Número 107 | Octubre 2025

NTT DATA

Radar

El magazine de ciberseguridad

La identidad es la nueva zona de "máxima seguridad"

Por Hans Vigil Navas

Si 2024 fue el año de consolidar **Zero Trust**, 2025–2026 serán los años de operacionalizar la identidad como perímetro real. Tres fuerzas lo aceleran: la madurez de las guías de NIST sobre identidad digital, la presión de las APIs como columna vertebral del negocio y la profesionalización de ataques contra factores débiles de autenticación.

En nuestra región (con ecosistemas *multi-cloud*, servicios públicos digitales en expansión y cadenas de suministro cada vez más SaaS) el costo de no modernizar IAM ya no es técnico: es estratégico.

1. Del "cumplir MFA" a la autenticación resistente al *phishing*

NIST publicó la revisión 4 de SP 800-63 (agosto de 2025) que actualiza los requisitos de prueba de identidad, autenticación y federación e incorpora consideraciones de privacidad y experiencia de usuario. Para los CISOs, esto se traduce en elevar la vara hacia MFA resistente al *phishing* y en estandarizar niveles de aseguramiento a lo largo de todo el *journey* digital (*onboarding*, recobro, federación con terceros).

2. *Passwordless* en serio (y con métricas)

El empuje global de *passkeys* (FIDO2/WebAuthn) dejó de ser "futuro": más de 15 mil millones de cuentas ya pueden usarlas y la adopción corporativa sigue creciendo, con guías y métricas públicas de la FIDO Alliance. En 2025, casi la mitad del top-100 de sitios ya las soporta. Para Latam, esto implica planificar migraciones graduales, políticas de recuperación y portabilidad y educación del usuario para evitar fricciones.

3. *Zero Trust* en el plano de la identidad

NIST SP 800-207 y su complemento 800-207A reposicionan controles hacia decisiones continuas y contextuales de acceso, desacoplando la red de recurso. Llevarlo a la práctica exige políticas a nivel de aplicación, señales de postura de dispositivo y re-autenticación adaptativa. El objetivo no es "cerrar la red", sino autorizar cada solicitud con contexto actualizado.

4. APIs: donde se rompe (o se gana) el control de acceso

Mientras el OWASP Top 10 para web mantiene Broken Access Control como riesgo crítico, el OWASP API Security Top 10 (2023) evidencia que los fallos más explotados son BOLA/BOPLA y autenticación rota.

La recomendación para 2025–2026 es explícita: *policy-as-code* para autorización a nivel de objeto/propiedad, inventario y clasificación de APIs, pruebas de seguridad en el *pipeline* y gobernanza de tokens (rotación, *scopes* mínimos, detección de uso anómalo).

5. ISO/IEC 27001:2022 como ancla de gestión

El estándar vigente sigue siendo ISO/IEC 27001:2022 (con enmienda 2024), que alinea controles con realidades *cloud* e identidad. Para CISOs, ofrece el marco para integrar IAM con riesgo, auditoría y proveedores, evitando que IAM sea solo "tecnología" y no proceso y mejora continua.

6. Nuevos frentes: máquinas, agentes y detección de amenazas de identidad

La explosión de identidades no humanas (*workloads*, contenedores, claves de servicio y agentes de IA) obliga a una visibilidad, emisión "*just-in-time*", *Zero Standing Privilege* y rotación automatizada. El mercado ya trata ITDR (Identity Threat Detection & Response) como categoría necesaria para detectar abuso de *tokens*, "*impossible travel*", sesiones secuestradas y "*consent phishing*".

Prioridades concretas para 12–18 meses

- Endurecer autenticación: hoja de ruta a *passkeys* para apps críticas, MFA resistente al *phishing* y recuperación sin SMS; medir adopción y éxito por cohorte.
- Gobernar acceso en APIs: inventario unificado, tests de autorización en CI/CD y *scopes* mínimos por cliente; telemetría de *token* y revocación en tiempo real.
- *Zero Trust* "*identity-first*": políticas dinámicas con señales de dispositivo/ubicación/riesgo; revalidación continua de sesión y privilegios.
- *No-human* IAM: emitir credenciales efímeras, rotación automática y registro criptográfico de uso y separar *guardrails* para agentes de IA.

- Alinear con ISO 27001:2022: KPIs de IAM en el ISMS, auditorías a terceros (federación, IDaaS), y gestión de riesgos de identidad en el comité de seguridad.

- ITDR: detección de anomalías centrada en identidad y "*kill-switch*" para *tokens*/sesiones comprometidas integrado al SOC.

Finalmente, modernizar el Identity & Access Management (IAM) no es un proyecto, es un modelo operativo empresarial.

Adoptar NIST SP 800-63-4, endurecer APIs con OWASP, y anclar la gobernanza en ISO/IEC 27001:2022 permitirá a las organizaciones de Perú y Latam sostener crecimiento digital, cumplir regulaciones y reducir de forma medible el riesgo de fraude, intrusión y abuso de privilegios en 2025–2026.

Hans Vigil Navas
Cybersecurity Manager

Identidad digital, la llave maestra

Cibercrónica por Marlon Santiago Nivia Devia

Entre mediados de 2024 y agosto de 2025, el panorama de la ciberseguridad dejó claro que incluso las organizaciones más preparadas pueden caer si su gestión de identidades y accesos (IAM) es vulnerada. Más que un *firewall* o un antivirus, la identidad digital se ha convertido en la llave maestra para infiltrarse, escalar privilegios y comprometer infraestructuras críticas. En menos de un año, una serie de ataques encadenados mostró que la debilidad no siempre está en el código, sino en las credenciales, los *tokens* y las personas que los gestionan.

La primera señal de alarma se dio a mediados de 2024, cuando el grupo ShinyHunters protagonizó uno de los robos de datos más masivos de los últimos tiempos. Armados con credenciales robadas mediante *malware* tipo *infostealer*, accedieron a cuentas de clientes de Snowflake que carecían de autenticación multifactor. El ataque fue silencioso y quirúrgico: identificaron credenciales comprometidas en máquinas infectadas, probaron accesos contra la nube de Snowflake y, una vez dentro, descargaron bases de datos completas sin disparar alertas críticas.

