//ZERO TRUST CONSULTING

26 OCTUBRE 2026 · NÚMERO 010

ZTC CYBER INTELLIGENCE

LA CONFIANZA HEREDADA ES LA NUEVA BRECHA.

Cuando un proveedor, un paquete de software o una identidad de aplicación conserva más autoridad de la necesaria, el atacante no tiene que romper toda la arquitectura.

6 SEÑALES

8 CONTROLES

RADAR MÉXICO

IA OFENSIVA / CADENA DE SUMINISTRO / CERTIFICADOS / PAGOS / IDENTIDADES

EDITORIAL / CRITERIO DE LA SEMANA

El acceso heredado también es superficie de ataque.

La velocidad de la IA importa. Pero la amplitud de la autoridad delegada importa más.

En seis señales recientes aparece una misma falla estructural: sistemas que delegan confianza en software, certificados, aplicaciones o marcas y no vuelven a comprobar el alcance de esa delegación. Un paquete puede ejecutar código antes de ser importado; una aplicación de terceros puede actuar con permisos ya concedidos; una autoridad certificadora puede dejar de ser fiable.

La consecuencia para dirección es concreta: los inventarios tradicionales describen activos, pero con frecuencia no representan las relaciones de autoridad que esos activos ejercen sobre otros. Ese mapa debe incorporar identidades no humanas, pipelines, librerías, raíces de confianza y dependencias operativas.

PREGUNTA DEL LUNES

Si hoy se comprometiera una identidad de aplicación, un paquete de desarrollo o una autoridad de certificados, ¿qué otros sistemas aceptarían sus acciones sin una verificación independiente?

TRES DISTINCIONES QUE SOSTIENEN ESTA EDICIÓN

- Un objetivo reportado no equivale a una intrusión confirmada.
- La presencia de una dependencia vulnerable no demuestra explotación en una organización concreta.
- La actualización de un componente no reemplaza la búsqueda de compromiso previo ni la rotación de secretos expuestos.

FUENTES PRIMARIAS **Edición 009** **Straiker** **Microsoft**

PANORAMA / SEIS SEÑALES

Seis señales. Una pregunta: ¿quién puede actuar por quién?

Ventana de análisis: 19–25 de octubre de 2026. Corte editorial: 26 de octubre.

01

MÉXICO / IA Y PAGOS

CyberCartel y CARLIY0S

Straiker describe una infraestructura multiagente contra objetivos financieros de la región. No acredita 400 intrusiones exitosas.

02

IDENTIDADES / TERCEROS

ARTEX y abuso de OAuth

Microsoft atribuye a Storm-0940 una campaña acelerada por IA que aprovechó identidades de aplicaciones ConnectWise.

03

CADENA DE SUMINISTRO

LiteLLM 1.107.0

Una publicación comprometida en PyPI y contenedores oficiales podía ejecutar código al iniciar Python.

04

CRIPTOGRAFÍA / PKI

Las claves que dejaron de ser fiables

Ocho certificados intermedios eMudhra tenían claves privadas recuperables por entropía insuficiente.

05

EXPLOTACIÓN / CONTROL

Collabora y VeloCloud en KEV

CISA agregó dos fallas con evidencia de explotación activa: un servidor documental y un orquestador.

06

MÉXICO / SUPLANTACIÓN

La marca bancaria como vector

CONDUSEF alertó del uso no autorizado de identidad de entidades del grupo Kapital México.

FUENTES PRIMARIAS Straiker Microsoft LiteLLM Google CISA CONDUSEF

SEÑAL 01 / MÉXICO / SERVICIOS FINANCIEROS

La IA escala la ofensiva; las credenciales amplían el impacto.

Investigación de Straiker sobre CARLIY0S y objetivos financieros latinoamericanos.

QUÉ ESTÁ DOCUMENTADO

Straiker publicó el 21 de octubre una reconstrucción basada en archivos atribuidos a CyberCartel. Reporta más de 400 objetivos financieros y una base de 4,493 registros, con credenciales, llaves y artefactos técnicos. La investigación incluye referencias a 43 credenciales de una empresa fintech —11 claves de API y 32 claves criptográficas— asociadas por los investigadores a posibles riesgos para operaciones vinculadas con SPEI.

MECANISMO DE ATAQUE

Agentes de IA distribuyen reconocimiento, análisis y tareas de explotación sobre una infraestructura que conserva hallazgos y material de autenticación. La escalabilidad proviene de automatizar decisiones repetibles y reutilizar credenciales.

