Número 116 | Julio 2026

NTT DATA

Radar

El magazine de ciberseguridad

Identity as the New Perimeter: La confianza empieza en cada identidad

Por Hans Vigil Navas

Durante años, la ciberseguridad se apoyó en una idea simple: proteger el perímetro. Había una red interna, usuarios conocidos, sistemas bajo control y una frontera relativamente clara entre lo confiable y lo externo. Firewalls, segmentos de red y controles en la entrada parecían suficientes para defender aquello que la organización consideraba crítico. **Pero esa frontera dejó de ser evidente.**

La nube, el trabajo híbrido, las APIs, los terceros, la automatización industrial y la inteligencia artificial han convertido el acceso en una conversación permanente entre personas, aplicaciones, máquinas y sistemas que operan dentro y fuera de la organización. **Hoy, el riesgo ya no aparece únicamente cuando alguien intenta cruzar una barrera**. Muchas veces, el riesgo ya está dentro, usando una credencial válida, un token activo, un certificado olvidado o una cuenta de servicio con más privilegios de los necesarios.

En este nuevo escenario, la identidad se ha convertido en el nuevo perímetro. No se trata solo de una frase de tendencia. Es una realidad operativa. **Cada identidad representa una posibilidad de acceso, una decisión de confianza y, al mismo tiempo, una puerta potencial hacia los activos críticos de la organización**. Algunas identidades pertenecen a personas. Otras, a aplicaciones, servicios, dispositivos, procesos automatizados o agentes capaces de ejecutar tareas en nombre de alguien más. Y muchas de ellas no aparecen en los inventarios tradicionales ni son revisadas con la misma rigurosidad que un usuario humano.

El desafío es que la confianza digital se ha vuelto más difícil de observar. Una organización puede contar con buenas herramientas de monitoreo, cifrado, respuesta ante incidentes y protección de red; pero si no sabe quién accede, qué accede, con qué privilegios, desde dónde, por cuánto tiempo y en nombre de quién actúa, su postura de seguridad sigue incompleta. **La identidad deja de ser un componente administrativo de TI para convertirse en una capacidad crítica de gobierno, resiliencia y continuidad.**
En banca, una identidad comprometida puede convertirse en fraude. En seguros, en exposición de información sensible. En minería, en interrupción productiva. En industria, en impacto operacional. En todos los casos, el origen suele ser el mismo: una confianza mal gobernada.

Para los sectores financiero y asegurador, esta realidad es especialmente relevante. La identidad está en el centro de la prevención del fraude, la protección de datos de clientes, el control de accesos privilegiados, la seguridad de canales digitales, el uso de APIs y la relación con terceros. En estos entornos, no basta con implementar controles; es necesario demostrar que funcionan, que se revisan, que generan evidencia y que permiten responder ante auditores, reguladores y directorios.

En minería e industria, el impacto puede ser aún más tangible. Una identidad comprometida no siempre termina en una filtración de datos; también puede abrir la puerta a accesos remotos no autorizados, cuentas compartidas, credenciales persistentes de proveedores, estaciones de ingeniería o sistemas que sostienen procesos críticos. En estos sectores, la identidad no solo protege información. También protege disponibilidad, continuidad operacional, seguridad física y capacidad productiva.

Por eso, hablar de Identity as the New Perimeter no significa hablar únicamente de una nueva herramienta de IAM. Significa replantear la forma en que la organización entiende la confianza. Cada acceso debe ser explícito, verificable, mínimo, trazable y revocable. Cada identidad debe tener un propósito, un responsable, un ciclo de vida y controles asociados. Cada privilegio debe responder a una necesidad real del negocio. Y cada excepción debe tratarse como un riesgo, no como una costumbre operativa.

Los principales marcos internacionales vienen señalando ese camino desde distintas perspectivas. NIST lo plantea desde Zero Trust: no confiar de forma implícita y verificar continuamente. ISO/IEC 27001 lo aterriza desde la gestión del riesgo, los controles de acceso, la relación con terceros y la mejora continua. OWASP lo evidencia desde las fallas recurrentes en autenticación, autorización, seguridad de APIs e identidades no humanas. Aunque parten de enfoques distintos, todos apuntan a una misma conclusión: la confianza debe gobernarse.

La gestión de identidades no humanas se vuelve, entonces, un punto crítico. En muchas organizaciones, estas identidades ya superan ampliamente a las humanas en volumen y criticidad. Certificados digitales, secretos, tokens, cuentas de automatización, integraciones entre plataformas, servicios cloud, dispositivos conectados y procesos automatizados operan en segundo plano sosteniendo funciones esenciales del negocio. Cuando una de estas identidades es comprometida, el atacante no necesita romper el perímetro: simplemente actúa como si perteneciera a él.

A este escenario se suma una nueva capa de complejidad: los agentes de identidad o **ID Agents**. **A medida que la inteligencia artificial evoluciona hacia modelos más autónomos, aparecen agentes capaces de actuar en nombre de una persona, una aplicación o un proceso**. Pueden consumir APIs, ejecutar tareas, tomar decisiones asistidas y operar con cierto grado de independencia. La pregunta, entonces, ya no es solo "quién accede", sino "en nombre de quién actúa este agente, con qué autoridad, bajo qué límites y con qué trazabilidad".

La autonomía sin gobierno puede convertir a la identidad en un punto ciego. La autonomía con controles, en cambio, puede fortalecer la eficiencia sin sacrificar seguridad. Ese es el reto para los CISOs. Integrar el gobierno de accesos, la gestión de privilegios, la protección de secretos, la seguridad de APIs, el control de terceros y la supervisión continua bajo una misma visión de riesgo. En banca y seguros, esto se traduce en prevención del fraude, cumplimiento, evidencia y confianza del cliente. En minería e industria, se traduce en continuidad, disponibilidad y protección de entornos físico-digitales. En ambos casos, la identidad deja de ser un control aislado para convertirse en un eje transversal de defensa y resiliencia.

En esta edición de *Radar*, abordamos precisamente ese cambio de paradigma. La seguridad ya no puede depender de fronteras que el negocio ha dejado atrás. Debe construirse alrededor de identidades verificables, humanas y no humanas, gestionadas durante todo su ciclo de vida y alineadas con estándares, riesgo y regulación.