Sin necesidad de vulnerar el código de la plataforma ni comprometer a empleados internos, aprovecharon la ausencia de un segundo factor como puerta de entrada, exponiendo millones de registros pertenecientes a empresas como Ticketmaster, Santander, Advance Auto Parts, LendingTree y AT&T. La filtración alcanzó tal magnitud que gran parte de los datos terminaron circulando en foros clandestinos como BreachForums, donde fueron revendidos y compartidos entre distintos grupos criminales. Este episodio no solo evidenció la amenaza creciente de los *infostealers*, sino también lo frágil que puede ser la seguridad cuando un proveedor externo concentra información crítica sin exigir autenticación reforzada.

La industria aún procesaba el impacto de este golpe cuando, en diciembre de 2024, otro incidente encendió las alarmas en el corazón del gobierno estadounidense. El Departamento del Tesoro sufrió lo que denominó su “mayor incidente de ciberseguridad” tras ser atacado por un grupo de amenaza persistente avanzada (APT) presuntamente vinculado al Estado chino. Aprovechando dos vulnerabilidades de día cero en el servicio de soporte de BeyondTrust, proveedor de gestión de acceso privilegiado (PAM), los atacantes irrumpieron en la red y robaron una clave API con privilegios amplios. Con ella, no solo restablecieron contraseñas de cuentas críticas, sino que obtuvieron acceso remoto a estaciones de trabajo con información clasificada sobre operaciones financieras y políticas de sanciones.

Aunque BeyondTrust revocó de inmediato el secreto comprometido y desactivó instancias sospechosas, el incidente dejó claro que, en entornos IAM y PAM, un único *token* mal protegido puede convertirse en la llave para abrir todas las puertas. La dimensión política del ataque fue igualmente significativa: mientras Estados Unidos acusó formalmente a China, Pekín negó cualquier implicación, elevando el incidente a un terreno de tensión diplomática.

Sin tiempo para asimilar esta lección, en abril de 2025, dos gigantes del retail británico, Marks & Spencer y Co-op, se encontraron en el centro de un “evento cibernético combinado” según el Cyber Monitoring Centre. En apenas días de diferencia, un mismo grupo llevó a cabo ataques casi idénticos, basados no en sofisticadas vulnerabilidades técnicas, sino en manipulación psicológica. Mediante llamadas y correos internos falsificados, se hicieron pasar por personal del departamento de TI para engañar a operadores de *help desk* y obtener el restablecimiento de credenciales con privilegios administrativos. Una vez dentro, accedieron a sistemas internos de logística, inventario y ventas, causando interrupciones y filtrando datos comerciales.

El impacto fue profundo: dos objetivos principales seriamente dañados y un efecto dominó que alcanzó a proveedores y socios cuya operación dependía de estas cadenas de suministro. Poco después, el Google Threat Intelligence Group advirtió que el grupo Scattered Spider estaba reutilizando el mismo patrón contra aseguradoras estadounidenses, confirmando que la técnica había demostrado ser rentable y difícil de detener.

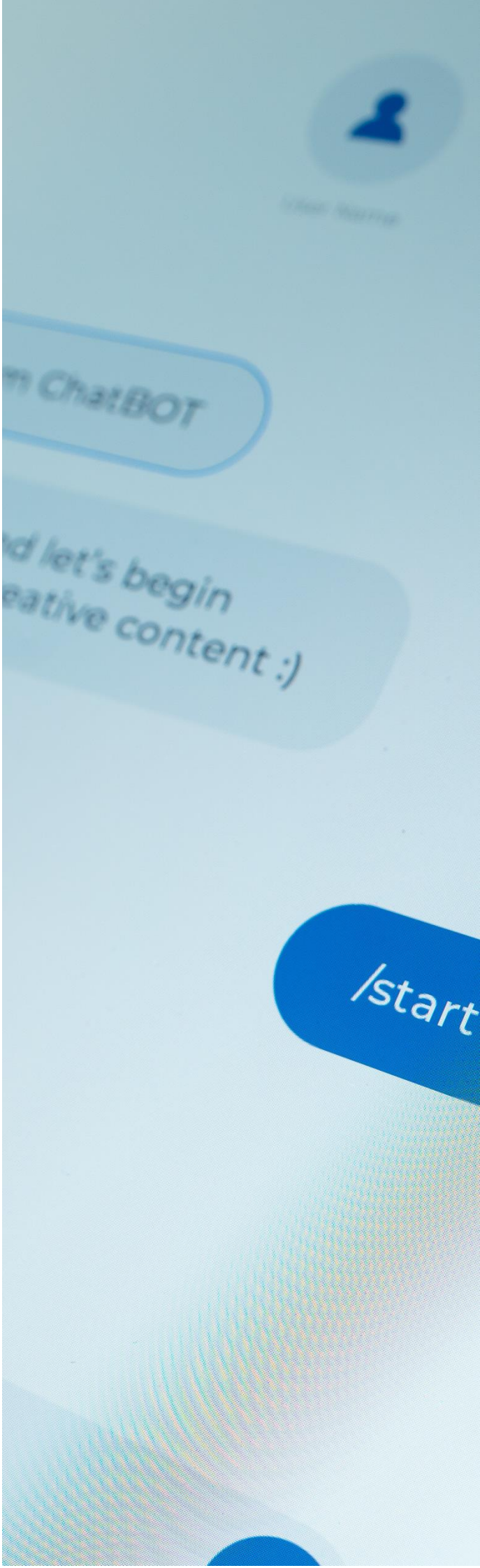
Y cuando parecía que el año no podía ofrecer otra lección amarga, en agosto de 2025, Cisco se convirtió en la nueva víctima. Esta vez, el ataque no se apoyó en vulnerabilidades de software, sino en persuasión humana. Un actor malicioso ejecutó un plan de *vishing* — *phishing* por voz— que incluyó múltiples llamadas, construcción de confianza y un guion meticulosamente diseñado para convencer a un representante de soporte de conceder acceso a un CRM externo.

Además, los sistemas de IA pueden aprender de incidentes pasados, mejorando continuamente su capacidad para reconocer nuevas amenazas y reducir los falsos positivos. Esto se traduce en una respuesta más rápida y efectiva ante incidentes, ya que la IA puede priorizar alertas y sugerir acciones correctivas.

Por último, estas técnicas facilitan la integración de diferentes fuentes de información, permitiendo una visión más completa del panorama de amenazas y ayuda a los analistas a tomar decisiones informadas.

En conjunto, estas capacidades hacen que los SOC sean más proactivos y eficientes en la defensa contra ciberataques.