IMPACTO Y LÍMITES

La exposición de claves puede desplazar un ataque desde la aplicación inicial hacia APIs, servicios internos y flujos de pago. No se ha establecido públicamente una intrusión en la infraestructura central de Banxico ni que los más de 400 objetivos hayan sufrido compromisos exitosos.

QUÉ DEBERÍA DEMOSTRAR UNA ORGANIZACIÓN

- Inventario de claves de API, certificados, llaves de firma y cuentas técnicas con acceso a pagos.
- Separación entre credenciales de consulta, autorización y ejecución de operaciones sensibles.
- Correlación de emisión, uso, rotación y revocación de credenciales con eventos de negocio.

PREGUNTA PARA DIRECCIÓN

¿Podría una clave de aplicación comprometida autorizar movimientos financieros sin un segundo control independiente?

FUENTES PRIMARIAS **Straiker · 21 OCT** **CONDUSEF**

SEÑAL 02 / IA / IDENTIDADES DE APLICACIÓN

Una aplicación legítima puede convertirse en la vía de intrusión.

Microsoft relaciona Storm-0940, ARTEX y un compromiso de cadena de suministro de ConnectWise.

QUÉ ESTÁ DOCUMENTADO

El 21 de octubre, Microsoft describió operaciones atribuidas a Storm-0940 en las que el marco ARTEX aceleró el reconocimiento y el abuso de aplicaciones con permisos existentes. Reportó casos con acceso privilegiado en menos de tres horas y actividades posteriores en Microsoft Graph tras el acceso a identidades de aplicaciones vinculadas con ConnectWise.

MECANISMO DE ATAQUE

El atacante no necesita iniciar sesión como empleado cuando puede aprovechar credenciales de una aplicación previamente autorizada. La relación de confianza entre proveedor, tenant y permisos OAuth se convierte en ruta de ataque.

IMPACTO Y LÍMITES

Un inicio de sesión de una aplicación comprometida no acredita por sí mismo lectura o exfiltración de datos de clientes. Sí exige revisar consentimientos, credenciales nuevas, cambios de privilegios y operaciones Graph posteriores.

QUÉ DEBERÍA DEMOSTRAR UNA ORGANIZACIÓN

- Inventariar todas las aplicaciones multi-tenant con consentimientos privilegiados y propietario explícito.
- Cruzar sign-ins de service principals con auditoría de Microsoft Graph y modificaciones de permisos.
- Conservar evidencia, limitar accesos afectados y revocar credenciales confirmadamente indebidas.

PREGUNTA PARA DIRECCIÓN

¿Qué proveedores conservan hoy privilegios sobre el tenant que nadie revisa desde su autorización inicial?

FUENTES PRIMARIAS **Microsoft · 21 OCT**

SEÑAL 03 / CADENA DE SUMINISTRO / IA

Una dependencia comprometida puede ejecutar antes de utilizarse.

LiteLLM 1.107.0: cuando la inicialización del intérprete se convierte en mecanismo de ejecución.

QUÉ ESTÁ DOCUMENTADO

Microsoft documentó el 23 de octubre que una versión comprometida de LiteLLM 1.107.0 se distribuyó el 21 de octubre mediante PyPI e imágenes oficiales. Archivos añadidos permitían ejecutar código al inicio de Python, sin que la aplicación tuviera que importar explícitamente LiteLLM. El código intentó recolectar credenciales de herramientas de desarrollo, nube y servicios de IA.

MECANISMO DE ATAQUE

Los mecanismos de arranque del intérprete amplían el impacto desde la librería hacia estaciones de trabajo, pipelines CI/CD, contenedores y entornos de prueba donde el paquete esté instalado.

IMPACTO Y LÍMITES

Desinstalar o sustituir la versión no prueba recuperación. Si el proceso tuvo acceso a secretos, deben evaluarse el entorno, la persistencia y las credenciales alcanzables. Microsoft advierte evitar iniciar Python o pip en entornos sospechosos para inspeccionarlos.

QUÉ DEBERÍA DEMOSTRAR UNA ORGANIZACIÓN

- Identificar por SBOM, lockfiles, imágenes y artefactos dónde se introdujo LiteLLM 1.107.0.
- Aislar y examinar fuera de línea los entornos afectados; preservar artefactos de ejecución.
- Rotar los secretos potencialmente expuestos y validar integridad de pipelines y registros.