El nuevo perímetro no está en la red, sino en cada identidad con capacidad de actuar. Algunas son humanas, otras son máquinas y otras serán agentes autónomos. Todas requieren gobierno. Porque en la era de la hiperconexión, la confianza ya no se concede: se verifica, se limita, se monitorea y se revoca.

Hans Vigil Navas
Cybersecurity Manager

Las llaves del reino: la identidad como principal vector de ataque

Cibercrónica Nelson Andrés Barboza Landinez

Durante décadas, la seguridad corporativa se construyó sobre una premisa simple: hay un adentro y un afuera. El firewall era la muralla, la VPN el puente levadizo, los antivirus eran guardias apostados en cada esquina. Una fortaleza sólida, predecible y diseñada para un mundo donde los enemigos venían del exterior, y los aliados permanecían en el interior. Pero ese mundo desapareció. El trabajo remoto abrió puertas laterales; las integraciones SaaS entregaron las llaves a decenas de proveedores externos. Hoy no hay adentro. Hay identidades.

De acuerdo con el reporte de respuesta de incidentes de Unit 42 para 2026, el 65% de los accesos iniciales en ciberataques fueron llevados a cabo por medio de técnicas basadas en identidad, permitiendo acceso no autorizado, movimientos laterales, y escalamiento de privilegios. Técnicas como el phishing, credenciales robadas, intentos de fuerza bruta, malas configuraciones en IAM y actividad por parte de insiders llevan las riendas de las brechas modernas. En un mundo donde se invierten cantidades significativas de dinero y recursos en ciberdefensas, los atacantes optan por pasar directamente por la puerta principal. El DBIR 2025 de Verizon lo confirma: el 22% de las brechas comienzan con credenciales robadas, un incremento del 34% con respecto al año anterior. No están irrumpiendo. Están iniciando sesión.

La rápida adopción de infraestructura en la nube, SaaS, cuentas empleadas por aplicaciones, servicios y procesos automatizados gestaron el entorno digital en el cual cada integración representa una potencial ruta de acceso. El mismo reporte de Unit 42 demostró que, en una muestra de 680.000 identidades en la nube, el 99% de usuarios, roles y servicios poseían permisos excesivos, incluidos accesos que no habían sido utilizados durante más de 60 días.

El atacante no necesita escalar por la fuerza; simplemente camina por los pasillos que nadie cerró. A esto se suma la creciente amenaza de la computación cuántica sobre los esquemas de cifrado actuales y la anticipada reducción del tiempo de vida de certificados TLS. El reloj corre, y la superficie de exposición crece. El reporte de CyberArk 2025 encuestó a 1.200 líderes de seguridad en organizaciones de Estados Unidos, Reino Unido, Australia, Francia y Alemania, revelando que la mayoría presenta inconvenientes serios en el manejo efectivo de las identidades de sus máquinas.

Los casos del 2025 lo ilustran con contundencia. Marks & Spencer, minorista multinacional británico, fue blanco de un ciberataque atribuido al grupo “Scattered Spider” en Abril del 2025.

La compañía confirmó el cifrado de múltiples servidores, impactando significativamente su infraestructura.

La brecha de seguridad no ocurrió de la nada; fue todo un proceso donde la gestión de identidades fue el eslabón más débil. Durante la intrusión, los actores maliciosos obtuvieron acceso un archivo NTDS.dit, lo que les permitió extraer hashes de contraseñas facilitando a los actores maliciosos el escalamiento de privilegios en la red. Si bien el mecanismo exacto de compromiso inicial no ha sido confirmado, diversas fuentes apuntan a que el grupo Scattered Spider emplea habitualmente campañas de phishing, vishing e intentos de fatiga MFA para obtener acceso a cuentas corporativas. Posteriormente, el despliegue del DragonForce ransomware encryptor resultó en la afectación en la continuidad de múltiples servicios corporativos y comerciales, además del acceso no autorizado a información de clientes, confirmado por la organización.

Meses después, entre el 8 y 18 de Agosto otra campaña de robo de información se llevó a cabo sobre la plataforma de automatización de compras Salesloft, apuntando especialmente a instancias de clientes de Salesforce por medio del compromiso de tokens Oauth asociados con el agente de inteligencia artificial Drift. Según Cloudflare, la ruta de ataque fue la enumeración de objetos, el reconocimiento del alcance del entorno comprometido, y la descarga de información mediante interfaces legitimas de Salesforce.

Finalmente, y como parte de una operación cuidadosamente ejecutada, la eliminación de los jobs para ocultar su cometido. El actor malicioso, identificado por Google Threat Intelligence Group (GTIG) como UNC6395, habría afectado alrededor de 700 organizaciones, incluyendo instituciones financieras, proveedores de salud, compañías de tecnología y agencias gubernamentales.

Cory Michal, CSO de AppOmni, afirmó que muchas de las organizaciones comprometidas son en sí compañías de software y seguridad, lo cual indica que la campaña puede ser un movimiento de apertura hacia futuros ataques de cadena de suministro.

No fue un error técnico en endpoints o en la red. Fue una falla en la identidad del agente. Tokens OAuth de larga duración, con scopes permisivos, de un agente de confianza que nadie monitoreaba. Las organizaciones confían en las integraciones como en los empleados, pero no las gobiernan. Los agentes son identidades. Y las identidades sin gobernanza son puertas abiertas.

Solo un par de semanas después, Jaguar Land Rover reveló que sufrió un devastador ciberataque el 31 de Agosto del 2025, que le costó a la compañía £196 millones. Adicionalmente, de acuerdo con The Cyber Monitoring Center, generó un impacto sobre la economía del Reino Unido estimado en £1.900 millones debido al cierre total de las operaciones globales de manufactura por cinco semanas. El ataque, atribuido al grupo Scattered LAPSUS$ Hunters, cuya filosofía es "log in, not hack in", fue posible gracias al robo de credenciales mediante un infostealer, un tipo de malware diseñado para extraer contraseñas, cookies de sesión y otra información sensible de los equipos comprometidos, pertenecientes en este caso a un tercero con acceso al sistema Jira de JLR.

