

ZTC CYBER INTELLIGENCE

México & Latinoamérica

STORM-3168 · AGENTES · FIPS 140-2 · PQC

CUANDO LA AUTORIDAD SE VUELVE RIESGO

Producción borrada en minutos · agentes con permisos reales
· transición FIPS · PQC entra al acceso empresarial

6 señales · 4 capas de análisis
8 controles · 8 preguntas ejecutivas

LECTURA EJECUTIVA >

Edición 006 · 28 de septiembre de 2026

MENOS TITULARES. MÁS CONTEXTO PARA DECIDIR.

La confianza cambia de capa.

La seguridad empresarial ya no puede modelarse solo alrededor del usuario humano. Esta semana, Microsoft documentó actividad destructiva en Azure mediante service principals comprometidos; CISA llevó a KEV cuatro fallas explotadas en infraestructura de seguridad y conectividad; y Zenity mostró cómo un agente puede convertir datos no confiables en acciones con identidad propia. Al mismo tiempo, el CMVP de NIST alcanzó el hito que mueve FIPS 140-2 a Historical para sistemas nuevos, mientras IETF y OpenSSL empujan PQC hacia autenticación de red y runtimes reales. En México y Latinoamérica, los pagos digitales siguen creciendo: la superficie de confianza crece con ellos.

ESTA SEMANA

Microsoft observó una secuencia destructiva automatizada sobre Azure; CISA confirmó explotación activa de cuatro fallas en Check Point, Arista VeloCloud y F5; Zenity Labs publicó SalesBleed tras validar las correcciones; NIST movió los certificados FIPS 140-2 a Historical para nuevos sistemas; IETF llevó PQC a EAP-TLS y OpenSSL 4.1 beta optimizó ML-KEM/ML-DSA; y nuevas señales sobre pagos digitales muestran que crecimiento y confianza deben avanzar juntos.

LA PREGUNTA DE CADA LUNES

¿Qué identidad no humana, agente, módulo criptográfico o dependencia puede actuar hoy con más autoridad de la que la organización puede explicar y demostrar?

Storm-3168: una identidad de servicio puede borrar producción en minutos

Microsoft Security Research publicó el 25 de septiembre actividad asociada a Storm-3168 en Azure. En el tenant analizado, dos service principals comprometidos realizaron descubrimiento, operaciones destructivas y recolección de credenciales. Una de las secuencias destructivas duró aproximadamente siete minutos; Microsoft observó más de 150 operaciones destructivas o de recolección en 35 minutos, incluyendo eliminación de cuentas de Storage, Key Vault y recursos de App Service, además de intentos contra SQL y mecanismos de recuperación.

2

service principals comprometidos

7 min

secuencia destructiva

150+

operaciones destructivas / credenciales

30+

ListKeys exitosos después

ALCANCE CORRECTO

Microsoft no confirmó el vector inicial. Un client secret de la organización había aparecido previamente en texto plano dentro del historial de edición de un issue público de GitHub, pero el informe no atribuye de forma concluyente la actividad a ese secreto. La lección verificable es otra: una workload identity con permisos amplios puede ejecutar impacto masivo sin una sesión humana interactiva.

REVISAR ESTA SEMANA

Inventariar service principals, managed identities y secretos de aplicaciones; eliminar credenciales de larga vida cuando sea posible; rotar cualquier secreto alguna vez expuesto; revisar RBAC efectivo, grupos y permisos heredados; proteger backup y recovery con controles independientes; y alertar sobre borrado masivo, ListKeys y cambios a locks. La capacidad de restaurar debe sobrevivir a la identidad que administra producción.

CISA: el perímetro de seguridad también está bajo explotación activa

El 22 de septiembre CISA agregó cuatro vulnerabilidades al catálogo Known Exploited Vulnerabilities por evidencia de explotación activa: dos fallas en productos Check Point, una en Arista VeloCloud Orchestrator y una en F5 BIG-IP APM. La concentración importa porque son componentes que participan en administración de seguridad, conectividad, acceso remoto o control de tráfico.