PREGUNTA PARA DIRECCIÓN

¿Sabemos qué secretos puede leer cada dependencia durante el arranque de nuestros procesos?

FUENTES PRIMARIAS **Microsoft · 23 OCT**

SEÑAL 04 / CRIPTOGRAFÍA / CERTIFICADOS

El candado puede ser válido y la confianza estar rota.

Ocho certificados intermedios de eMudhra expusieron un defecto en la generación de claves.

QUÉ ESTÁ DOCUMENTADO

Google informó el 20 de octubre que un investigador notificó claves privadas comprometidas de ocho certificados de CA subordinadas eMudhra, generadas con entropía insuficiente. Chrome bloqueó las claves afectadas y anunció la retirada de una raíz relacionada para el 27 de octubre. Un boletín de Google Cloud del 23 de octubre describió acciones sobre almacenes de confianza, imágenes, runtimes y SDK.

MECANISMO DE ATAQUE

Una CA intermedia con clave privada recuperable podría emitir certificados HTTPS fraudulentos que algunos clientes vulnerables aceptarían, en especial cuando no reciban las actualizaciones de confianza.

IMPACTO Y LÍMITES

Google indica que su infraestructura Cloud no fue comprometida y que no observó explotación contra sus workloads. El riesgo operativo alcanza clientes, SDK y almacenes de confianza administrados por terceros; la corrección puede generar interrupciones en cadenas de certificados legítimas afectadas.

QUÉ DEBERÍA DEMOSTRAR UNA ORGANIZACIÓN

- Inventariar raíces e intermedias de confianza en servidores, contenedores, SDK y clientes móviles.
- Actualizar trust stores y comprobar la cadena real en APIs, integraciones y servicios críticos.
- Preparar cambio de certificados y pruebas de interoperabilidad antes de retirar confianza.

PREGUNTA PARA DIRECCIÓN

¿Qué parte de la operación depende de almacenes criptográficos que actualizamos fuera del ciclo normal?

FUENTES PRIMARIAS Google Chrome · 20 OCT Google Cloud · 23 OCT

SEÑAL 05 / KEV / SOFTWARE EXPUESTO

El producto no define la prioridad; la explotación sí.

Collabora Online y Arista VeloCloud ingresaron al catálogo KEV el 23 de octubre.

QUÉ ESTÁ DOCUMENTADO

CISA incorporó CVE-2026-110447, inyección de comandos en Collabora Online Built-in CODE Server, y CVE-2026-114625, inyección SQL en Arista VeloCloud Orchestrator. La inclusión en KEV responde a evidencia de explotación activa; no implica que cada instalación esté comprometida.

MECANISMO DE ATAQUE

Los sistemas de edición documental y los planos de orquestación pueden convertirse en rutas hacia archivos, credenciales, configuraciones de red y funciones administrativas. El alcance depende de versión, modalidad y exposición.

IMPACTO Y LÍMITES

El 26 de octubre es la fecha de remediación federal estadounidense indicada en estas entradas, no un plazo normativo para empresas mexicanas. La decisión empresarial exige inventario, corrección del fabricante e investigación de actividad previa donde corresponda.

QUÉ DEBERÍA DEMOSTRAR UNA ORGANIZACIÓN

- Confirmar instalación, edición, versión y exposición real de Collabora y VeloCloud.
- Aplicar versiones corregidas publicadas por fabricante tras validar compatibilidad.
- Inspeccionar logs, cambios de privilegios y artefactos de compromiso antes de declarar cierre.

PREGUNTA PARA DIRECCIÓN

¿Podemos distinguir en horas los activos realmente explotables de los CVE irrelevantes para nuestra operación?

FUENTES PRIMARIAS **CISA · 23 OCT** **Catálogo KEV**

SEÑAL 06 / MÉXICO / SUPLANTACIÓN FINANCIERA

Una marca auténtica no autentica el canal.

CONDUSEF alertó sobre posible suplantación de identidad de entidades del grupo Kapital México.

QUÉ ESTÁ DOCUMENTADO

El 23 de octubre, CONDUSEF informó del uso no autorizado del nombre y elementos de identidad de instituciones de Kapital México Grupo Financiero. Mencionó una aplicación denominada “KapitalMex” y la promoción de un supuesto evento de inversionistas. La autoridad aclaró que las instituciones señaladas no organizan eventos mediante grupos de WhatsApp que solicitan descargar aplicaciones.