El primero de Septiembre, el equipo de TI del JLR detectó una intrusión en su red y tomó una medida drástica al apagar todos sus sistemas para contener el daño. El grupo de hackers, como evidencia, publicó imágenes de los sistemas internos en Telegram, donde exponían el acceso a dominios como jlrint.com. Sin embargo, los análisis posteriores revelaron que la intrusión no fue el resultado de una zero day; fue un conjunto de tácticas tales como ingeniería social, abuso de credenciales, una detección deficiente y una segmentación débil entre la red corporativa y los sistemas de producción.

Casos como estos no ocurren en el vacío. La inteligencia artificial juega un rol determinante en la velocidad en la que se ejecutan estas campañas de robo de identidad. El análisis de 32 millones de correos de phishing documentado en el Darktrace Annual Threat Report 2026 mostró una tendencia clara: los ataques de phishing son cada vez más sofisticados y potencialmente más efectivos en casos donde dichos emails llegan a manos de usuarios altamente privilegiados.

Lo cual no parece descabellado, teniendo en cuenta que el 70% de estos emails pasaron controles de autenticación DMARC, permitiendo evadir controles de monitoreo y detección.

Nathaniel Jones, vicepresidente de seguridad y estrategia de IA en Darktrace, afirma: "El perímetro de defensa tradicional fue construido para un mundo donde los atacantes tenían que irrumpir". Aun cuando los actores malintencionados históricamente basaban sus estrategias en exploits técnicos, el desarrollo de la IA les ha permitido operar con mayor precisión, adoptando técnicas como el vishing y los deepfakes, apuntando a las identidades como vector de acceso inicial más que a la infraestructura en sí.

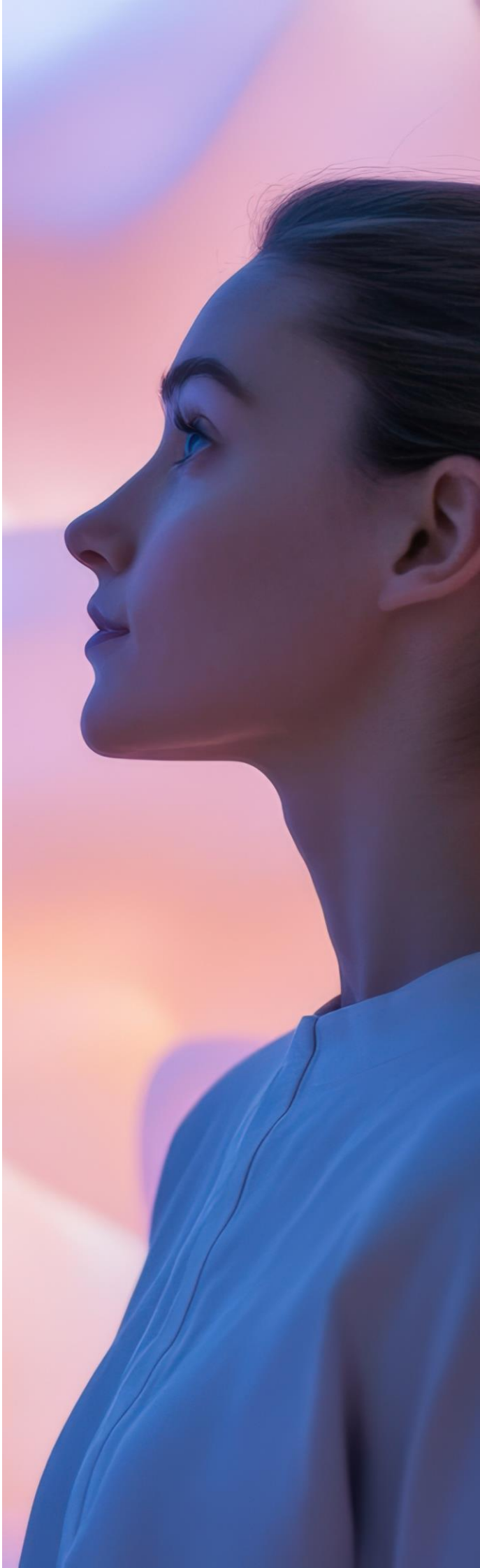
Mitigaciones efectivas, tales como el despliegue de MFA resistente a phishing, la gobernabilidad de identidades, la implementación y ejecución efectiva del principio del mínimo privilegio, además de soluciones de monitoreo integradas con inteligencia artificial donde se detecten comportamientos anómalos; tales como tokens creados por primera vez desde nuevas regiones o patrones inusuales en el consumo de APIs, entre otros, son elementos fundamentales de una estrategia de defensa moderna.

También resulta indispensable una respuesta a incidentes mediante playbooks que contemplen la posibilidad de que intrusos se encuentren dentro del sistema. De igual manera, ejercer un control sobre la reutilización de contraseñas y la identificación de identidades divulgadas que ya circulan online, son prácticas esenciales en este nuevo mundo donde las identidades han tomado su lugar en el desarrollo tecnológico.

Si bien es cierto que las contraseñas nunca han sido seguras, en este momento los hechos hablan por sí solos. En esta nueva era revolucionada por la inteligencia artificial, las contraseñas como único mecanismo de autenticación han demostrado ser insuficientes frente a las amenazas actuales. Es momento de migrar hacia mecanismos de autenticación más robustos. La confidencialidad, integridad y disponibilidad de los sistemas no pueden depender únicamente de murallas diseñadas para resistir ataques externos; también requieren proteger las puertas principales y vigilar quién tiene acceso al interior.

A través de los años, se han invertido millones en reforzar murallas digitales, convencidos de que el peligro vendría desde afuera. Sin embargo, algunos de los incidentes más catastróficos de los últimos meses muestran una realidad distinta: los atacantes ya no necesitan derribar puertas. Les basta con obtener las llaves. En la era de la nube, los agentes inteligentes y la inteligencia artificial, cada usuario, servicio, token, aplicación y máquina posee una identidad propia. Esa identidad se ha convertido en el nuevo perímetro de seguridad.

