ZTC CYBER INTELLIGENCE

México & Latinoamérica

México: Ley de Ciberseguridad · Revolut: autoridad suplantada · IA en horas

6 señales para iniciar la semana con mejores decisiones

DESLIZA >

Edición 004 · 14 de septiembre de 2026

00 / PROPÓSITO EDITORIAL

La autoridad aparente tampoco basta.

Un dominio oficial, una cuenta recuperada, una sesión cloud o un componente empresarial crítico pueden parecer legítimos y, aun así, estar en el centro de una operación adversaria. Las seis señales de esta semana convergen en una idea: validar la autoridad y el contexto, no solo la identidad que presenta una acción.

ESTA SEMANA

En México se presenta una nueva iniciativa de Ley de Ciberseguridad; Revolut confirma divulgación de datos tras solicitudes falsas enviadas desde un dominio gubernamental legítimo; Google observa ataques asistidos por agentes ejecutados en menos de seis horas; npm introduce una pausa de 72 horas tras el uso de códigos de recuperación; Brasil desarticula una red vinculada con ClickFix; y SAP corrige vulnerabilidades críticas de hasta CVSS 10.0.

LA PREGUNTA DE CADA LUNES

¿Qué proceso sensible confía hoy en que el remitente, la sesión o la cuenta son legítimos sin volver a validar la autoridad para ejecutar la acción?

FUENTES / SIL · Revolut/TechCrunch · Google GTIG · GitHub/npm · MJSP Brasil · SAP/CERT-EU

01 / MÉXICO + POLÍTICA PÚBLICA

México vuelve a poner una Ley de Ciberseguridad sobre la mesa

El 10 de septiembre se presentó en el Senado una iniciativa para expedir una Ley de Ciberseguridad. El proyecto propone un marco nacional, protección de infraestructuras críticas, una Agencia Nacional de Ciberseguridad, CSIRTs y un Sistema Nacional de Ciberseguridad.

ALCANCE CORRECTO

Es una iniciativa legislativa, no una ley vigente. Sus obligaciones, instituciones y alcance pueden cambiar durante el proceso parlamentario.

REVISAR ESTA SEMANA

Identificar activos y servicios que podrían considerarse críticos; revisar gobierno de incidentes, responsabilidades, intercambio de información y dependencias con terceros. Preparar escenarios, sin asumir obligaciones que aún no existen.

FUENTE / Sistema de Información Legislativa · 10 sep 2026

02 / FINTECH + PRIVACIDAD

Un correo oficial no convierte una solicitud en legítima

Revolut confirmó que un tercero no autorizado usó una cuenta de correo en un dominio legítimo de una agencia gubernamental para enviar solicitudes fraudulentas de información. Un número limitado de clientes fue afectado; los datos potencialmente expuestos incluyeron identidad, documentos, selfies de verificación, estados de cuenta y transacciones. Sistemas y fondos no fueron afectados.

LA FALLA DE CONFIANZA

El dominio no era falso. El problema fue tratar una identidad técnica legítima como evidencia suficiente de que la solicitud también lo era.

REVISAR ESTA SEMANA

Tratar solicitudes regulatorias, judiciales o de autoridades como flujos de alto riesgo: verificación fuera de banda, doble aprobación, minimización de datos, registro inmutable y validación del mandato antes de revelar información.

FUENTE / Revolut vía TechCrunch · 12 sep 2026

03 / IA + VELOCIDAD

La ventana defensiva ya puede medirse en horas

Google GTIG observó adversarios pasar de prompts aislados a flujos agentivos. En un caso de Q2 2026, un actor comprometió un recurso cloud y, en menos de seis horas, planeó, construyó y ejecutó una campaña masiva de recolección de credenciales asistida por agentes.

LA SEÑAL

La IA no elimina las etapas del ataque; comprime el tiempo entre ellas. Playbooks que dependen de investigación humana secuencial pueden llegar demasiado tarde.

REVISAR ESTA SEMANA

Medir tiempo real para detectar, revocar credenciales, aislar workloads y bloquear egress. Limitar privilegios de agentes, credenciales de servicio y capacidad de crear infraestructura o secretos sin aprobación.

FUENTE / Google Threat Intelligence Group · 8 sep 2026

04 / SUPPLY CHAIN + IDENTIDAD

Recuperar una cuenta ya no debería restaurar toda la confianza

npm extendió a todas las cuentas un periodo preventivo de 72 horas después de un inicio de sesión exitoso con código de recuperación. Durante ese lapso se pausan publicaciones y escrituras sensibles, incluida la creación de tokens, aunque el usuario puede seguir autenticándose e instalando paquetes.

