

ZTC CYBER INTELLIGENCE

México & Latinoamérica

Aeroméxico: datos bajo investigación
· **Cisco ISE: explotación activa** · **PQC: evidencia local**

**6 señales + 4 capas de análisis
para mejores decisiones**

DESLIZA >

Antes de decidir, comprobar.

Esta semana convergen tres tipos de presión: una posible exposición de datos todavía bajo investigación, explotación confirmada de infraestructura de identidad y un entorno donde la IA comprime el tiempo entre una debilidad y su aprovechamiento. A eso se suman dependencia cloud, cumplimiento traducido a arquitectura y una línea base mexicana de transición post-cuántica que obliga a separar señales de evidencia. Esta edición agrega una segunda capa: cómo se conectan esas señales, qué nivel de certeza tiene cada una y qué evidencia debería exigir dirección antes de considerar un riesgo realmente atendido.

ESTA SEMANA

Buen Gobierno identificó indicios de una posible exposición vinculada con Aeroméxico y anunció el análisis de los datos obtenidos; Cisco confirmó explotación activa de una falla crítica en ISE; Microsoft vuelve a poner el foco en permisos, autenticación y parchado frente a ataques acelerados por IA; AWS publicó una referencia arquitectónica específica para PCI DSS; Salesforce registró una interrupción de Data Cloud ligada a almacenamiento de un tercero; y ZTC Research encontró dependencias criptográficas visibles, pero evidencia PQC local todavía insuficiente para medir madurez organizacional.

LA PREGUNTA DE CADA LUNES

¿Qué decisión crítica estamos tomando hoy sobre una señal que todavía no hemos validado con evidencia suficiente?

01 / MÉXICO + PRIVACIDAD

Aeroméxico: indicios de exposición, investigación en curso

La Secretaría Anticorrupción y Buen Gobierno informó el 20 de septiembre que localizó en Telegram una base supuestamente atribuible a Aeroméxico con más de 15 millones de registros. La autoridad obtuvo una muestra de 100,092 registros e indicó que analizará los datos obtenidos para iniciar de oficio una investigación que permita determinar posibles responsabilidades. Aeroméxico respondió que investiga y que, con la información disponible, no ha identificado exposición de datos financieros, tarjetas o contraseñas.

ALCANCE CORRECTO

La autenticidad, origen, sistema fuente y alcance de la base no están públicamente determinados. La señal verificable hoy es doble: existe una revisión oficial y existe una investigación interna de la empresa. La muestra descrita por la autoridad incluye identificadores útiles para suplantación y fraude contextual. No corresponde tratar la exposición como plenamente confirmada ni descartarla por anticipado; el trabajo correcto es preservar evidencia, reconstruir accesos y validar si hubo extracción.

REVISAR ESTA SEMANA

Validar inventario y minimización de datos personales, accesos a bases de clientes, trazabilidad de exportaciones, retención, terceros y playbooks de comunicación. Preparar vigilancia de phishing y suplantación usando datos que podrían haber quedado expuestos.

02 / IDENTIDAD + INFRAESTRUCTURA

Cisco ISE: una falla crítica ya está siendo explotada

Cisco publicó el 16 de septiembre CVE-2026-76460 en Identity Services Engine (ISE) e ISE-PIC. La vulnerabilidad, con CVSS 10.0, permite a un atacante remoto no autenticado evadir autenticación mediante una API. Cisco confirmó explotación activa, publicó versiones corregidas y señaló que no existe workaround; una explotación exitosa puede llegar a ejecución de comandos con privilegios root.

LA SEÑAL

La infraestructura que decide quién puede entrar también es una superficie crítica. Cuando el plano de identidad falla, la segmentación lógica y las políticas posteriores pueden dejar de ser una barrera suficiente.

REVISAR ESTA SEMANA

Confirmar versiones y parches de todos los nodos ISE/ISE-PIC, restringir tráfico de administración con iACLs, revisar access.log por usuarios sospechosos y correlacionar firewall/network logs externos. Ante indicios, seguir la recomendación del fabricante para reimagen y restauración segura.