Nelson Andrés Barboza Landinez
Cybersecurity Engineer



La Identidad: El riesgo que ha evolucionado junto a la IA

Artículo por Jaime Andrés Tovar Prieto

¿Cuántos agentes de IA operan ahora mismo en tu organización con acceso amplio y sin identidad verificable? ¿Se sabe qué identidad están usando? ¿Desde cuándo llevan operando con esa identidad asignada? En los últimos años, la inteligencia artificial ha consolidado su presencia en el ecosistema tecnológico empresarial y ha evolucionado más allá de los modelos generativos o conversacionales estandarizados, diseñados para interpretar un contexto y generar respuestas bajo la supervisión constante de un ser humano, modelo conocido como Human-in-the-Loop (HITL). La siguiente etapa de esta evolución son los agentes de IA: componentes de software autónomos que no solo interpretan entradas y planifican estrategias, sino que ejecutan tareas tangibles a través de la comunicación con APIs (Application Programming Interface), interactúan con bases de datos, otros agentes y sub-agentes en flujos de trabajo coordinados, todo ello con una intervención humana mínima o nula en cada paso individual del proceso.

La gobernanza convencional de la IA se ha centrado en mitigar el riesgo asociado a las *respuestas* del modelo, evaluar si es preciso, justo, ético o libre de sesgos y alucinaciones, bajo la premisa de que un ser humano revisará los resultados antes de tomar una decisión o ejecutar una acción. Sin embargo, el gobierno de la IA agéntica exige un cambio estructural y conceptual, el control del riesgo debe orientarse hacia la ***acción***. Un agente dotado de autonomía puede iniciar transacciones financieras complejas, actualizar registros de clientes en sistemas corporativos o aplicar configuraciones en dispositivos de seguridad de infraestructura crítica, sin esperar ninguna confirmación humana interactiva. Por consiguiente, la ausencia de controles estrictos y dinámicos en tiempo de ejecución puede derivar en escaladas de privilegios no intencionadas, fuga masiva de datos y alteraciones sistémicas que comprometan la continuidad del negocio.

La nueva frontera del riesgo: la respuesta a la acción

Estos escenarios han generado alertas de alto nivel en la industria. Gartner proyecta que para el año 2027, el 40% de las empresas se verán obligadas a degradar o desmantelar por completo sus despliegues de agentes autónomos debido a debilidades en los modelos de gobierno. Las organizaciones que no logran distinguir entre la capacidad técnica de un agente para ejecutar una acción y el alcance legítimo de los permisos que se le han otorgado se enfrentan a un riesgo operativo inminente e insostenible.

Ante este escenario, resulta imperativo analizar la nueva frontera del riesgo, en la que la Identidad emerge como el componente crítico aún en evolución dentro del contexto de la IA.

Okta señala en su artículo *"What is AI Agent Identity? Securing Autonomous Systems"* que, en promedio, una organización gestiona 45 identidades de máquina — o NHIs (Non-Human Identities, identidades no humanas) — por cada usuario humano. Sin embargo, mientras las NHIs tradicionales operan bajo parámetros predecibles y secuencias de comandos predefinidas sin consciencia de su entorno, los agentes de IA poseen capacidad para razonar, adaptar sus estrategias iterativamente según el contexto, retener información para mejorar la toma de decisiones y ejecutar acciones autónomas con impacto real sobre los entornos. Aplicar los modelos de identidad rígidos vigentes a la IA agéntica puede generar brechas de seguridad de alto impacto.

IAM Estándar vs. Identidad Agéntica: diferencias fundamentales

Las diferencias estructurales entre la gestión de identidad convencional y los requerimientos únicos de la identidad agéntica se manifiestan en tres dimensiones críticas que alteran fundamentalmente el ciclo de vida de la identidad:

- **Vigencia:** La identidad de un usuario humano puede mantenerse activa durante días, meses o años, y requiere validaciones interactivas — biometría, contraseñas, tokens o mecanismos de doble factor. Los agentes, en cambio, operan de forma continua y sin intervención humana constante; sus identidades pueden ser efímeras, existiendo apenas los segundos que tarda en completarse una transacción.

- **Autorización Delegada:** Las cuentas humanas actúan por sí mismas. Los agentes de IA, en cambio, actúan *en nombre de* (On-Behalf-Of — OBO) un humano, un sistema o un servicio. Esto exige cadenas de delegación criptográficamente rigurosas e intercambios de tokens que preserven la responsabilidad y la trazabilidad forense, vinculadas de forma indisoluble al delegante original.

- **Control de Acceso:** La asignación estática de roles es incapaz de seguir el ritmo de un agente que encadena tareas complejas y toma miles de decisiones de acceso por minuto. Los agentes requieren una evaluación continua del contexto, del riesgo ambiental y de los atributos específicos de cada tarea, instrumentada mediante Policy-as-Code (políticas como código).

Vectores de riesgo en entornos de IA no gobernados

Cuando la velocidad de implementación supera la madurez del gobierno sobre IA (escenario altamente probable en el contexto actual), las organizaciones se exponen a riesgos estructurales derivados de NHIs no gestionadas. Los principales vectores son:

- **Acceso Persistente No Gobernado:** Los agentes que operan con credenciales permanentes o tokens de acceso de larga vida se convierten en objetivos de alto valor. Si un modelo es comprometido por ejemplo, mediante una inyección de prompts maliciosa, el atacante hereda todo el acceso permanente del agente y puede operar libremente dentro del perímetro corporativo.

- **Escalada de Privilegios y Deriva de Autoridad (Privilege Drift):** En entornos dinámicos, un agente puede invocar herramientas o asumir roles que acumulan derechos nunca aprobados explícitamente por un administrador de seguridad. Esta deriva se manifiesta frecuentemente como una expansión progresiva de autoridad a lo largo del tiempo, no como un cambio abrupto e inmediato en los resultados generados.

- **Falta de Atribución y Evasión de Auditoría:** Cuando un agente modifica una base de datos utilizando una cuenta de servicio genérica o compartida, la acción pierde su contexto de delegación. La imposibilidad de distinguir algorítmicamente una acción humana de una sintética elimina la auditoría de cuentas (Accountability) y vulnera normativas de cumplimiento estrictas.

Marco de gobierno para identidades agénticas

El primer paso hacia un gobierno efectivo es el establecimiento de un marco de medición de riesgo aplicado a los agentes.