POR QUÉ IMPORTA

Una recuperación exitosa demuestra acceso a un mecanismo alterno; no demuestra que el riesgo haya terminado. npm convierte ese evento en una señal para reducir privilegios temporalmente.

REVISAR ESTA SEMANA

Aplicar el mismo principio en CI/CD, repositorios, PAM y consolas cloud: recovery, step-up, periodo de enfriamiento y revalidación antes de permitir releases, cambios de IAM o nuevos secretos.

FUENTE / GitHub / npm · 9 sep 2026

05 / BRASIL + CIBERCRIMEN

ClickFix ya aparece en una operación de fraude millonario

El Ministerio de Justicia de Brasil informó que, durante la Operação ClickFix, se ejecutaron 17 órdenes de registro e incautación y dos de prisión contra una organización vinculada con fraude electrónico e invasión de sistemas públicos. Se incautaron R$8.78 millones en criptoactivos; el bloqueo de cuentas podría alcanzar R$93 millones.

LA EVIDENCIA

Según la investigación, las víctimas eran inducidas por falsos mensajes de error a ejecutar código malicioso. Se comprometieron credenciales de organismos públicos, sistemas policiales y judiciales, y datos sensibles de empresas de la cadena financiera, incluidas entidades BaaS.

REVISAR ESTA SEMANA

Bloquear instrucciones de copiar y ejecutar desde navegadores, elevar telemetría de shell/PowerShell, correlacionar fraude con endpoints e identidad y preservar evidencia financiera y cripto desde el inicio.

FUENTE / Ministerio de Justicia y Seguridad Pública de Brasil · 11 sep 2026

06 / EMPRESA + SAP

SAP publica fallas críticas de hasta CVSS 10.0

SAP publicó 19 nuevas notas de seguridad el 8 de septiembre. Destacan CVE-2026-44756 (CVSS 10.0) en Extended Passport y CVE-2026-58240 (CVSS 9.8) en NetWeaver Message Server. CERT-EU señala que ambas pueden explotarse remotamente sin autenticación y derivar en ejecución de comandos.

ALCANCE CORRECTO

La criticidad no significa explotación confirmada en todas las organizaciones. La prioridad depende de productos, versiones, exposición y controles compensatorios.

REVISAR ESTA SEMANA

Inventariar versiones afectadas, priorizar sistemas SAP expuestos o con rutas de red amplias, aplicar notas y hotfixes del fabricante y buscar señales de ejecución anómala en hosts SAP.

FUENTE / SAP Security Patch Day + CERT-EU · 8-9 sep 2026

07 / RADAR EJECUTIVO

Seis revisiones para comenzar la semana

01	**LEY MX**	Seguir el trámite; mapear servicios críticos, dueños y escenarios de reporte potenciales.
02	**DATOS**	Revalidar solicitudes de autoridades por un canal independiente antes de revelar información.
03	**IA**	Medir respuesta operativa para credenciales, workloads y egress frente a ataques de menos de seis horas.
04	**RECOVERY**	Aplicar privilegio reducido tras recuperación de cuentas críticas antes de restaurar escrituras sensibles.
05	**CLICKFIX**	Buscar comandos iniciados desde navegador, shells anómalas y fraude correlacionado con identidad.
06	**SAP**	Confirmar versiones y exposición; ejecutar parchado y hunting sobre sistemas afectados.

SALIDA ESPERADA — **Seis responsables, seis decisiones y evidencia de cierre antes del viernes.**

PERSPECTIVA ZTC

La identidad no equivale a autoridad

Gran parte de la seguridad moderna se construyó para responder una pregunta: ¿quién eres? Esta semana muestra por qué ya no alcanza. Una cuenta gubernamental puede ser real; una sesión recuperada puede ser válida; un agente puede operar con credenciales legítimas; un servicio SAP puede estar autenticado. El riesgo aparece cuando de esa identidad se hereda automáticamente el derecho de actuar.

Una arquitectura madura vuelve a preguntar: ¿puede esta identidad ejecutar esta acción, sobre este dato, en este momento y bajo este contexto? La diferencia separa autenticación de autorización, confianza de legitimidad y control de evidencia.

¿Qué proceso crítico concede hoy autoridad solo porque la identidad parece legítima?

ZEROTRUST.CONSULTING

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