MECANISMO DE ATAQUE

El fraude aprovecha signos de identidad legítimos —nombre, marca, datos institucionales— para trasladar a un canal no verificado la confianza que el usuario atribuye a una entidad supervisada.

IMPACTO Y LÍMITES

La alerta documenta un riesgo de suplantación; no prueba intrusión en los sistemas del banco o la casa de bolsa. La defensa requiere combinar verificación del canal, control de aplicaciones y monitoreo de dominios y mensajes apócrifos.

QUÉ DEBERÍA DEMOSTRAR UNA ORGANIZACIÓN

- Publicar y verificar un directorio inequívoco de canales oficiales y apps autorizadas.
- Buscar dominios, perfiles y aplicaciones que simulen la marca; conservar evidencia y reportar.
- Probar un protocolo de autenticación independiente para instrucciones de inversión o pago.

PREGUNTA PARA DIRECCIÓN

¿Qué canal permite a un cliente demostrar que está hablando realmente con la institución?

FUENTES PRIMARIAS CONDUSEF · 23 OCT

MATRIZ EDITORIAL / ESTADO DE EVIDENCIA

Hecho, atribución y límite: no son lo mismo.

Cada señal tiene una fuerza probatoria distinta. La prioridad no depende de dramatizarla.

SEÑAL	BASE DOCUMENTAL	LO QUE NO DEBE INFERIRSE
01 / CARLIY0S	Investigación de Straiker	Objetivos y credenciales reportados; víctimas anonimizadas; sin prueba pública de afectación al núcleo SPEI.
02 / ARTEX	Telemetría atribuida por Microsoft	Compromisos de identidad de aplicación; no toda autenticación implica acceso o extracción de datos.
03 / LiteLLM	Análisis técnico de Microsoft	Paquete contaminado documentado; impacto por entorno requiere inventario, análisis y rotación.
04 / eMudhra	Avisos de Google y Cloud	Claves subordinadas comprometidas; Google Cloud indica infraestructura no comprometida.
05 / KEV	Inclusión oficial de CISA	Explotación acreditada para las CVE, no compromiso confirmado de cada instalación.
06 / Kapital	Comunicado de CONDUSEF	Suplantación presunta mediante canales no oficiales; no evidencia de intrusión bancaria.

Criterio ZTC: toda decisión de riesgo debe distinguir existencia del activo, exposición efectiva, explotación observada, impacto probado y evidencia de recuperación.

FUENTES PRIMARIAS **Straiker** **Microsoft** **Google** **CISA** **CONDUSEF**

LECTURA TRANSVERSAL / ARQUITECTURA

Cuatro fronteras que deben hacerse explícitas.

No basta con inventariar sistemas: hay que representar quién confía en quién y con qué autoridad.

01

APLICACIONES Y PROVEEDORES

Consentimientos OAuth, integraciones, permisos de aplicación y cuentas no humanas.

Punto de ruptura: Fallo: autoridad persistente sin revisión de propósito.

02

COMPONENTES Y BUILD

Paquetes, imágenes, dependencias, artefactos firmados y secretos de pipelines.

Punto de ruptura: Fallo: ejecución implícita desde una dependencia.

03

CRIPTOGRAFÍA Y PKI

Raíces de confianza, certificados intermedios, trust stores, claves y SDK.

Punto de ruptura: Fallo: confianza criptográfica heredada fuera del control operativo.

04

CANALES Y MARCAS

Aplicaciones oficiales, dominios, mensajería, suplantación y validación fuera de banda.

Punto de ruptura: Fallo: legitimidad atribuida a una apariencia.

Principio de diseño: una dependencia debe recibir la autoridad mínima necesaria, durante el tiempo mínimo necesario, con revocación y evidencia independientes.

CHECKPOINT EJECUTIVO / OCHO CONTROLES

Ocho controles para cerrar la brecha de confianza.

No son compras recomendadas. Son pruebas de capacidad y resultados verificables.

01 **Inventario de autoridad**
Mapa de apps OAuth, identidades no humanas, permisos y dueños.
EVIDENCIA: Registro reconciliado con configuraciones reales.

02 **Consentimiento acotado**
Permisos de terceros por acción, recurso y vigencia.
EVIDENCIA: Prueba de acceso denegado fuera del alcance.