4 vulnerabilidades añadidas a KEV	2 productos Check Point	1 Arista VeloCloud Orchestrator	1 F5 BIG-IP APM
---	-----------------------------------	---	---------------------------

LA SEÑAL

Cuando un producto existe para proteger, autenticar o administrar infraestructura, su compromiso puede ampliar el radio de impacto. KEV no significa que todos los equipos del mundo hayan sido comprometidos; significa que existe evidencia de explotación real y que la priorización debe considerar exposición y posibilidad de compromiso previo, no solo severidad teórica.

REVISAR ESTA SEMANA

Cruzar inventario con los cuatro CVE, confirmar exposición a internet y versión, aplicar la mitigación del fabricante y conservar evidencia del cierre. Para activos previamente expuestos, ejecutar triage forense: parchear no demuestra por sí solo que el sistema no fue explotado antes. Registrar fecha de exposición, fecha de corrección, hunting realizado y criterio de cierre.

SalesBleed: cuando datos no confiables se convierten en acciones

Zenity Labs publicó el 24 de septiembre una investigación sobre Agentforce en Slack. El equipo encontró que la acción "Reply to a Slack Thread" podía ejecutarse sin confirmación del usuario y sin atribución clara del invocador. Combinada con un bypass de redacción de URLs descrito por los investigadores, la ruta podía permitir que instrucciones maliciosas llegaran al agente y terminaran en mensajes de phishing emitidos con la identidad del propio agente. Zenity indicó que Salesforce corrigió los hallazgos y que las correcciones fueron confirmadas antes de la publicación.

SLACK canal interno de confianza	WRITE acción con capacidad de escritura	0 confirmación antes del fix	21 SEP fixes confirmados y probados
--	---	--	---

POR QUE IMPORTA

El problema general no es un chatbot que "se equivoca". Es un sistema que puede leer datos no confiables, interpretarlos como instrucciones y después usar acciones internas con permisos reales. La autoridad del agente debe evaluarse por acción, contexto, destino y dato involucrado, no solo por el hecho de que el agente esté autenticado.

REVISAR ESTA SEMANA

Clasificar fuentes externas como no confiables; separar acciones de lectura y escritura; exigir confirmación humana para operaciones de impacto; mantener atribución del invocador; limitar egress y destinos; aplicar mínimo privilegio a herramientas del agente; y conservar logs que permitan reconstruir quién inició la acción, qué contexto recibió el agente y que herramienta ejecutó.

FIPS 140-2 ya es Historical para sistemas nuevos

NIST establece que los módulos validados bajo FIPS 140-2 podían seguir siendo aceptados para sistemas nuevos hasta el 21 de septiembre de 2026. A partir del 22 de septiembre, las validaciones FIPS 140-2 pasan a la lista Historical; los organismos federales de Estados Unidos pueden seguir usando esos módulos en sistemas existentes según evaluación de riesgo, pero las nuevas implementaciones deben mirar a FIPS 140-3. Historical no equivale a revoked.

21 SEP último día para nuevos sistemas con 140-2	22 SEP 140-2 pasa a Historical	140-3 referencia para nuevos sistemas	HIST. no equivale a revoked
--	--	---	---------------------------------------

ALCANCE CORRECTO

La validación pertenece al módulo criptográfico y a su configuración validada, no automáticamente a todo producto que lo incorpora. Tampoco una etiqueta "FIPS" demuestra por sí sola que el despliegue real usa el módulo, versión, modo y configuración que soportan la afirmación de cumplimiento.

REVISAR ESTA SEMANA

Inventariar módulos y certificados CMVP reales, no solo productos; identificar dependencias FIPS 140-2 en proyectos nuevos; exigir roadmap FIPS 140-3 a proveedores; mapear HSM, librerías, appliances y servicios cloud a su evidencia de validación; y documentar excepciones de legado con owner, fecha de retiro y riesgo aceptado.