03 / IA + CONTROL

La IA cambia la velocidad; los fundamentos siguen decidiendo el impacto

Microsoft señaló el 17 de septiembre que los atacantes están probando más rutas, adaptando técnicas y atravesando identidades, endpoints, aplicaciones, redes y sistemas de IA con mayor velocidad. Las debilidades que permiten el avance siguen siendo conocidas: permisos excesivos, flujos de autenticación débiles, sistemas sin parchear, rutas de ejecución expuestas y controles que no se conectan entre sí.

QUÉ CAMBIA

El riesgo no es que la IA invente una nueva clase de vulnerabilidad cada día, sino que combine debilidades existentes con menos latencia. Un control que funciona solo cuando un analista puede revisar cada paso manualmente puede quedar fuera de tiempo.

REVISAR ESTA SEMANA

Reducir privilegios acumulados, proteger flujos de autenticación resistentes a phishing, cerrar exposición innecesaria, acelerar parchado y conectar telemetría entre identidad, endpoint, cloud y aplicaciones. Incluir identidades de agentes y cuentas de servicio en el mismo gobierno. Medir tiempo real desde la alerta hasta la contención, no solo la existencia del playbook.

04 / PCI DSS + CLOUD

PCI DSS baja del checklist a la arquitectura cloud

AWS publicó el 14 de septiembre un “PCI DSS Deep Dive” de su Security Reference Architecture. El material conecta alcance de cuentas, segmentación, identidad, logging, cifrado y controles por capas con requisitos PCI DSS, e incluye patrones para comercios y proveedores de servicio, diagramas de arquitectura y tablas de mapeo.

POR QUÉ IMPORTA

La señal no es “AWS cumple por el cliente”. Es lo contrario: el cumplimiento efectivo se vuelve una propiedad de diseño. Scope, separación de funciones, trazabilidad, cifrado y respuesta deben quedar reflejados en la arquitectura y luego demostrarse con evidencia operativa.

REVISAR ESTA SEMANA

Dibujar el CDE real, clasificar cuentas en alcance / conectadas / security-impacting / fuera de alcance, verificar segmentación y acceso humano, y comprobar que logs, claves, alertas y evidencias se producen desde la arquitectura, no al final de la auditoría. El objetivo es que el alcance sea demostrable y repetible, no una interpretación reconstruida pocas semanas antes de la evaluación.

05 / CLOUD + RESILIENCIA

Una dependencia de terceros también forma parte de su disponibilidad

Salesforce registró una interrupción de Data Cloud entre el 19 y 20 de septiembre con una duración de 13 horas y 41 minutos. La compañía informó que el problema se originó en un servicio de almacenamiento cloud de un tercero, aplicó un cambio de configuración y preparó una opción de almacenamiento alternativa antes de cerrar el incidente.

LA SEÑAL

La disponibilidad de una plataforma no termina en su propio SLA. Servicios administrados, storage, identidad, telecomunicaciones, APIs y proveedores pueden convertirse en dependencias críticas aunque no aparezcan frente al usuario final.

REVISAR ESTA SEMANA

Mapear dependencias de segundo nivel, RTO/RPO por servicio, alternativas reales, degradación controlada y procedimientos de failover. Probar qué ocurre cuando el proveedor principal está disponible pero una dependencia que habilita una función crítica no lo está. Incluir en el ejercicio quién decide el cambio, cuánto tarda la conmutación y qué evidencia confirma que la recuperación fue completa.

Las dependencias criptográficas se ven; la transición PQC todavía no

La línea base “México ante la Transición Post-Cuántica 2026” de ZTC Research analizó 50 unidades y 500 decisiones entidad-dimensión con evidencia pública. Identificó dependencias criptográficas convencionales en 30 de 50 unidades, pero solo cuatro decisiones PQC técnicamente estimables y localmente atribuibles. El estudio no adjudicó ORS parciales o completos por falta de cobertura suficiente.

ALCANCE CORRECTO

El resultado no significa que México no esté haciendo nada. Significa que la evidencia pública disponible todavía no permite ordenar organizaciones por madurez PQC de manera responsable. Una capacidad global, una mención o un producto no demuestran adopción local.

REVISAR ESTA SEMANA

Iniciar inventario criptográfico, vida útil de datos, dependencias con terceros, capacidad de sustitución de algoritmos y pruebas controladas. Separar “capacidad disponible del proveedor” de “adopción local verificable”. La primera decisión no es “comprar PQC”; es saber exactamente qué tendría que migrarse, quién es dueño de cada dependencia y cuánto tardaría una sustitución controlada.