Es fundamental evitar la implementación de un modelo de seguridad uniforme para todos ellos, dicho enfoque puede derivar tanto en una sobreprotección operativa que limite la productividad como en una exposición al riesgo por subestimación de las capacidades reales del agente. Las políticas de seguridad deben ser proporcionales al contexto y las capacidades específicas de cada entidad agéntica.

El IAM tradicional fue diseñado para gestionar identidades humanas con ciclos de vida predecibles y autenticación interactiva. En entornos de IA agéntica, este modelo resulta estructuralmente insuficiente: los agentes no poseen credenciales propias en el sentido convencional, actúan por delegación y operan a velocidades que superan cualquier proceso de revisión humana. Para salvar esta brecha, la arquitectura demanda una capa de abstracción superior conocida como Identity Fabric. Plataformas empresariales avanzadas, actúan como este Identity Fabric, conectando diversas aplicaciones, proveedores de identidad (IDPs) y entornos híbridos y multi-nube sin requerir la reescritura de aplicaciones existentes.

La orquestación que ofrece el Identity Fabric no se limita a conectar sistemas: centraliza la gestión de identidad en seis dimensiones operativas:

- **Autenticación:** Proveer servicios de inicio de sesión modernos y adaptativos, superando los protocolos heredados con vulnerabilidades conocidas.

- **Control de Acceso (Access Control):** Imponer políticas granulares y consistentes a nivel de individuo, grupo o máquina a través de un único plano de control unificado.

- **Autorización:** Establecer reglas precisas que determinen qué funciones específicas puede ejecutar un agente y bajo qué condiciones exactas de entorno.

- **Atributos:** Proveer datos dinámicos del usuario desde cualquier IDP en tiempo de ejecución para soportar decisiones de seguridad contextualizadas y personalizadas.

- **Administración:** Gestión centralizada y visual de políticas a través del ecosistema.

- **Auditoría:** Observabilidad profunda de la actividad real frente a los permisos otorgados, para demostrar cumplimiento normativo de forma continua.

Hacia un framework de autenticación para agentes: SPIFFE

Los mecanismos de autenticación habituales en entornos web — JWT, OAuth, credenciales estáticas y API Keys — resultan insuficientes para gestionar la autenticación en ecosistemas de IA agéntica. Para mitigar esta brecha, emerge un componente arquitectónico clave: **SPIFFE** (Secure Production Identity Framework for Everyone).

SPIFFE aborda específicamente un riesgo de seguridad anidado, frecuentemente descrito como el efecto de "*muñeca rusa*": si un atacante compromete a un sub-agente en un nivel profundo de la cadena mediante inyección de prompts, podría heredar los amplios privilegios otorgados al agente principal, causando un daño catastrófico a través de una técnica documentada como "*Contrabando de Sesión Agéntica*" (Agent Session Smuggling).

SPIFFE proporciona un mecanismo estandarizado para emitir identidades criptográficamente verificables al software, basándose en su procedencia y contexto de ejecución, sin requerir intervención humana para el aprovisionamiento de credenciales. Su elemento central es el **SVID** (SPIFFE Verifiable Identity Document): una credencial efímera, firmada criptográficamente una asersión.

Los **SVIDs** son administrados mediante **SPIRE** (SPIFFE Runtime Environment), que garantiza su rotación automática a lo largo de todo el ciclo de vida del agente. Este mecanismo elimina por completo el vector de persistencia maliciosa y materializa un enfoque puro de Zero Trust.

Conclusión

La identidad en entornos de IA agéntica no es un problema técnico menor: es el eje central sobre el que se construye — o se destruye — la confianza operativa de una organización. Mientras los agentes continúen proliferando sin identidades verificables, sin ciclos de vida gobernados y sin trazabilidad criptográfica, cada automatización autónoma representa un vector de riesgo abierto. El camino hacia una postura de seguridad madura en IA exige adoptar los principios de Zero Trust no como lineamientos estáticos teóricos, sino como arquitectura ejecutable: identidades efímeras, aprovisionadas Just-in-Time, con privilegios mínimos y auditabilidad continua.

Jaime Andrés Tovar Prieto
Cybersecurity Architect

El riesgo invisible: Cómo las Identidades No Humanas están redefiniendo la Ciberseguridad

Artículo por César Vega Calderón

Las identidades no humanas actualmente constituyen uno de los vectores de riesgo de más rápido crecimiento. Su adecuada gestión será determinante para la ciber resiliencia de las organizaciones en la era de la nube, la automatización, la transformación digital y la inteligencia artificial.

La adopción acelerada de servicios en la nube, automatización, DevOps e inteligencia artificial ha impulsado un crecimiento exponencial de las identidades no humanas (NHI, por sus siglas en inglés). Estas identidades —utilizadas por aplicaciones, APIs, cuentas de servicio, contenedores, dispositivos IoT y agentes de IA— son esenciales para la operación moderna de las organizaciones, pero también representan una de las superficies de ataque de más rápido crecimiento.

La explosión de las identidades no humanas

Durante años, las estrategias de gestión de identidades y accesos (IAM, por sus siglas en inglés) se concentraron principalmente en usuarios humanos. Hoy esa realidad ha cambiado. Las organizaciones modernas operan miles de identidades asociadas a sistemas automatizados que requieren autenticarse continuamente para acceder a datos, servicios y recursos críticos.
Diversos estudios de la industria muestran que las identidades no humanas superan ampliamente a las identidades humanas en una proporción promedio de 50 a 1 en muchos entornos empresariales. Okta, una de las compañías líderes en la gestión de identidades y accesos, destaca que las organizaciones modernas administran ecosistemas completos de identidades distribuidas entre usuarios, aplicaciones y cargas de trabajo. Esta expansión incrementa la complejidad operativa y la superficie de ataque.

¿Qué son las identidades no humanas?

Son credenciales digitales asignadas a máquinas, aplicaciones y procesos automatizados que suelen operar de forma autónoma y permanente. Utilizan certificados, claves API, tokens y secretos criptográficos en lugar de contraseñas, biometría o autenticación multi-factor(MFA) basada en dispositivos móviles para autenticarse e interactuar con otros sistemas.

¿Dónde se utilizan?