Marlon Santiago Nivia Devia
Cybersecurity Junior Analyst



CIAM: Seguridad y Experiencia del Cliente en la Era Digital

Artículo por Alicia Lara Herrera

En un mundo donde la experiencia del cliente es tan importante como la seguridad digital, el Customer Identity and Access Management (CIAM) se ha convertido en un pilar fundamental para las organizaciones que desean ofrecer servicios personalizados, seguros y eficientes. A diferencia del Identity and Access Management (IAM) tradicional, orientado a empleados y recursos internos, el CIAM se enfoca en gestionar de forma segura la identidad de millones de clientes externos, combinando seguridad, escalabilidad y experiencia de usuario.

IAM vs CIAM: entendiendo las Diferencias

El IAM corporativo está diseñado para controlar el acceso de empleados, socios y dispositivos a los recursos internos de una organización. Se centra en la eficiencia operativa, cumplimiento normativo y gestión de privilegios internos.
Por otro lado, el CIAM está orientado al cliente final. Sus prioridades son la usabilidad, escalabilidad, seguridad y cumplimiento de normativas de protección de datos (como el GDPR). Además, incorpora funcionalidades clave como el registro social (*social login*), gestión de consentimiento, personalización de la experiencia y soporte a múltiples canales (web, móviles, kioscos, etc.).

La Importancia Estratégica del CIAM para las Empresas

En un entorno cada vez más digitalizado, donde la interacción con los clientes ocurre a través de múltiples canales como aplicaciones móviles, portales web, redes sociales o *call centers*, gestionar la identidad del cliente de forma eficaz se ha convertido en una ventaja competitiva clave. Más allá de una simple capa de seguridad, el Customer Identity and Access Management (CIAM) se posiciona como una plataforma estratégica que impacta directamente en la experiencia del cliente, el cumplimiento normativo, la eficiencia operativa y el crecimiento del negocio.

1. Experiencia del Cliente (CX) Sin Fricciones

El CIAM bien implementado permite a los usuarios:

- Registrarse de manera rápida y segura.
- Iniciar sesión utilizando identidades sociales (Google, Apple, Facebook, etc.).
- Autenticarse sin contraseñas (*passwordless*).
- Gestionar su perfil, preferencias de privacidad y consentimiento en un panel de autoservicio.

Esto se traduce en interacciones más ágiles, menos abandono en procesos de registro y una mayor fidelización. En el contexto actual, donde el cliente espera una experiencia fluida y personalizada, el CIAM es un habilitador fundamental.

2. Seguridad y Confianza

El aumento de fraudes digitales, robo de identidad y violaciones de datos ha hecho que la seguridad sea una prioridad crítica. CIAM proporciona:

- Autenticación fuerte y multifactor (MFA).
- Detección de anomalías e inteligencia de comportamiento para detectar accesos inusuales.
- Gestión de sesiones y revocación de *tokens* en tiempo real.

Proteger la identidad del cliente es también proteger la reputación de la empresa. Un incidente de seguridad puede provocar pérdida de confianza, daños reputacionales y sanciones regulatorias.

3. Cumplimiento Normativo

Los marcos regulatorios actuales exigen un control riguroso sobre:

- El consentimiento explícito del usuario.
- La trazabilidad y seguridad de los datos personales.

Un CIAM moderno incluye herramientas nativas para gestionar el consentimiento, registrar auditorías, y permitir a los clientes ejercer sus derechos de forma autónoma.

4. Datos confiables para el análisis

El CIAM es la puerta de entrada a datos valiosos sobre el comportamiento del cliente: ¿desde dónde acceden?, ¿qué dispositivos utilizan?, ¿con qué frecuencia inician sesión?, ¿qué canales prefieren?

Puntos Clave del Customer Journey

A lo largo del ciclo de vida del cliente, el CIAM interviene en momentos críticos:

1) **Registro:** integración de opciones como *social login*, email y SMS. Captura de consentimiento.
2) **Autenticación: a**utenticación segura mediante MFA, biometría o autenticación adaptativa.
3) **Gestión de identidad:** autoservicio para actualización de datos y preferencias de privacidad.
4) **Acceso a recursos:** autorización basada en roles, atributos o políticas.
5) ***Logout* y revocación:** mecanismos seguros para cerrar sesión y revocar *tokens*.

Protocolos de Autenticación y Autorización

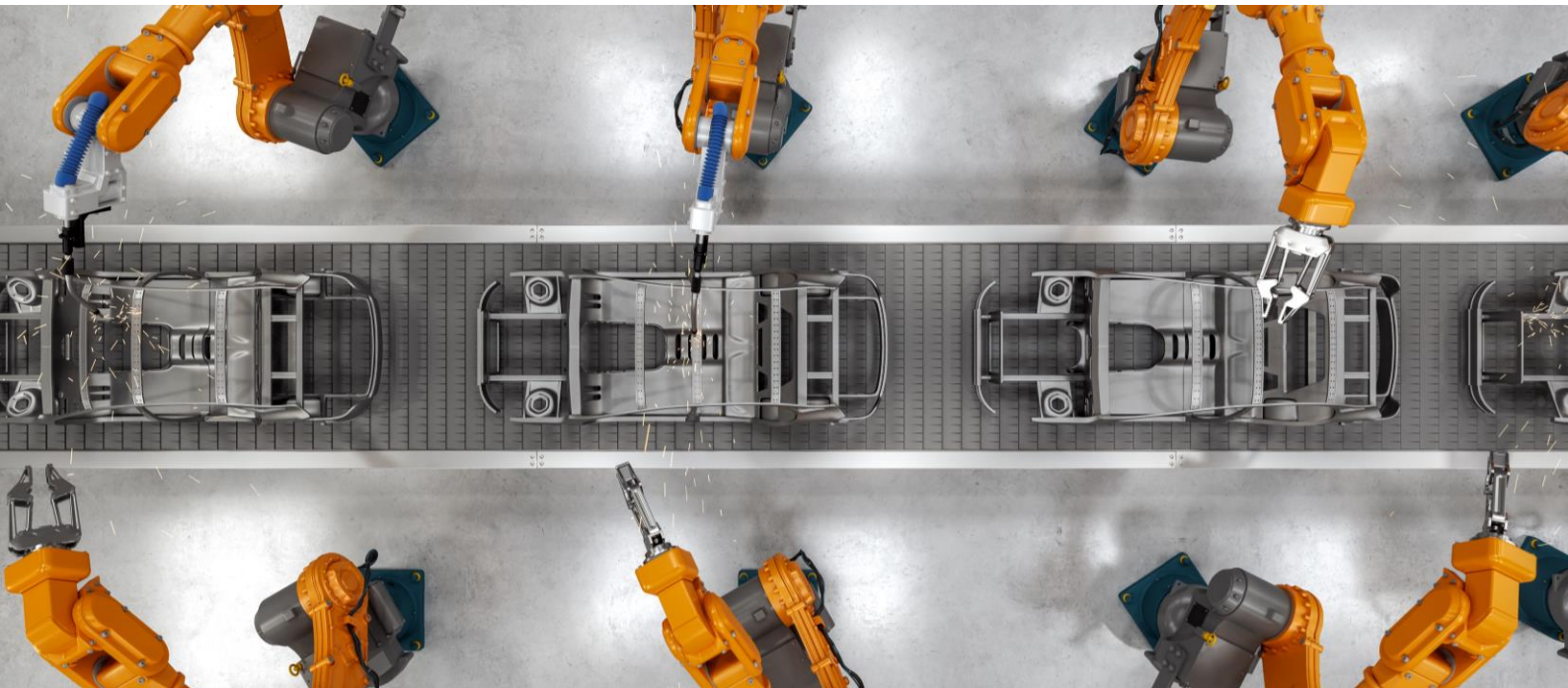
El CIAM se basa en estándares abiertos para garantizar interoperabilidad, seguridad y escalabilidad:

- OAuth 2.0: protocolo de autorización que permite a las aplicaciones acceder a recursos en nombre del usuario sin compartir credenciales. Sus características clave incluyen: :
  - Delegación de acceso
  - Soporte a tokens de acceso de corta duración
  - Adopción en APIs y servicios modernos.
- OpenID Connect (OIDC): extiende OAuth 2.0 para incorporar autenticación. Permite a las aplicaciones conocer la identidad del usuario, obteniendo información adicional mediante un ID Token (JWT).
- JSON Web Token (JWT): formato compacto y seguro que transporta información entre partes como *tokens* de autenticación o autorización. Incluye *claims* (afirmaciones) firmadas digitalmente y, en algunos casos, cifradas.

En resumen, la adopción de un CIAM moderno no solo fortalece la ciberseguridad de una organización, sino que también mejora radicalmente la experiencia del cliente. Integrar autenticación robusta, gestión de consentimiento, estándares abiertos y un enfoque centrado en el usuario es esencial para competir en un entorno digital cada vez más exigente.

En este sentido, el CIAM es más que una tecnología: es un facilitador clave del crecimiento, la confianza y la innovación empresarial.

Alicia Lara Herrera
Cybersecurity Expert Engineer



El Mundo PAM (Privileged Access Management)

Artículo por Mijail Muñoz Loja

En el contexto de la ciberseguridad, uno de los riesgos más significativos es el mal manejo de accesos privilegiados, ya que los usuarios con permisos elevados pueden acceder a información crítica y sistemas sensibles que, si caen en manos equivocadas, pueden causar daños irreparables. El **Privileged Access Management (PAM)** es un conjunto de políticas, herramientas y prácticas de seguridad diseñadas para controlar y monitorizar los accesos privilegiados, con el objetivo de minimizar los riesgos relacionados con estos accesos altamente sensibles. PAM juega un papel crucial en la protección de la infraestructura digital de una organización, asegurando que los privilegios sean concedidos y utilizados de manera apropiada.

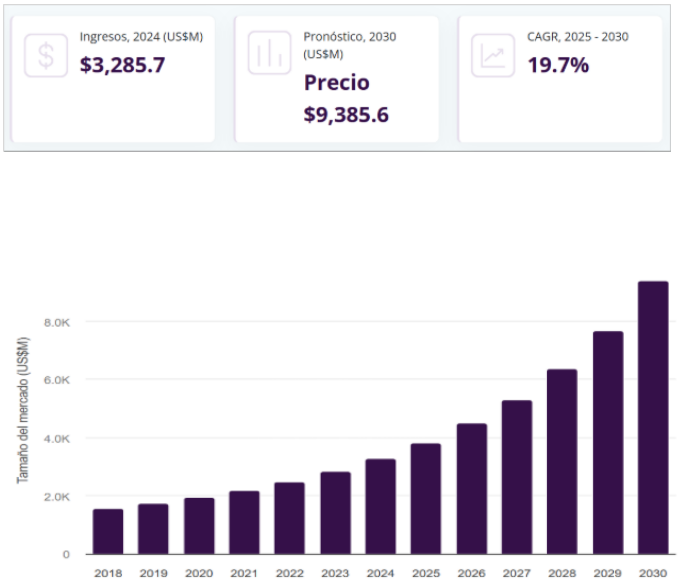
1. ¿Qué es Privileged Access Management (PAM)?

PAM hace referencia a las estrategias y herramientas implementadas para gestionar, asegurar, monitorizar y auditar los accesos privilegiados dentro de una organización. Los accesos privilegiados son aquellos que otorgan a un usuario, administrador o aplicación capacidades para realizar tareas críticas, como la configuración de sistemas, la gestión de bases de datos o el control de redes y servidores. Debido a que estas cuentas tienen el potencial de hacer cambios significativos en el entorno de TI, un mal manejo de estas cuentas puede ser el punto de entrada ideal para ciberataques.
El principal objetivo de PAM es limitar, gestionar y monitorizar el acceso a recursos críticos, asegurando que los usuarios solo tengan los privilegios necesarios para realizar su trabajo, y que esos accesos estén constantemente vigilados y auditados para detectar cualquier actividad sospechosa. (CyberArk, s.f.) (Fortinet, s.f.) (Techopedia, s.f.)

2. El tamaño del mercado de PAM

i. Tamaño y perspectivas del mercado global de gestión de acceso privilegiado

El tamaño del mercado global de gestión de acceso privilegiado se estimó en USD 3,285.7 millones en 2024 y se proyecta que alcance los USD 9,385.6 millones para 2030, creciendo a una CAGR del 19.7% de 2025 a 2030. El aumento de las amenazas de ciberseguridad, incluidas las violaciones de datos y los ataques internos, están impulsando a las organizaciones a adoptar prácticas más seguras de gestión del acceso. Los estrictos requisitos reglamentarios y los mandatos de cumplimiento, como el GDPR y el HIPAA, aceleran aún más la necesidad de sistemas seguros. (Global, s.f.)