03 **Cadena de build confiable**
SBOM, artefactos inmutables, procedencia y control de dependencias.
EVIDENCIA: Reconstrucción de versión e integridad.

04 **Custodia de secretos**
Inventario y rotación de llaves de API, firmas, tokens y credenciales.
EVIDENCIA: Registro de revocación y uso posterior nulo.

05 **PKI y trust stores**
Cadenas de certificación y actualización en runtimes y clientes.
EVIDENCIA: Prueba de rechazo de CA comprometida.

06 **Exposición explotable**
Cruce KEV, activo, versión, conectividad e importancia.
EVIDENCIA: Activos corregidos y evidencia forense.

07 **Canales auténticos**
Marca, dominios, aplicaciones, mensajería y confirmación independiente.
EVIDENCIA: Trazabilidad de reportes y bajas.

08 **Recuperación comprobada**
Restauración, continuidad de pagos, segregación y contingencia.
EVIDENCIA: Prueba periódica con tiempos y responsables.

FUENTES PRIMARIAS Microsoft LiteLLM Google Cloud CISA

RADAR MÉXICO / CONSEJO Y DIRECCIÓN

México: tres exposiciones que convergen.

Una institución puede operar normalmente mientras su confianza digital se deteriora por capas.

PAGOS Y CREDENCIALES

La investigación de Straiker amerita revisar custodia de claves, controles de doble autorización, origen de solicitudes y posibilidad de limitar transacciones ante un compromiso de identidades técnicas.

IDENTIDAD FINANCIERA

La alerta de CONDUSEF sobre Kapital México exige canales oficiales verificables y respuesta documentada ante suplantaciones; no representa una confirmación de intrusión en infraestructura bancaria.

NUBE Y CONTINUIDAD

Cambios en confianza TLS, dependencias de IA y aplicaciones de terceros pueden afectar operaciones esenciales aun sin explotar vulnerabilidades propias del banco.

OCHO PREGUNTAS PARA LA PRÓXIMA REUNIÓN DE RIESGOS

- ¿Qué identidad de aplicación puede crear privilegios o modificar credenciales?
- ¿Dónde están las llaves de firma y los secretos de integraciones de pago?
- ¿Qué pipeline ejecuta dependencias antes de validarlas?
- ¿Qué clientes TLS no reciben cambios de confianza automáticamente?
- ¿Qué hallazgos KEV están expuestos de verdad?
- ¿Qué evidencia demuestra que una corrección eliminó persistencia?
- ¿Cómo comprueba un cliente que un canal financiero es auténtico?
- ¿Qué operación seguiría funcionando si fallara el tercero más crítico?

FUENTES PRIMARIAS **Straiker** **CONDUSEF** **Google Cloud**

FUENTES / MÉTODO / CIERRE

Trazabilidad antes que titulares.

Fuentes seleccionadas por cercanía al hecho, fecha, pertinencia y posibilidad de contrastación.

01 Straiker / STAR Labs
Inside CARLIY0S — 21 oct 2026
ABRIR FUENTE

02 Microsoft Security Research
Storm-0940, ARTEX y ConnectWise — 21 oct
ABRIR FUENTE

03 Microsoft Security Research
LiteLLM 1.107.0 supply chain — 23 oct
ABRIR FUENTE

04 Google Chrome / Android
Compromiso de certificados eMudhra — 20 oct
ABRIR FUENTE

05 Google Cloud
Boletín GCP-2026-071 — 23 oct
ABRIR FUENTE

06 CISA
KEV: Collabora Online — 23 oct
ABRIR FUENTE

07 CISA
Catálogo KEV y Arista VeloCloud — 23 oct
ABRIR FUENTE

08 CONDUSEF
Alerta Kapital México — 23 oct
ABRIR FUENTE

09 Genesys / contexto
Actualización de incidente interno — 23 oct
ABRIR FUENTE

POLÍTICA EDITORIAL

La edición distingue alertas de autoridades, investigación de terceros, hechos confirmados e interpretación arquitectónica. No presenta objetivos como víctimas verificadas, una falla como intrusión universal ni un riesgo operativo como daño acreditado. Los controles son criterios de revisión, no dictámenes sobre sistemas específicos.

LA PREGUNTA QUE QUEDA

¿Cuánta autoridad puede conservar hoy una dependencia sin que nadie vuelva a examinarla?