Principalmente en cargas de trabajo automatizadas en la nube (roles que permiten acceso seguro entre servicios), pipelines CI/CD (DevOps) que automatizan despliegues, comunicación entre microservicios mediante OAuth y certificados, integraciones SaaS basadas en APIs, dispositivos IoT conectados, plataformas de analítica avanzada y agentes de inteligencia artificial que consumen y procesan datos automáticamente. En todos estos casos de uso se requieren credenciales para operar, convirtiéndose en un nuevo elemento de riesgo para la ciberseguridad.

El riesgo invisible y en expansión

Cada cuenta de servicio, token o certificado representa un posible punto de entrada a la organización. Como las identidades no humanas suelen operar de forma autónoma, con privilegios elevados y escasa supervisión, cuando una identidad privilegiada es comprometida, los atacantes pueden acceder a datos sensibles, escalar privilegios y desplazarse lateralmente dentro del entorno tecnológico de la organización.

Cinco factores de riesgo críticos

- Exceso de privilegios
- Credenciales estáticas de larga duración
- Falta de inventario y visibilidad limitada sobre las identidades existentes
- Gestión deficiente de secretos
- Monitoreo insuficiente de comportamientos automatizados

La inteligencia artificial acelera el desafío

La IA agéntica incorpora nuevas identidades autónomas capaces de consumir APIs, consultar datos y ejecutar acciones. Cada agente requiere autenticación, autorización y monitoreo continuo.

Hacia una estrategia de NHIM

La Gestión de Identidades No Humanas (NHIM, por sus siglas en inglés) permite descubrir, inventariar, gobernar, proteger y supervisar estas identidades durante todo su ciclo de vida. Las capacidades clave incluyen descubrimiento automático, mínimo privilegio, rotación de secretos, monitoreo continuo, detección de anomalías y gobierno unificado.

Recomendaciones para CISOs

Implementar el descubrimiento automático de identidades no humanas, aplicar estrictamente el principio del mínimo privilegio, revisar privilegios periódicamente, adoptar modelos de Zero Trust, automatizar la gestión de secretos, monitorear los comportamientos anómalos y unificar la gestión de identidades humanas y no humanas, asignando siempre propietarios para cada identidad no humana.

Conclusión

Las identidades no humanas ya no son un asunto exclusivamente técnico. Son un componente estratégico de la ciber resiliencia moderna, por lo que las organizaciones que las gobiernen adecuadamente estarán mejor posicionadas para reducir los riesgos derivados de la nube, la automatización, la transformación digital y la inteligencia artificial y fortalecer su postura de ciberseguridad para proteger sus activos digitales más críticos.

César Vega Calderón
Cybersecurity Manager

La seguridad sin perímetro: el auge de la identidad como eje de protección

Tendencias por Whendy Oré Crisostomo

El modelo tradicional de ciberseguridad basado en el perímetro ha quedado atrás. En entornos cloud, distribuidos y altamente dinámicos, la identidad se consolida como el nuevo eje de control. Este cambio no solo impacta a los usuarios, sino también a sistemas, aplicaciones y procesos automatizados. Hoy, proteger significa validar continuamente quién —o qué— accede a los recursos, incluso en escenarios tan cotidianos como conectarse desde casa, usar una aplicación corporativa o automatizar procesos entre sistemas.

La identidad como eje de control

La seguridad ya no depende de estar "dentro" o "fuera" de la red. Cada acceso debe evaluarse considerando identidad, dispositivo, contexto y nivel de riesgo. Este enfoque, alineado con Zero Trust, elimina la confianza implícita y exige verificación constante. En este nuevo modelo, la identidad se convierte en el verdadero punto de defensa. Gestionarla de forma precisa y dinámica es ahora la base de cualquier estrategia de seguridad moderna.

El crecimiento de las identidades de máquina

Más allá de los usuarios, el ecosistema digital está dominado por interacciones entre sistemas. APIs, microservicios, contenedores y automatizaciones utilizan **identidades de máquina** para autenticarse. Estas identidades —certificados, tokens o claves— permiten que aplicaciones, servicios y procesos automatizados se comuniquen entre sí sin intervención humana, por ejemplo, cuando una aplicación consulta datos de otra o ejecuta tareas programadas. Sin embargo, crecen de forma exponencial y muchas veces carecen de visibilidad y control, lo que las convierte en un punto crítico de riesgo dentro de las organizaciones.

Machine Identity Management: control y visibilidad

Para mitigar estos riesgos, las organizaciones necesitan saber exactamente qué identidades existen, dónde se usan y por cuánto tiempo. Aquí es donde la gestión de identidades de máquina (Machine Identity Management) cobra relevancia. Su objetivo es establecer control integral mediante:

- Inventario y descubrimiento continuo
- Automatización de credenciales
- Aplicación de mínimo privilegio
- Monitoreo constante
- Una estrategia madura de MIM permite reducir la superficie de ataque y fortalecer la resiliencia organizacional.

Una estrategia madura de MIM permite reducir la superficie de ataque y fortalecer la resiliencia organizacional.

¿Por qué importa ahora?

Este cambio hacia una seguridad centrada en la identidad no es casual. Responde a la evolución natural de los entornos digitales, donde los usuarios ya no trabajan desde una única ubicación y las aplicaciones ya no residen en un solo lugar. Hoy es común que una organización utilice múltiples nubes, aplicaciones externas y dispositivos personales, lo que incrementa los puntos de acceso y reduce el control tradicional. En este contexto, confiar únicamente en la red ya no es suficiente.

Además, los atacantes han adaptado sus estrategias y buscan comprometer credenciales en lugar de vulnerar infraestructuras. Esto hace que proteger la identidad —humana y de máquina— sea el factor decisivo para prevenir accesos indebidos. No abordar este desafío puede traducirse en accesos no autorizados difíciles de detectar, exposición de datos críticos y un aumento significativo del riesgo operativo. Este cambio refleja una tendencia clara: el paso de un modelo de seguridad basado en infraestructura a uno centrado en la gestión de identidades.

Agentes de identidad (ID Agents): seguridad en el punto de ejecución

En entornos distribuidos, los **ID Agents** llevan la seguridad directamente a donde ocurre la ejecución. Estos componentes permiten:

- Validar accesos de forma local
- Proteger credenciales sin exposición
- Aplicar políticas en tiempo real
- Generar telemetría de seguridad
- Su implementación refuerza el concepto de identidad como perímetro, integrando la seguridad en cada capa del entorno digital.
- En entornos modernos, estos agentes permiten que la seguridad no dependa de un único punto central, sino que acompañe a cada sistema y aplicación donde se ejecuta.