Mercado global de gestión de acceso privilegiado, 2018-2030 (US$M)

Aspectos destacados del mercado global de gestión de acceso privilegiado

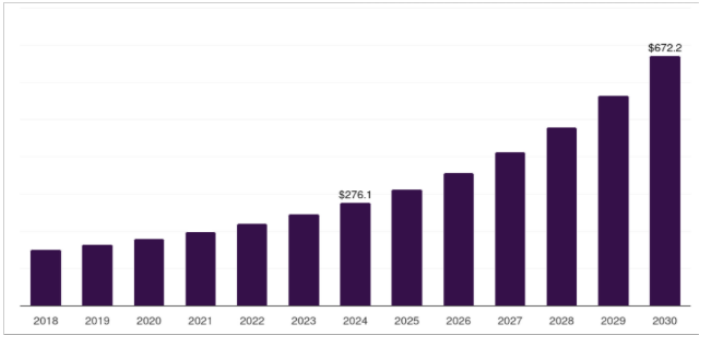
- Se espera que el mercado crezca a una CAGR (2025 - 2030) del 19,7% para 2030.
- En términos de segmento, el *software* de gestión de acceso privilegiado representó unos ingresos de 2.407,2 millones de dólares en 2024.
- El *software* de gestión de acceso privilegiado es el segmento de tipo más lucrativo que registra el crecimiento más rápido durante el período de pronóstico.
- En términos de región, América del Norte fue el mercado generador de mayores ingresos en 2024.
- En cuanto a los países, se espera que Corea del Sur registre la CAGR más alta de 2025 a 2030.

Otras tendencias clave de la industria

En términos de ingresos, América del Norte representó el 35,1% del mercado global de gestión de acceso privilegiado en 2024.
Por país, se prevé que EE. UU. lidere el mercado mundial en términos de ingresos en 2030.
Por países, Corea del Sur es el mercado regional de más rápido crecimiento y se prevé que alcance los USD 326,7 millones para 2030. (Global, s.f.)

ii. Tamaño y perspectivas del mercado de gestión de acceso privilegiado de América Latina

Se espera que el mercado de gestión de acceso privilegiado en América Latina alcance un ingreso proyectado de US$ 672,2 millones para 2030. Además, se espera una tasa de crecimiento anual compuesta del 16,5% del mercado de gestión de acceso privilegiado de América Latina de 2025 a 2030. (Latam, s.f.)



Mercado de gestión de acceso privilegiado de América Latina, 2018-2030 (US$M)

Aspectos destacados del mercado de gestión de acceso privilegiado de América Latina

- El mercado de gestión de accesos privilegiados de América Latina generó unos ingresos de 276,1 millones de dólares en 2024.
- Se espera que el mercado crezca a una CAGR del 16,5 % de 2025 a 2030.
- En términos de segmento, el *software* de gestión de acceso privilegiado fue el tipo que más ingresos generó en 2024.
- El *software* de gestión de acceso privilegiado es el segmento de tipo más lucrativo que registra el crecimiento más rápido durante el período de pronóstico.
- En cuanto al país, se espera que Brasil registre la CAGR más alta de 2025 a 2030. (Latam, s.f.)

3. Beneficios de implementar PAM

Implementar una solución de PAM en una organización aportará una serie de beneficios clave para la seguridad:

- Reducción de riesgos de Accesos No Autorizados.
- Minimización del Daño Potencial en Caso de Compromiso.
- Cumplimiento Regulatorio.
- Mejora de la Visibilidad y Control sobre las actividades de los Administradores.
- Automatización de Procesos de Gestión de Cuentas

4. Conclusiones

La gestión de accesos privilegiados (PAM) es una de las piezas clave en cualquier estrategia de ciberseguridad moderna. Dada la gran cantidad de ataques que se enfocan en explotar cuentas privilegiadas, implementarlo adecuadamente ayuda a reducir significativamente los riesgos, asegurando la protección de la infraestructura crítica de la organización.

Con las crecientes amenazas y el entorno digital cada vez más complejo, la implementación de PAM no es solo una opción, sino una necesidad para proteger los activos más valiosos de cualquier organización.

Mijail Muñoz Loja
Cybersecurity Lead Engineer

Baterías cuánticas

Espacio cuántico
por María Gutiérrez

La transición energética depende de un elemento esencial: las baterías. Desde los teléfonos móviles hasta los vehículos eléctricos, pasando por las redes inteligentes, el almacenamiento eficiente y seguro de energía es un desafío clave. Sin embargo, comprender y mejorar las baterías requiere adentrarse en un terreno donde la física clásica (el mundo de los electrones y las interacciones químicas) empieza a quedarse corto mientras que la computación cuántica emerge como una herramienta transformadora.

El límite de la simulación clásica

Hoy en día, los investigadores utilizan la química computacional y la dinámica molecular para predecir el comportamiento de los materiales de las baterías. Estos métodos permiten, por ejemplo, estimar cómo un ion de litio se mueve a través de un electrolito o cómo reacciona una molécula en el cátodo. Pero, a medida que aumenta la complejidad —como ocurre en la formación de la llamada interfase sólido-electrolito (SEI), que determina la vida útil de la batería— los algoritmos clásicos se vuelven prohibitivos en tiempo y coste. El problema es intrínseco: simular con exactitud los estados electrónicos de un sistema crece de manera exponencial con el número de partículas.

El salto cuántico. La batería de Dicke

La computación cuántica promete superar ese muro, estos ordenadores son capaces de abordar directamente problemas que en un sistema clásico requieren aproximaciones. En concreto, para este caso de las baterías, y debido a su viabilidad experimental, el equipo de NTT DATA ha propuesto un proyecto de investigación en torno a la batería Dicke, que es, dentro de la termodinámica y la tecnología cuánticas de almacenamiento de energía, uno de los diseños más prometedores para baterías cuánticas.

Se basa en el modelo propuesto en 1954 por Robert Dicke, que describe cómo un conjunto de átomos o emisores cuánticos (como cúbits, iones o moléculas) interactúan colectivamente con un campo electromagnético. En lugar de comportarse de forma independiente, los átomos se acoplan colectivamente al mismo modo de radiación, este acoplamiento puede generar fenómenos como la "superradiancia": todos los átomos descargan su energía de forma sincronizada y mucho más rápida de lo que lo harían de manera individual. Trasladado a baterías, la idea es cargar y descargar energía cuánticamente de forma colectiva y ultrarrápida.