PQC llega a EAP-TLS: la transición entra al acceso empresarial

El 23 de septiembre el grupo EMU del IETF publicó la revisión 02 de un Internet-Draft para incorporar criptografía post-cuántica a métodos EAP basados en TLS, incluyendo EAP-TLS, EAP-TTLS, PEAP y TEAP. El documento también trata el aumento de tamaño de certificados y cadenas, un problema práctico en autenticación de red. Ese mismo día OpenSSL anunció la beta de 4.1 con optimizaciones de ML-KEM y ML-DSA para varias arquitecturas, incluyendo x86_64, ppc64le y s390x.

4

métodos EAP cubiertos

DRAFT -02

IETF work in progress

23 SEP

publicación del draft

4.1 BETA1

OpenSSL con optimizaciones PQC

ALCANCE CORRECTO

El documento de IETF es trabajo en progreso, no un estándar final. La señal es operativa: PQC ya está tocando protocolos de acceso, tamaños de handshake, compatibilidad y rendimiento. La pregunta deja de ser solo "qué algoritmo" y pasa a "qué ocurre cuando ese algoritmo atraviesa Wi-Fi, RADIUS, NAC, certificados, supplicants y hardware real".

REVISAR ESTA SEMANA

Construir un laboratorio de interoperabilidad con EAP real; medir tamaño de certificados, fragmentación, round trips, latencia y fallos; identificar equipos y librerías que no soporten los nuevos parámetros; y separar pruebas de capacidad del proveedor de una decisión de producción. Crypto-agility incluye poder probar y revertir sin romper autenticación.

Pagos digitales: 97% de adopción en la muestra; el fraude frena expansión

El 24 de septiembre, la Presidencia de México describió una propuesta de Ley de Economía Digital cuyo objetivo incluye acelerar pagos digitales mediante el teléfono móvil. Dos días antes, Mastercard publicó un estudio regional con 2,400 propietarios y tomadores de decisión de PyMEs en 12 países de América Latina y el Caribe: 97% de la muestra ya acepta pagos digitales y aproximadamente la mitad dijo que el temor al fraude y los ciberataques limita una mayor expansión digital.

2,400 PyMEs encuestadas	12 países de América Latina y Caribe	97% ya acepta pagos digitales	~50% temor a fraude/ciberataques frena crecimiento
-----------------------------------	--	---	--

ALCANCE CORRECTO

La propuesta mexicana es una iniciativa de política pública y el estudio de Mastercard describe una muestra regional; ninguno de los dos elementos, por sí solo, permite inferir el nivel de seguridad de todas las empresas mexicanas. Juntos sí muestran una tensión relevante: la infraestructura de pago puede expandirse más rápido que la confianza operativa de quienes la usan.

REVISAR ESTA SEMANA

Para organizaciones que incorporan o amplían pagos digitales: mapear autenticación, antifraude, chargebacks, APIs, terceros, datos personales y continuidad; medir fraude por canal y no solo volumen de transacciones; probar recuperación ante indisponibilidad; y asegurar que el crecimiento de aceptación venga acompañado de telemetría, límites y respuesta verificable.

Las seis señales convergen en cuatro planos de control

La superficie cambia, pero los patrones de control se repiten. Esta semana la autoridad ya no vive solo en usuarios: también reside en service principals, agentes, módulos criptográficos, protocolos y rails de pago.

PLANO 01 / IDENTIDAD Y AUTORIDAD

Service principals y agentes muestran que las identidades no humanas necesitan owner, permisos mínimos, ciclo de vida y límites por acción. Autenticado no significa autorizado para todo.

PLANO 02 / EXPOSICION Y CONTROL

KEV recuerda que firewalls, VPN, gestores y control planes también son superficie atacable. Parchar debe incluir validación de exposición previa y evidencia forense suficiente.