Las seis señales no están aisladas: convergen en cuatro planos de control

La utilidad de la inteligencia no está en acumular incidentes, sino en identificar qué controles se repiten detrás de problemas distintos. Esta semana, privacidad, identidad, IA, PCI, cloud y PQC vuelven a converger en los mismos cuatro planos: autoridad, arquitectura, dependencia y evidencia.

PLANO 01

Identidad y autoridad

Cisco ISE y las rutas descritas por Microsoft muestran que una identidad válida o una decisión de autorización débil puede convertirse en pivote. Usuarios, administradores, cuentas de servicio y agentes requieren límites verificables.

PLANO 02

Arquitectura y alcance

PCI DSS deja de ser una lista de requisitos cuando el CDE, la segmentación, los flujos y el logging están modelados desde el diseño. El mismo principio aplica a datos personales y a componentes criptográficos.

PLANO 03

Dependencias y continuidad

El incidente de Salesforce recuerda que una función crítica puede depender de infraestructura invisible al usuario. Un SLA directo no describe por sí solo la cadena real de disponibilidad.

PLANO 04

Evidencia y velocidad

Con ataques más rápidos, la organización necesita distinguir en minutos qué está confirmado, qué sigue bajo investigación y qué exige acción inmediata. Sin evidencia conectada, la respuesta se vuelve una discusión de percepciones.

LECTURA ZTC

La madurez no se demuestra por el número de herramientas. Se demuestra cuando identidad, arquitectura, dependencias y evidencia permiten explicar por qué una decisión fue correcta, quién la autorizó y cómo se verificó su cierre.

Seis señales, seis niveles de certeza y seis respuestas distintas

Responder igual a todo produce dos errores: sobrereaccionar ante información incompleta o subestimar hechos ya confirmados. Esta matriz separa el estado de la evidencia del tipo de decisión que corresponde.

SEÑAL	ESTADO	DECISIÓN CORRECTA
Aeroméxico	BAJO INVESTIGACIÓN	Preservar evidencia, validar origen y alcance, revisar exposición y preparar mitigación de abuso sin presentar como confirmado lo que aún no lo está.
Cisco ISE	EXPLOTACIÓN CONFIRMADA	Parchear a release fijo, revisar todos los nodos afectados y ejecutar hunting. Cisco indica CVSS 10.0, acceso remoto no autenticado y ausencia de workaround.
IA + ataques	INTELIGENCIA / GUÍA	Reducir permisos, asegurar autenticación, limitar ejecución y egress, conectar telemetría y medir la velocidad real de respuesta.
PCI + AWS	REFERENCIA ARQUITECTÓNICA	Usarla como patrón y contraste; no como sustituto de la responsabilidad propia, la evaluación de alcance ni la evidencia del control en operación.
Salesforce	INCIDENTE RESUELTO	Actualizar mapas de dependencia, revisar alternativas y probar failover para funciones cuyo proveedor de segundo nivel puede interrumpir el servicio.
PQC México	LÍNEA BASE DE EVIDENCIA	Inventariar criptografía y preparar crypto-agility; evitar convertir ausencia de evidencia pública en afirmación de ausencia de actividad interna.

REGLA OPERATIVA

Mayor gravedad no siempre significa mayor incertidumbre. Cuando la explotación está confirmada, la prioridad es actuar. Cuando el hecho sigue bajo investigación, la prioridad es validar sin perder tiempo ni contaminar la narrativa.

Ocho controles que conectan las seis señales de esta edición

No son ocho productos. Son capacidades que deberían producir evidencia repetible y cruzar varias superficies de riesgo al mismo tiempo.