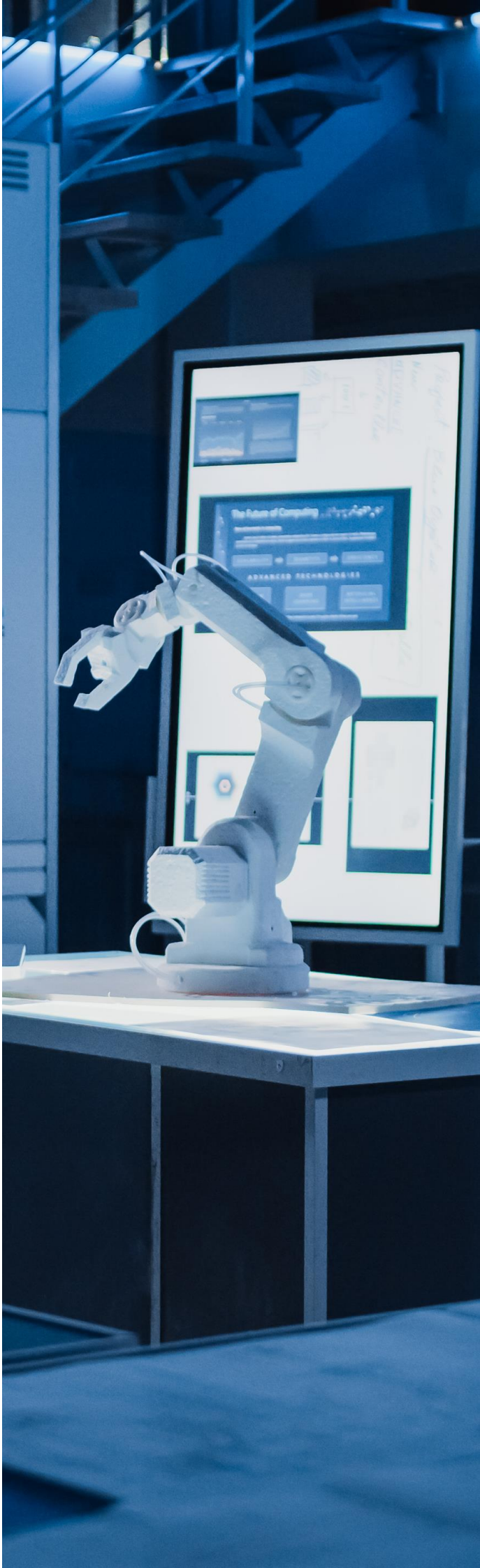
En el proyecto de investigación de NTT DATA se utiliza el aprendizaje por refuerzo (RL) para optimizar el proceso de carga de una batería Dicke, centrando el esfuerzo en diseñar el algoritmo de la función de políticas de un agente RL utilizando algoritmos de optimización cuántica aproximada (QAOA). Se verifica si la energía extraíble (ergotropía) y las fluctuaciones de la energía mecánica cuántica (precisión de carga) se podrían mejorar con respecto a las estrategias de carga estándar. Por otra parte, el estudio también incluirá un análisis del mapa de valor en función de las estrategias utilizadas comparándolas con su "Ground Truth". Esto último tiene como objetivo cuantificarlo a nivel de negocio para verificar cuál sería su impacto económico.

¿Qué beneficios aporta?

Todavía son prototipos de laboratorio a pequeña escala (decenas de cúbits como máximo). No hay una batería Dicke operativa en el sentido clásico (almacenar y recuperar energía eléctrica para dispositivos).

Lo que se ha demostrado es la viabilidad física del efecto de carga colectiva, que es la base de su potencial.

Se espera que estas baterías no sustituyan a las químicas convencionales (litio, sodio, etc.), sino que tengan aplicaciones en nanodispositivos, sensores, y tecnologías cuánticas donde la recarga ultrarrápida y la eficiencia cuántica puedan marcar la diferencia.



La identidad rota: una llamada a la acción en la era de la IA

Tendencias por Jordy Javier Ruiz Sánchez

Llevo años trabajando en la trinchera de la seguridad digital y he sido testigo de una verdad incómoda: la forma en que concebimos la identidad está fundamentalmente rota. Durante décadas, nos aferramos a la idea del usuario y la contraseña como si fueran un castillo inexpugnable. Hoy, ese castillo es de arena, y la marea de la Inteligencia Artificial (IA) está subiendo a una velocidad que nos obliga a actuar.

La IA no es solo una nueva herramienta en el arsenal tecnológico; es el agente de cambio que redefine las reglas del juego. Se ha convertido en una dualidad con la que debemos aprender a vivir: es, por un lado, la mayor amenaza que ha enfrentado la gestión de identidades y, por otro, nuestra defensa más poderosa. Este no es un análisis técnico más, sino una llamada a la acción basada en la guía sobre Gestión de Identidad en IA Agéntica de la Cloud Security Alliance e investigación propia. Por tanto, es hora de dejar de hablar de *"puertas"* y empezar a hablar de *"confianza"*.

Cuando "ser" y "hacer" ya no es suficiente

En esencia, la gestión de identidad siempre ha intentado responder dos preguntas simples: "¿quién eres?" (autenticación) y "¿qué tienes permitido hacer?" (autorización).

Con frecuencia uso analogías simples para explicarlo: la identidad es como entrar al edificio donde trabajas. Muestras tu credencial al guardia, quien comprueba tu foto y tu nombre en la lista. Eso es autenticación. Una vez dentro, tu tarjeta solo te da acceso a un piso y una área, pero no a otros espacios como el despacho del CEO u otros departamentos. Eso es autorización. Este modelo nos sirvió durante un tiempo; sin embargo la IA lo hizo obsoleto. El desafío ya no es solo verificar una identidad estática, sino comprender un contexto dinámico y responder a preguntas mucho más profundas: ¿bajo qué cadena de delegación está actuando este agente de IA?, ¿qué permisos necesita para esta tarea específica (y solo durante los próximos cinco minutos)? y ¿cómo puedo confiar, criptográficamente, en que no ha sido suplantado?

La paradoja de la IA: el pirómano y el bombero

Ahora, la IA ha puesto herramientas increíblemente poderosas tanto en manos de los atacantes como de los defensores. A mi modo de ver, es una carrera tecnológica en la que no podemos permitirnos quedar atrás.

La amenaza: La industrialización del engaño

La IA generativa ha democratizado el fraude; de correos de *phishing* con faltas ortográficas a correos compuestos y personalizados, creados con "Prompt engineering", siendo estos indistinguibles de una comunicación real. Por otro lado, los famosos *deepfakes* y las identidades sintéticas. Procesos que dábamos por seguros, como la verificación de un cliente (Know your customer), se han convertido en un campo minado. Un atacante ya no necesita robar una credencial; puede fabricar una identidad biométricamente perfecta que engañe a nuestros sistemas.