PLANO 03 / CRIPTOGRAFIA Y CAMBIO

FIPS 140-2 -> 140-3 y PQC en EAP demuestran que la criptografía tiene dependencias, ciclos de vida e interoperabilidad. Inventario y crypto-agility son capacidades operativas, no documentos.

PLANO 04 / RECUPERACION Y EVIDENCIA

Ataques automatizados y pagos más digitales exigen restaurar, detectar fraude y explicar decisiones con evidencia. La recuperación debe seguir funcionando aún cuando una identidad privilegiada sea comprometida.

LECTURA ZTC

La frontera ya no es "dentro" contra "fuera". Es autoridad explícita contra autoridad implícita. Cuanto más automatizada es la operación, más importante resulta demostrar que cada identidad, agente, módulo y proveedor solo puede hacer lo que la arquitectura pretende - y que el cierre se verifica con evidencia.

Seis señales, seis estados de evidencia y respuestas distintas

Responder igual a una explotación confirmada, una investigación corregida, una transición normativa y un borrador de estándar produce decisiones deficientes. El estado de la evidencia debe decidir el tipo de acción.

SEÑAL	ESTADO	RESPUESTA CORRECTA
Storm-3168	ACTIVIDAD OBSERVADA	Reducir autoridad de workload identities, rotar secretos, proteger recovery y revisar telemetría de acciones destructivas.
CISA KEY	EXPLOTACION CONFIRMADA	Parchar/mitigar, validar exposición y ejecutar triage por posible compromiso previo en activos afectados.
SalesBleed	INVESTIGACION + FIX VALIDADO	Verificar configuraciones y extraer el patron: datos no confiables, acciones de escritura, confirmación, atribución y egress.
FIPS 140-2	TRANSICIÓN PROGRAMATICA EFECTIVA	Evitar FIPS 140-2 en nuevos sistemas federales; mapear módulos reales y plan de migración a 140-3.
PQC + EAP	IETF DRAFT + BETA	Probar interoperabilidad y rendimiento; no tratar trabajo en progreso o beta como estándar final de producción.
Pagos digitales	PROPUESTA + ENCUESTA REGIONAL	Usar como señal de planeación: reforzar antifraude, APIs, terceros, continuidad y telemetría a medida que crece la adopción.

REGLA OPERATIVA

La severidad define urgencia; el estado de la evidencia define como actuar. Explotacion confirmada exige contención. Un draft exige prueba. Una corrección validada exige verificar configuración. Una transición normativa exige inventario y plan.

Ocho controles que conectan la edición 006

No son ocho productos. Son capacidades que producen evidencia y reducen el radio de acción de identidades, agentes, dependencias y cambios criptográficos.

1. Gobierno de workload identities

Owner, inventario, RBAC efectivo, secretos, managed identities, rotación y alertas por acciones destructivas.

STORM-3168 · CLOUD

2. Gestión de exposición

Inventario confiable, internet exposure, KEV, parchado, mitigación y triage posterior.

KEV · INFRA

3. Gobierno de agentes

Permisos por herramienta, separación read/write, confirmación, atribución, egress y registro de tool calls.

SALESBLEED · IA

4. Ciclo de vida de secretos

No basta borrar una publicación: secretos expuestos se revocan/rotan y se investiga su uso histórico.

CLOUD · AGENTES

5. Recuperación independiente

Backup, locks, immutability, break-glass y restore que no dependen de la misma identidad que administra producción.

STORM-3168

6. Gobierno de módulos criptográficos

Mapeo producto -> módulo -> certificado -> versión/configuración; roadmap FIPS 140-3.

FIPS · CUMPLIMIENTO

7. Crypto-agility e interoperabilidad

Algoritmos, certificados, EAP/TLS, librerías, performance, compatibilidad y rollback probado.

PQC · EAP

8. Evidencia de cierre

Owner, cambio aplicado, prueba, telemetría, resultado, riesgo residual y fecha de nueva validación.

