularmente en inteligencia y ciberseguridad.

RADAR MÉXICO / PQC

Quantum Safe México adquiere estructura institucional

La Asociación de Internet MX instaló el Consejo Consultivo Quantum Safe México. Es una señal institucional; no equivale a regulación ni crea obligaciones por sí sola.

PRIMERAS 24 HORAS

Alcance y exposición

Inventario afectado, versiones, internet exposure, owner y contención temporal.

EN 72 HORAS

Remediación + hunting

Aplicar corrección, revisar compromiso previo, rotar secretos y validar segmentación.

ANTES DEL VIERNES

Cierre verificable

Evidencia, residual, excepciones con fecha y métrica de tiempo de respuesta registrada.

DUEÑOS SUGERIDOS

Vulnerability Management / SecOps para alcance y hunting; dueño de aplicación para remediación; IAM/Network para limitar propagación; Riesgo para aceptar excepciones.

La velocidad ya es el riesgo

La ciberseguridad siempre ha sido una carrera contra el tiempo. Lo distinto es la escala. Miles de vulnerabilidades pueden publicarse en un mes y solo una fracción será explotada. Algunas estarán en software que la organización ni utiliza; otras estarán en el dispositivo que protege su acceso remoto, en el servidor que recibe su correo o en una aplicación que sostiene un proceso crítico.

Intentar responder a todo con la misma urgencia produce una paradoja: cuanto más ruido recibe el equipo, más lentamente puede reaccionar ante lo que realmente importa. La capacidad estratégica consiste en saber qué existe, qué está expuesto, qué se está explotando, qué puede permitir movimiento hacia otro sistema y qué evidencia demuestra que el riesgo quedó contenido.

No gana quien parchea más CVE. Gana quien identifica antes cuál puede convertirse en incidente.

1 / SABER QUÉ IMPORTA

Priorizar por explotación, exposición y criticidad; no por volumen de tickets.

2 / LIMITAR EL RADIO

Diseñar edge, identidad y administración para que una intrusión no herede toda la autoridad.

3 / PARCHEAR Y BUSCAR

Cuando hubo explotación activa, remediar y revisar evidencia de compromiso previo.

4 / DEMOSTRAR EL CIERRE

El riesgo termina cuando existe evidencia verificable, no cuando el ticket cambia a resuelto.

¿Cuánto tarda hoy su organización en convertir una amenaza real en riesgo cerrado?

VELOCIDAD · EXPOSICIÓN · CONTENCIÓN · EVIDENCIA

ZERO TRUST CONSULTING

Dirección editorial: Dr. Juan Pablo Ybarra Llamas

Zero Trust Consulting · Arquitectura · Ciberseguridad · Criptografía · Cumplimiento