Del control a la confianza dinámica

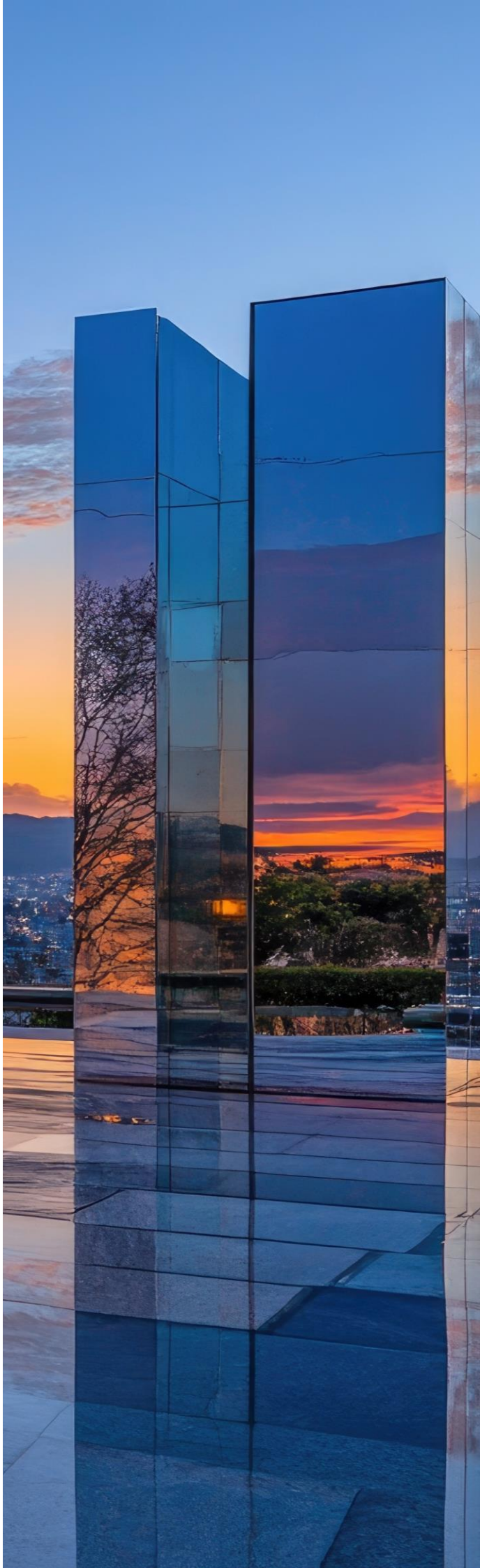
Más que una evolución tecnológica, este cambio representa una transformación en la forma en que las organizaciones entienden la confianza. Ya no se trata de asumir que todo lo interno es seguro, sino de validar continuamente cada identidad, cada acceso y cada interacción.

Este enfoque no solo mejora la seguridad, sino que permite a las organizaciones operar con mayor flexibilidad en entornos cada vez más distribuidos.

Conclusión

El perímetro tradicional ha desaparecido. En su lugar, la identidad se posiciona como el núcleo de la ciberseguridad. Entender este cambio deja de ser un tema exclusivamente técnico para convertirse en una necesidad operativa en cualquier organización. Esta evolución no es temporal, sino una transformación estructural en la forma en que las organizaciones entienden la seguridad.

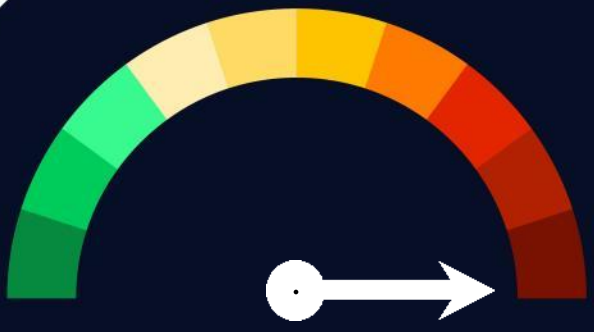
Whendy Oré Crisostomo
Cybersecurity Analyst



Vulnerabilidades

OneUptime Sandbox Escape

Fecha: 27 de mayo de 2026
CVE: CVE-2026-45102



CVSS: 9.9

CRÍTICA

Descripción

CVE-2026-45102 es una vulnerabilidad crítica de ejecución remota de código (RCE) en OneUptime. El problema se debe al uso inseguro del módulo "*vm*" de Node.js como mecanismo de aislamiento.

Un atacante autenticado con pocos privilegios puede explotar esta falla para ejecutar código arbitrario en el servidor, acceder a información sensible y comprometer la aplicación. Debido a su alto impacto, la vulnerabilidad tiene una puntuación CVSS de 9,9.

Solución

- Actualizar a OneUptime 10.0.98 o superior, versión en la que el problema ha sido corregido.

Productos afectados

- OneUptime anteriores a la versión 10,0,98.

Referencias

- nvd.nist.gov
- github.com

Vulnerabilidades

WordPress WP Maps Pro

Fecha: 29 de mayo de 2026
CVE: CVE-2026-8732

CVSS: 9.8

CRÍTICA

Descripción

El complemento de WordPress, WP Maps Pro, un plugin para crear mapas interactivos basado en Google Maps, es vulnerable a la escalada de privilegios mediante la creación de una cuenta de administrador.

Cuando el atacante visita una página pública, extrae un *nonce:* un ticket temporal de acceso, expuesto dentro del código JavaScript. Posteriormente, envía una petición AJAX en segundo plano con el *nonce* oculto en la petición.

El sistema no comprueba si el usuario es administrador, solo si el *nonce* es correcto, lo que le da al atacante el rol de administrador.

Solución

Se recomienda:

- Revisar/Desinstalar los *plugins* instalados recientemente sin autorización.
- Actualizar el plugin a la versión 6.1.1 o superior

Productos afectados

Algunos de los productos afectados son:

- Versiones de WP Maps Pro anteriores a la 6.1.0

Referencias

- thehackernews.com
- wordfence.com
- incibe.es

Parches

Android corrige una vulnerabilidad de escalada de privilegios explotada activamente.

