ZTC CYBER INTELLIGENCE

México & Latinoamérica

CISA + G7: migrar a PQC ahora · pagos bajo ataque · confianza digital

6 señales para iniciar la semana con mejores decisiones

DESLIZA >

Edición 003 · 7 de septiembre de 2026

00 / PROPÓSITO EDITORIAL

Confiar en el canal ya no basta.

Esta semana, la señal más fuerte no es una sola vulnerabilidad. Es que la autoridad y la confianza están cambiando de lugar: criptografía, autenticación, pagos, colaboración e infraestructura de terceros dependen cada vez más del contexto que rodea una acción.

ESTA SEMANA

CISA y el G7 llaman a iniciar la migración PQC; la CNBV incorpora SMS como canal para un Factor de Autenticación Categoría 3 en ciertos flujos; atacantes manipulan infraestructura de pagos en Brasil; la IA aparece en campañas regionales; Teams se usa para falso soporte; y un proveedor financiero confirma un incidente iniciado por vishing.

LA PREGUNTA DE CADA LUNES

¿Qué acción crítica puede ejecutarse hoy en la organización solo porque el canal o la credencial parecen legítimos?

FUENTES / CISA · CNBV/DOF · Google GTIG/Mandiant · Unit 42 · Microsoft · Jack Henry

01 / PQC + POLÍTICA PÚBLICA

CISA y el G7 piden empezar la transición PQC ahora

El 3 de septiembre, CISA y el G7 Cyber Security Working Group publicaron un llamado conjunto que subraya la urgencia de que organizaciones y gobiernos comiencen la transición a criptografía postcuántica para proteger datos sensibles, autenticación y activos críticos.

ALCANCE CORRECTO

No es una obligación general para el sector privado. Es un llamado coordinado a organizaciones públicas y privadas para adoptar una migración gradual y basada en riesgo.

REVISAR ESTA SEMANA

Asignar responsable. Inventariar activos criptográficos. Identificar sistemas críticos y datos de larga vida. Mapear dependencias. Definir una hoja de ruta de transición y criterios de compra compatibles con PQC.

FUENTE / CISA + G7 Cyber Security Working Group · 3 sep 2026

02 / MÉXICO + AUTENTICACIÓN

La CNBV amplía el canal para autenticación bancaria

La CNBV modificó las disposiciones para comisionistas de base tecnológica. Un Factor de Autenticación Categoría 3 podrá enviarse por correo, mensajería instantánea cifrada o a un número móvil habilitado para SMS. Para ciertas consultas de saldos y movimientos podrá requerirse solo el Factor Categoría 2.

POR QUE IMPORTA

El cambio no es solo de experiencia de usuario. Cada nuevo canal incorpora dependencias: enrolamiento del número, modificación del contacto, recuperación, operador móvil, dispositivo, ingeniería social y monitoreo de fraude.

REVISAR ESTA SEMANA

Mapear alta, cambio y recuperación del medio de contacto. Confirmar alertas ante modificaciones, correlación de dispositivo y comportamiento transaccional, revocación y controles contra fraude o SIM swapping.

FUENTE / CNBV · Diario Oficial de la Federación · 1 sep 2026

03 / BRASIL + PAGOS

El objetivo ya no es el cliente. Es la capacidad de ordenar el pago

Google GTIG y Mandiant detallaron las operaciones de BREEZE COMET contra organizaciones brasileñas con permiso para operar software bancario, APIs y sistemas como Pix, STR y Boleto. El actor busca cuentas privilegiadas, credenciales mTLS y acceso a aplicaciones financieras centrales.

LA EVIDENCIA

En un caso, dentro de las 24-48 horas posteriores al acceso a aplicaciones financieras centrales, el actor ejecutó dos oleadas de cientos de transacciones fraudulentas.

DECISION

Separar identidad humana, identidad de workload, credenciales mTLS, permisos de API y contexto transaccional. Una conexión autenticada no demuestra por sí sola que la operación sea legítima.

FUENTE / Google Threat Intelligence Group + Mandiant · 1 sep 2026

04 / LATINOAMÉRICA + IA

La IA ya está dentro del playbook criminal regional

Unit 42 analizó dos campañas de intrusión y exfiltración dirigidas a América Latina: una con impacto en transporte, gobierno y servicios de agua en México y Ecuador; otra contra el sector financiero de Brasil. Los operadores usaron técnicas LotL, túneles, RATs y modelos comerciales para superar obstáculos tácticos.