La defensa: hacia una confianza que se adapta

Por suerte, la misma IA nos ofrece la solución. El viejo sueño de "prevenir la brecha" ha muerto. Debemos asumir que el atacante ya está dentro y centrar nuestros esfuerzos en detectarlo y responder con agilidad. Aquí nace la Detección y Respuesta a Amenazas de Identidad (ITDR), una disciplina que usa la IA para aprender cómo se comporta cada identidad (humana o no), y detectar cualquier anomalía en tiempo real.

Imagina a un desarrollador que siempre trabaja desde Madrid de 9 a 5. Si de repente su cuenta intenta acceder a un repositorio de código desde un servidor en Europa del Este a las 3 de la mañana, el sistema no lo bloquea ciegamente. En su lugar, activa una autenticación adaptativa: le exige un segundo factor imposible de falsificar, como una llave física FIDO2. No se trata de construir muros más altos, sino de tener un sistema inmunitario inteligente.

La nueva fuerza laboral: gobernando a las identidades no humanas

Si me preguntan cuál es el mayor punto ciego en la seguridad actual, mi respuesta es clara: tratamos a las máquinas como ciudadanos de segunda clase.

En la mayoría de las empresas, el número de APIs, microservicios, contenedores y agentes de IA ya supera con creces al de los empleados humanos. Son nuestra nueva fuerza de trabajo digital, y el mayor error estratégico es gestionarlos con las herramientas del pasado.

Estas identidades no usan contraseñas. Operan con *tokens*, certificados y claves de API. El reto es gestionar su ciclo de vida a la velocidad de la máquina, no a la velocidad humana. La práctica de incrustar una clave secreta en el código de una aplicación es, sin rodeos, una negligencia. La solución es abandonar las credenciales estáticas y de larga duración por credenciales efímeras y de corta duración. Una aplicación debe poder probar su propia identidad para obtener un *token* válido solo por unos minutos, para una tarea específica, y luego desaparecer.
Como bien señala la Cloud Security Alliance, los protocolos tradicionales son insuficientes para la naturaleza dinámica de la IA. La frontera ahora está en los Identificadores Descentralizados (DIDs) y las Credenciales Verificables (VCs) que permiten a un agente probar criptográficamente quién es, qué puede hacer y quién le dio esa autoridad. Estamos construyendo una economía de confianza para las máquinas.

Un ciclo de vida para cada identidad: principios para la acción

Por tanto, un enfoque moderno de IAM debe ser implacable en cada fase del ciclo de vida, tanto para humanos como para máquinas.

- En el alta (*provisioning*): el primer paso es un inventario. Asigna un propietario humano a cada identidad no humana para erradicar las "cuentas huérfanas". Para tus empleados, exige desde el día uno un MFA resistente al *phishing*, como los *passkeys* (FIDO2). Por el momento, es la medida más efectiva que podemos adoptar.

- Durante su vida (gestión – modificación - cambio): la gobernanza debe ser continua. Las revisiones de acceso periódicas, asistidas por IA que sugiere eliminar permisos no utilizados (ingeniería de roles), son cruciales para mantener el principio de mínimo privilegio.

- En la baja (deprovisioning): esta fase es crítica. Cuando un empleado se va o una aplicación se retira, sus accesos deben ser revocados de forma instantánea y total. Las credenciales huérfanas son puertas traseras esperando a ser descubiertas. Necesitamos sistemas que puedan ejecutar una revocación global e inmediata de todas las sesiones activas de una identidad comprometida.

Conclusión: la identidad es el nuevo perímetro

Hemos dejado atrás la era en que la gestión de identidades se centraba en una función de soporte de TI. Hoy, es el núcleo estratégico que habilita o frena la innovación segura con IA. Ya no gestionamos personas que acceden a sistemas; gobernamos un ecosistema vivo de humanos, máquinas y agentes autónomos. Adoptar estas estrategias no es una opción, es un imperativo.

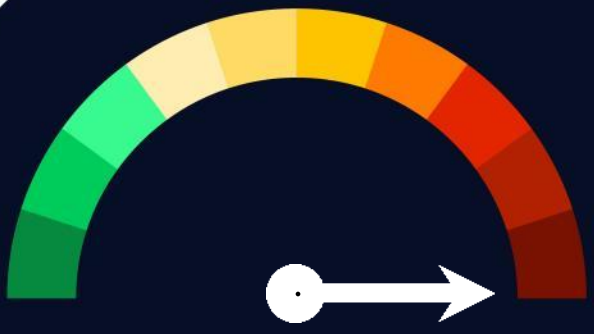
En un mundo donde la identidad se puede fabricar, la única defensa es una confianza que nunca se asume y siempre se verifica. La Confianza Cero (*Zero Trust*) no es una arquitectura, es la filosofía que nos permitirá navegar esta nueva frontera. Y la IA, con todos sus riesgos, es la opción más viable que tenemos para hacerlo a escala.

Jordy Javier Ruiz Sánchez
Cybersecurity Analyst

Vulnerabilidades

Vulnerabilidad crítica en SAP NetWeaver

Fecha: 8 de septiembre de 2025
CVE: CVE-2025-42944



CVSS: 10

CRÍTICA

Descripción

La vulnerabilidad CVE-2025-42944 representa una amenaza crítica para los entornos que operan con SAP NetWeaver, ya que permite la ejecución remota de comandos sin necesidad de autenticación.

Este fallo está basado en una deserialización insegura (CWE-502) debido al módulo vulnerable RMI-P4, que actúa como puerta de entrada para que un atacante manipule objetos serializados y ejecute código arbitrario en el servidor.

La ausencia de autenticación previa amplifica el riesgo de ataque, permitiendo a actores maliciosos externos interactuar directamente con el sistema vulnerable.

Solución

Las recomendaciones de SAP son las siguientes:

- Actualización inmediata a la última versión disponible.
- Implementación de controles adicionales de acceso a la herramienta.

Productos afectados

Esta vulnerabilidad crítica afecta a:

- SAP NetWeaver ServerCore versión 7.50

Referencias

- nvd.nist.gov
- zeropath.com

TLP:WHITE

Vulnerabilidades

Vulnerabilidad de WhatsApp explotada en iOS y MacOS

Fecha: 29 de agosto de 2025
CVE: CVE-2025-55177

CVSS: 5.4

MEDIA

Descripción

La vulnerabilidad CVE-2025-55177 en WhatsApp, de tipo *zero-click*, afecta a iOS, iPadOS y macOS.

Esta se debe a una autorización insuficiente en la sincronización de dispositivos, lo que permite ejecutar código o instalar *spyware* con solo recibir un mensaje manipulado.