1. Gobierno de identidades Inventario de identidades humanas, privilegiadas, de servicio y agentes; privilegio mínimo y autenticación resistente a phishing donde sea viable. ISE · IA · PCI	2. Gestión de exposición Inventario confiable, priorización por explotación activa, ventanas de parchado y verificación posterior. La alerta no equivale al cierre. ISE · IA
3. Gobierno de datos Minimización, retención, exportaciones, DLP y trazabilidad suficiente para responder qué datos salieron, por quién, cuándo y hacia dónde. DATOS MX · PCI	4. Segmentación y alcance Flujos documentados, trust boundaries, separación de cuentas y validación técnica de segmentación; no únicamente diagramas. PCI · CLOUD
5. Telemetría correlacionada Logs externos, identidad, endpoint, cloud, aplicaciones y cambios administrativos con retención y sincronización suficientes para reconstrucción. ISE · IA · DATOS MX	6. Resiliencia de terceros Dependencias de segundo nivel, RTO/RPO, degradación controlada, alternativa real y pruebas de conmutación con criterios de éxito. SALESFORCE · PCI
7. Crypto-agility Inventario de algoritmos, llaves, certificados, protocolos, librerías, proveedores, datos de larga vida y capacidad de sustitución controlada. PQC · PCI	8. Evidencia de cierre Owner, fecha, control aplicado, evidencia primaria, prueba negativa/positiva cuando corresponda y aceptación explícita del riesgo residual. TODAS LAS SEÑALES

10 / CHECKPOINT EJECUTIVO

Ocho preguntas que dirección debería poder contestar con evidencia

La conversación cambia cuando cada respuesta debe venir acompañada de un artefacto verificable y un responsable.

01

¿Podemos probar quién exportó o consultó datos sensibles?

Evidencia: logs de acceso/exportación, DLP, IAM y retención.

02

¿Todos los nodos ISE están en una versión fija y fueron revisados?

Evidencia: inventario, versión, fecha de parche, hunting e IOCs.

03

¿Qué identidades o agentes pueden ejecutar acciones autónomas?

Evidencia: owner, permisos, herramientas autorizadas, egress y logs.

04

¿Nuestro alcance PCI existe como arquitectura viva?

Evidencia: CDE, flujos, cuentas, segmentación, accesos y pruebas.

05

¿Conocemos las dependencias de segundo nivel de servicios críticos?

Evidencia: mapa de proveedores, RTO/RPO y último failover probado.

06

¿Sabemos qué criptografía tendríamos que migrar?

Evidencia: algoritmos, llaves, certificados, librerías, protocolos y owner.

07

¿Cuánto tardamos desde una explotación confirmada hasta contener?

Evidencia: SLA operativo y tiempos reales de los últimos casos.

08

¿Qué afirmaciones críticas siguen siendo solo supuestos?

Evidencia: registro de hipótesis, validación pendiente, owner y fecha límite.

SALIDA DEL VIERNES

Ocho respuestas, ocho responsables y evidencia primaria suficiente para sostener cada conclusión. Lo no demostrado permanece abierto, aunque exista confianza interna.

11 / RADAR EJECUTIVO

Seis revisiones para comenzar la semana

01	DATOS MX	Tratar la señal Aeroméxico como investigación abierta: validar exposición, trazabilidad, minimización y riesgo de phishing.
02	ISE	Confirmar parches de Cisco ISE/ISE-PIC y ejecutar hunting en todos los nodos con correlación de logs externos.
03	IA	Medir tiempos de contención y eliminar permisos, rutas de ejecución y exposición que dependan de revisión humana tardía.
04	PCI	Validar que scope, segmentación, identidad, cifrado, logging y evidencia existan en la arquitectura del CDE.
05	RESILIENCIA	Mapear dependencias de segundo nivel y probar alternativa/failover cuando una capacidad cloud de tercero falla.
06	PQC	Empezar por inventario criptográfico, datos de larga vida, terceros y crypto-agility antes de seleccionar tecnología.

SALIDA ESPERADA

Seis responsables, seis decisiones, ocho preguntas ejecutivas contestadas y evidencia verificable de cierre antes del viernes.

La evidencia es una capacidad operativa

Una organización madura no decide por el tamaño del titular ni por el prestigio del proveedor. Distingue señal, evidencia, alcance y acción. Ante una base supuestamente filtrada, no asume ni descarta: valida. Ante explotación confirmada, actúa. Ante un marco de cumplimiento, traduce requisito a arquitectura. Ante una dependencia de terceros, prueba continuidad. Ante PQC, no confunde anuncios con adopción.

La diferencia no está en tener más información, sino en saber qué puede afirmarse, qué debe verificarse y qué exige una respuesta inmediata. La seguridad ejecutiva empieza cuando el nivel de certeza determina el tipo de decisión.

¿Qué decisión crítica de esta semana puede demostrar con evidencia, no solo con confianza?

ZEROTRUST.CONSULTING