DISTINCION IMPORTANTE

La publicación es nueva, pero parte de la actividad descrita ocurrió antes. La señal de esta semana es la evidencia pública más concreta de IA incorporada a operaciones criminales dirigidas específicamente contra organizaciones latinoamericanas.

REVISAR ESTA SEMANA

Buscar en telemetría PowerShell anómalo, LotL, SOCKS5, túneles, DNS dinámico, egress no esperado, extracción de credenciales y comportamientos de persistencia. La IA acelera; los fundamentos siguen detectando.

FUENTE / Palo Alto Networks Unit 42 · 3 sep 2026

05 / IDENTIDAD + COLABORACIÓN

El falso soporte técnico ya puede tocar la puerta dentro de Teams

Microsoft observó una campaña que abusa de la colaboración externa de Teams para hacerse pasar por TI o helpdesk. El objetivo es convencer al usuario de otorgar una sesión remota; después aparecen PowerShell, un MSI malicioso, Node.js, reconocimiento de Active Directory y movimiento lateral por WinRM.

LO INCOMODO

El ataque funciona porque utiliza componentes que el usuario reconoce: Teams, soporte remoto, Windows Installer, Node.js y protocolos administrativos. Un canal corporativo real no autentica a la persona al otro lado.

REVISAR ESTA SEMANA

Restringir colaboración externa, verificar soporte por un canal conocido, controlar Quick Assist/RMM, exigir MFA resistente a phishing y limitar WinRM a estaciones administrativas autorizadas.

FUENTE / Microsoft Security Research · 2 sep 2026

06 / FINTECH + TERCEROS

No producción no significa no sensible

Jack Henry confirmó un incidente en una porción limitada de su entorno corporativo interno y no productivo. No reportó acceso o interrupción de plataformas core o servicios de procesamiento, pero indicó que PII asociada con menos de diez clientes fue afectada.

CAUSA INICIAL

La investigación atribuyó el acceso a vishing iniciado por ShinyHunters. La compañía también reportó un intento de extorsión y dijo que sus controles detectaron y contuvieron la actividad.

DECISION DE TERCEROS

Cuando un proveedor reporta un incidente, pedir evidencia por alcance: ambiente, datos, identidades, periodo, clientes afectados, rutas descartadas y acciones de contención. Servicio disponible no equivale a riesgo cerrado.

FUENTE / Jack Henry & Associates · 31 ago 2026

07 / RADAR EJECUTIVO

Seis revisiones para comenzar la semana

01	PQC	Asignar responsable, inventariar criptografía y definir una ruta de transición basada en riesgo.
02	AUTENTICACIÓN	Revisar alta, cambio y recuperación de número móvil en flujos que usen SMS.
03	PAGOS	Identificar identidades y aplicaciones que pueden ordenar transacciones y controles independientes de legitimidad.
04	LATAM	Hacer threat hunting sobre LotL, túneles, SOCKS5, PowerShell y egress no esperado.
05	COLABORACIÓN	Validar quién puede contactar usuarios desde tenants externos y cómo se autentica soporte remoto.
06	TERCEROS	Exigir alcance por ambiente, datos, identidades y rutas cuando un proveedor reporte un incidente.

SALIDA ESPERADA

Seis responsables, seis decisiones y evidencia de cierre.

PERSPECTIVA ZTC

La confianza no debería heredarse del canal

Un SMS puede ser auténtico. Una sesión de Teams puede ser real. Una credencial mTLS puede ser válida. Un proveedor puede seguir operando. Y aun así, la acción puede no ser legítima.

La siguiente etapa de la arquitectura de seguridad necesita comprobar no solo quién puede hacer algo, sino si debería poder hacerlo en ese momento, sobre ese activo y bajo ese contexto.

¿Qué acción crítica puede ejecutarse hoy en la organización solo porque el canal o la credencial parecen legítimos?

ZEROTRUST.CONSULTING

Dirección editorial: Dr. Juan Pablo Ybarra Llamas
Zero Trust Consulting · Arquitectura · Ciberseguridad · Criptografía · Cumplimiento