El fallo explota la forma en que WhatsApp procesa objetos y archivos multimedia, causando corrupción de memoria.

Aunque se detectó en pocos casos, evidencia el alto riesgo de ataques invisibles y cadenas de explotación para espionaje.

Solución

Se recomienda aplicar de inmediato los parches oficiales de WhatsApp y Apple:

- iOS e iPadOS: versión 2.25.21.73 o posteriores
- macOS: versión 2.25.21.78 o posteriores

Productos afectados

Las versiones vulnerables son las siguientes:

- iOS: desde 2.22.25.2 hasta 2.25.21.73
- macOS: hasta 2.25.21.78

Referencias

- incibe.es
- nvd.nist.gov

TLP:WHITE

Citrix corrige vulnerabilidades en NetScaler ADC y Gateway.

Fecha: 26 de agosto de 2025
CVE: CVE-2025-7775 y 2 más

Crítica

Descripción

Recientemente se han detectado varias vulnerabilidades Citrix NetScaler.

La CVE-2025-7775 es una vulnerabilidad crítica de desbordamiento de memoria que podría permitir la ejecución remota de código o provocar denegación de servicio. Esto, siempre y cuando NetScaler esté configurado como puerta de enlace o servidor virtual AAA, vinculado con servicios IPv6 o con un servidor virtual CR tipo HDX.

La CVE-2025-7776, de severidad alta, también es un desbordamiento de memoria que puede causar un comportamiento erróneo o denegación de servicio, requiriendo que NetScaler esté configurado como puerta de enlace con un perfil PCoIP vinculado.

Por su parte, la CVE-2025-8424 es una vulnerabilidad de control de acceso inadecuado en la interfaz de administración, que podría permitir acciones no autorizadas si el atacante tiene acceso a NSIP, IP de administración de clúster, IP de sitio GSLB local o SNIP con privilegios administrativos.

Productos afectados

- NetScaler ADC y NetScaler Gateway: versiones anteriores a 13.1-59.22 y versiones anteriores a 14.1-47.48.
- NetScaler ADC FIPS/NDcPP: versiones anteriores a 13.1-37.241 y 12.1-55.330, respectivamente.

Solución

Cloud Software Group recomienda a los clientes afectados instalar las versiones más actualizadas.

Referencias

- nvd.nist.gov
- support.citrix.com

TLP:WHITE

Google corrige una vulnerabilidad en Android Runtime

Fecha: 29 de agosto de 2025
CVE: CVE-2025-48543

Alta

Descripción

Google ha corregido la vulnerabilidad de escalada de privilegios conocida como CVE-2025-48543.

Esta vulnerabilidad explota un fallo de seguridad después de la liberación en Android Runtime para escapar del entorno aislado de Chrome y comprometer el proceso *system_server* en dispositivos Android.

Posteriormente, puede conducir a una escalada de privilegios locales sin requerir ninguna interacción por parte del usuario.

La explotación exitosa de CVE-2025-48543 podría permitir a los atacantes obtener privilegios elevados en el dispositivo Android.

Productos afectados

Algunos de los productos afectados son los siguientes:

- Google Android 16
- Google Android 15
- Google Android 14
- Google Android 13

Solución

Google reforzó la seguridad de Android Runtime (ART), distribuyendo el parche vía Google Play para proteger de inmediato los dispositivos con GMS, incluso antes de las actualizaciones del sistema operativo.

Referencias

- nvd.nist.go
- source.android.com

Eventos

Cyber Security World Asia
8 - 9 de octubre

El 8 y 9 de octubre de 2025 en el Marina Bay Sands Expo & Convention Centre de Singapur, se realizará este encuentro clave en ciberseguridad. El evento reunirá a líderes y especialistas para abordar temáticas como *Zero Trust*, inteligencia artificial aplicada a la ciberdefensa, gestión de identidades, seguridad en la nube, protección de redes, criptografía cuántica y respuesta ante incidentes, consolidándose como la cita más relevante de la región dentro de la Tech Week Singapore.

Enlace

Forum InCyber Canadá
14 – 15 de octubre

El 14 y 15 de octubre de 2025 en el Palais des Congrès de Montreal (Canadá) se celebrará este foro internacional sobre ciberseguridad y confianza digital. El evento abordará temas como amenazas emergentes, *ransomware*, seguridad en la nube, inteligencia artificial, criptografía cuántica, protección de infraestructuras críticas y movilidad inteligente, consolidándose como el principal punto de encuentro en Norteamérica para líderes y expertos del sector.

Enlace

InfoSec World 2025
27 - 29 de octubre

Del 27 al 29 de octubre de 2025 en Disney's Coronado Springs Resort, Florida (EEUU), se celebra esta conferencia líder en ciberseguridad. Abordará temáticas como inteligencia de amenazas, seguridad en la nube, gestión de identidades, *Zero Trust*, resiliencia, respuesta a incidentes y riesgos en la cadena de suministro, consolidándose como un espacio clave para profesionales y líderes del sector.

Enlace

Recursos

➢ EU Cybersecurity Index 2024

El EU Cybersecurity Index, publicado por ENISA, evalúa la postura de ciberseguridad de los Estados miembros de la UE, midiendo áreas clave como políticas, capacidades técnicas, mercado e industria, y operaciones. El informe identifica fortalezas y brechas, destacando desafíos en la adopción de IA, certificación de CSIRT, inversiones en ciberseguridad y acceso a fondos de innovación, sirviendo como herramienta de referencia para mejorar la resiliencia digital y armonizar estrategias a nivel europeo.

Enlace

➢ Guía Técnica de Implementación de NIS2

ENISA publica esta guía para apoyar a entidades de infraestructura digital, proveedores de servicios TIC y plataformas digitales en la implementación de la Directiva NIS2. Ofrece orientación práctica sobre gestión de riesgos, políticas de seguridad, manejo de incidentes, continuidad del negocio, seguridad en la cadena de suministro y desarrollo seguro, facilitando la adopción de medidas de ciberseguridad y mejorando la resiliencia digital en sectores críticos.

Enlace

➢ Metodología del Panorama de Amenazas Cibernéticas

ENISA ha actualizado su metodología para la elaboración del Panorama de Amenazas Cibernéticas con el objetivo de proporcionar un enfoque más práctico y estructurado en la producción de informes horizontales, temáticos y sectoriales. La metodología define procesos clave, partes interesadas, herramientas y elementos de contenido, promoviendo la transparencia y consistencia en el análisis de amenazas cibernéticas en Europa.

Enlace

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com