TODAS LAS SEÑALES

Ocho preguntas que dirección debería poder contestar con evidencia

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

01

Qué workload identities pueden borrar, listar llaves o cambiar recursos críticos?

Evidencia: inventario, owner, RBAC efectivo y última revisión.

02

Alguna credencial estuvo expuesta alguna vez en repositorios, issues o logs?

Evidencia: secret scanning, revocacion, rotación e investigación de uso.

03

Los activos afectados por KEV estan corregidos y fueron revisados por compromiso previo?

Evidencia: versión, fecha, exposición, hunting e IOCs.

04

Qué agentes pueden ejecutar acciones de escritura sin confirmación humana?

Evidencia: catálogo de tools, permisos, confirmación, atribución y egress.

05

Qué dependencia FIPS 140-2 sigue en proyectos o adquisiciones nuevas?

Evidencia: módulo, certificado CMVP, estado y roadmap 140-3.

06

PQC fue probado sobre autenticación de red real, no solo en una librería?

Evidencia: EAP/TLS, certificados, latencia, fallos, compatibilidad y rollback.

07

El crecimiento de pagos digitales tiene telemetría y antifraude equivalentes?

Evidencia: métricas por canal, límites, alertas, APIs y terceros.

08

Podemos restaurar si una identidad privilegiada intenta destruir recovery?

Evidencia: último restore, controles independientes, RTO/RPO y break-glass.

SALIDA DEL VIERNES

Ocho respuestas, ocho responsables y evidencia primaria suficiente para demostrar autoridad, corrección y recuperación. Lo no probado permanece abierto.

Seis decisiones para comenzar la semana

- 01

WORKLOAD ID

Reducir permisos de service principals, rotar secretos expuestos y validar protecciones independientes de recovery.
- 02

KEV

Cruzar inventario con Check Point, Arista VeloCloud y F5; corregir y ejecutar triage en activos previamente expuestos.
- 03

AGENTES

Revisar acciones de escritura, confirmación humana, atribución, herramientas autorizadas y egress de agentes.
- 04

FIPS

Identificar módulos FIPS 140-2 en nuevos proyectos y exigir evidencia concreta de FIPS 140-3 donde corresponda.
- 05

PQC

Probar EAP/TLS, tamaños de certificados, compatibilidad, rendimiento y rollback; tratar el IETF draft como trabajo en progreso.
- 06

PAGOS

Alinear expansión digital con antifraude, APIs seguras, terceros, continuidad y telemetría verificable.

SALIDA ESPERADA

Seis responsables, seis decisiones y evidencia de cierre antes del viernes. La meta no es "revisar"; es reducir autoridad innecesaria, corregir exposición y demostrar que recovery y criptografía pueden cambiar sin perder control.

PERSPECTIVA ZTC

La confianza cambia de capa

Un usuario ya no es la única entidad capaz de ejecutar una decisión. Service principals descubren y borran recursos; agentes leen datos y publican mensajes; módulos criptográficos sostienen cumplimiento; protocolos determinan interoperabilidad; proveedores y rails de pago extienden la cadena de confianza. La arquitectura madura cuando esa autoridad está explícitamente delimitada, registrada y recuperable. La nueva pregunta no es cuantas herramientas de seguridad existen, sino cuantas acciones críticas pueden ocurrir sin que podamos explicar quién - o que - tuvo autoridad, que evidencia dejó y como se revierte el impacto. En un entorno más automatizado, mínimo privilegio, crypto-agility, recovery independiente y evidencia dejan de ser buenas prácticas aisladas: forman un mismo sistema de control.

Qué componente no humano puede hoy actuar con más autoridad de la que su organización puede demostrar?

AUTORIDAD · EXPOSICIÓN · CRYPTO-AGILITY · RECUPERACIÓN

Z E R O T R U S T C O N S U L T I N G

Dirección editorial: Dr. Juan Pablo Ybarra Llamas

Zero Trust Consulting · Arquitectura · Ciberseguridad · Criptografía · Cumplimiento