Fecha: 2 de junio de 2026
CVE: CVE-2025-48595

Alta

Descripción

Google ha corregido la vulnerabilidad CVE-2025-48595, identificada en el componente Framework de Android. La falla corresponde a un desbordamiento de enteros (Integer Overflow - CWE-190) que puede derivar en una elevación local de privilegios y permitir la ejecución de código con permisos superiores a los previstos.

La explotación de esta vulnerabilidad no requiere privilegios elevados previos y puede comprometer la seguridad del dispositivo afectado. Google indicó que existían evidencias de explotación limitada y dirigida antes de la publicación de la actualización de seguridad.

La vulnerabilidad afecta a múltiples versiones de Android y forma parte del boletín de seguridad de junio de 2026.

Productos afectados

- Android 14
- Android 15
- Android 16
- Android Framework
- Dispositivos Android que no dispongan del nivel de parche de seguridad 2026-06-05 o superior

Solución

- Actualizar los dispositivos al nivel de parche de seguridad 2026-06-05 o posterior.

Referencias

- android.com
- nist.gov
- cisa.gov

Cisco parchea vulnerabilidades en Unified CM

Fecha: 04 de junio de 2026
CVE: CVE-2026-20230

Alta

Descripción

La vulnerabilidad CVE-2026-20230 en Cisco Unified Communications Manager (Unified CM) podía permitir que un atacante remoto no autenticado realizase ataques de falsificación de solicitudes del lado del servidor a través de un dispositivo.

Esta vulnerabilidad se debe a una validación incorrecta del servidor SSRF sobre ciertas peticiones HTTP.

Un atacante podría explotarla enviando una solicitud HTTP manipulada a un dispositivo afectado. Esto permitía al atacante escribir archivos en el sistema operativo subyacente, los cuales podrían usarse posteriormente para obtener privilegios de administrador.

Productos afectados

Los productos afectados son:

- Cisco Unified CM hasta la versión 14 y Unified CM SME hasta la versión 15 si tienen habilitado el servicio WebDialer.

Solución

Se recomienda:

- Deshabilitar el servicio WebDialer, por parte de los administradores.
- Instalar el parche de seguridad más reciente.

Referencias

- thehackernews.com
- sec.cloudapps.cisco.com
- incibe.es

Eventos

GITEX AI Europe 2026
30 de junio – 1 de julio

GITEX AI EUROPE 2026 se celebrará del 30 de junio al 1 de julio en Berlín, Alemania, como un espacio dedicado a analizar el papel de la inteligencia artificial en la transformación digital de Europa. El evento reunirá a empresas tecnológicas, organizaciones públicas, centros de investigación y líderes de la industria para compartir experiencias sobre la adopción de IA, los desafíos regulatorios y las oportunidades de innovación que esta tecnología está generando en distintos sectores. La agenda incluirá conferencias, demostraciones y debates sobre el desarrollo de soluciones basadas en IA, así como su impacto en ámbitos como la ciberseguridad, la productividad empresarial y la competitividad digital.

Enlace

RAISE Summit 2026
7 de julio – 9 de julio

RAISE Summit 2026 se celebrará del 7 al 9 de julio en París, Francia, reuniendo a miles de líderes empresariales, inversores, emprendedores y responsables tecnológicos para debatir el futuro de la inteligencia artificial. El evento contará con la participación de más de 2.000 compañías y cientos de ponentes de referencia del ecosistema tecnológico global, incluyendo representantes de organizaciones como Google, OpenAI, Anthropic, Meta y AWS. A lo largo de la agenda se analizarán los retos asociados a la adopción empresarial de la IA, desde la infraestructura y la gobernanza hasta la generación de valor de negocio, convirtiéndose en un espacio clave para conocer las estrategias que están definiendo la próxima generación de innovación digital.

Enlace

Gartner Security & Risk Management Summit
22 de julio – 24 de julio

Gartner Security & Risk Management Summit se celebrará del 22 al 24 de julio en Tokio y reunirá a CISOs, responsables de riesgo y líderes de ciberseguridad para analizar los desafíos que están redefiniendo la función de seguridad en las organizaciones. La agenda se estructurará en seis tracks especializados: liderazgo e innovación en ciberseguridad, gestión del riesgo y resiliencia, seguridad de infraestructuras y nube, seguridad de aplicaciones y datos, operaciones y respuesta ante incidentes, y el programa exclusivo CISO Circle para ejecutivos. A través de estos espacios, los asistentes podrán conocer las principales tendencias en inteligencia artificial, resiliencia cibernética, protección de datos, seguridad cloud y alineación de las estrategias de seguridad con los objetivos de negocio.

Enlace

Recursos

➢ ENISA NIS360

Publicado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el informe *NIS360 2026* ofrece una evaluación integral del nivel de madurez y criticidad en ciberseguridad de los sectores considerados esenciales bajo la Directiva NIS2. El estudio analiza el grado de preparación de sectores clave como energía, transporte, finanzas, salud, infraestructura digital, administraciones públicas, identificando fortalezas, brechas y áreas prioritarias de mejora. Además, proporciona una visión comparativa de cómo evoluciona la resiliencia cibernética en Europa y destaca aquellos sectores donde la importancia estratégica supera el nivel actual de madurez en seguridad, convirtiéndose en una referencia clave para responsables de ciberseguridad, reguladores y operadores de infraestructuras críticas.

Enlace

➢ NIST IR 8374r1: Ransomware Risk Management – A Cybersecurity Framework 2.0 Community Profile

Publicado por el National Institute of Standards and Technology (NIST), este documento ofrece una guía práctica para ayudar a las organizaciones a gestionar el riesgo asociado al ransomware utilizando el marco NIST Cybersecurity Framework (CSF) 2.0. El perfil identifica los objetivos de seguridad más relevantes para gobernar, prevenir, detectar, responder y recuperarse de incidentes de ransomware, proporcionando una referencia estructurada para evaluar el nivel de preparación de una organización frente a este tipo de amenazas. Además, el documento facilita la identificación de brechas de seguridad y la definición de estrategias de resiliencia que permitan reducir el impacto operativo y financiero de un ataque.

Enlace

NTT DATA

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com