ZTC CYBER INTELLIGENCE

México & Latinoamérica

Banxico en pagos · piloto PQC internacional · explotación activa

6 señales para iniciar la semana con mejores decisiones

DESLIZA >

Edición 002 · 31 de agosto de 2026

00 / PROPÓSITO EDITORIAL

Menos titulares. Más contexto para decidir.

ZTC CYBER INTELLIGENCE interpreta qué ocurrió, qué significa para México y Latinoamérica y qué merece una decisión ejecutiva.

ESTA SEMANA

Banxico abre una segunda consulta para cámaras de pagos; un piloto lleva firmas postcuánticas a pruebas financieras; y varias alertas confirman explotación activa en correo, IA, nube y software empresarial.

LA PREGUNTA DE CADA LUNES

¿Qué cambió esta semana y qué debería revisar hoy una organización mexicana o latinoamericana?

01 / MÉXICO + PAGOS

Banxico revisa las reglas de las cámaras de pagos

La segunda consulta propone cambios en interoperabilidad, competencia, gobierno, continuidad y ciberseguridad.

POR QUÉ IMPORTA

Las cámaras son infraestructura crítica para el procesamiento de tarjetas. Sus decisiones técnicas afectan conexiones, terceros, evidencias y capacidad de cambiar de proveedor.

REVISAR ESTA SEMANA

Determinar si la organización opera, contrata o depende de una cámara; comparar impactos técnicos y contractuales; y evaluar observaciones antes del 24 de septiembre.

FUENTE / Banco de México · 27 ago 2026

02 / CRIPTOGRAFÍA Y PQC

Las firmas postcuánticas llegan a pruebas financieras

Safeheron y RFI anunciaron un piloto con ML-DSA-65 para wallets y transferencias de activos digitales sobre una red de prueba de NEAR.

ALCANCE CONFIRMADO

Los bancos evalúan la tecnología y los reguladores observan la primera fase. Es un piloto de activos digitales: no forma parte de Banxico ni del procesamiento de tarjetas.

PREPARARSE SIN CONFUNDIR FUNCIONES

Inventariar firmas, encapsulación y custodia por separado. ML-DSA protege firmas digitales; no sustituye un mecanismo de establecimiento de llaves.

FUENTE / Anuncio de Safeheron y Responsible Fintech Institute · 24 ago 2026

03 / LATINOAMÉRICA + AMENAZAS

Zimbra exige una respuesta más allá del parche

CTIR Brasil alertó sobre CVE-2026-73570, incluida en CISA KEV y presente en versiones anteriores a 10.1.20.

POR QUÉ IMPORTA

Correo y colaboración concentran identidad, conversaciones y recuperación de cuentas. La inclusión en KEV significa que existe evidencia de explotación en entornos reales.

REVISAR ESTA SEMANA

Identificar versiones expuestas, actualizar inmediatamente y revisar accesos, sesiones, reglas de correo, cuentas administrativas e indicadores anteriores a la corrección.

FUENTE / CTIR Gov Brasil · Alerta 78/2026 · 28 ago 2026

04 / IA + NUBE + IDENTIDAD

La infraestructura de IA ya es un objetivo directo

Microsoft observó intrusiones contra LiteLLM, RAGFlow y Kestra orientadas a credenciales, persistencia y monetización de cómputo.

EL PUNTO DE CONCENTRACIÓN

Gateways y orquestadores pueden reunir llaves de proveedores, bases de datos, automatizaciones, secretos y permisos de ejecución en un solo contexto.

REVISAR ESTA SEMANA

Inventariar servicios expuestos; corregir versiones; restringir administración y salida a internet; rotar secretos; y buscar shells, cambios de archivos y uso anómalo de contenedores.

FUENTE / Microsoft Security Research · 26 ago 2026

05 / RESILIENCIA OPERATIVA

La segmentación convierte un incidente mayor en uno acotado

ATF reportó un incidente en un sistema independiente, cortó sus conexiones e inició actividades forenses.

LA EVIDENCIA DISPONIBLE

La agencia afirmó que el sistema afectado operaba separado de su red empresarial y que no había indicios de impacto en eForms u otros sistemas.

PROBAR ANTES DEL INCIDENTE

Validar límites de red, credenciales compartidas, rutas administrativas, capacidad de corte, telemetría y evidencia contra movimiento lateral.

FUENTE / ATF · 26 ago 2026

06 / EXPLOTACIÓN ACTIVA

KEV cambia la prioridad de tres tecnologías empresariales

CISA añadió fallas de ownCloud, Linux Kernel y JFrog Artifactory a su catálogo de vulnerabilidades explotadas.

POR QUÉ IMPORTA

El lote atraviesa almacenamiento, sistemas operativos y cadena de software. La explotación confirmada debe pesar más que la puntuación aislada de severidad.

REVISAR ESTA SEMANA

Inventariar ownCloud, Linux y Artifactory; confirmar exposición y versiones; preservar registros; corregir; reiniciar donde corresponda; y buscar actividad previa.

FUENTE / CISA Known Exploited Vulnerabilities · 27 ago 2026

07 / RADAR EJECUTIVO

Cinco revisiones para comenzar la semana

01 PAGOS Identificar dependencias con cámaras y cambios sujetos a consulta.

02 PQC Separar inventarios de firmas, encapsulación, llaves y custodia.

03 CORREO Actualizar Zimbra y buscar señales anteriores al parche.

04 IA Tratar gateways y orquestadores como infraestructura privilegiada.

05 EXPOSICIÓN Priorizar KEV y demostrar que la segmentación contiene.

PERSPECTIVA ZTC

El riesgo se concentra en los puntos de control

Cámaras de pagos, llaves criptográficas, correo, gateways de IA, repositorios y límites de red comparten una característica: concentran confianza y multiplican el impacto de una falla.

¿Qué componente concentra hoy más confianza de la que la organización puede demostrar?

ZEROTRUST.CONSULTING

Dirección editorial: Juan Pablo Ybarra Llamas
linkedin.com/company/zerotrustconsulting