Número 117 | Agosto 2026

NTT DATA

Radar

El magazine de ciberseguridad

Lo que ciframos hoy, lo descifran mañana

Por Lluis Quiles Ardila

Cada cierto tiempo reaparece el mismo titular: la computación cuántica está a punto de romper cualquier código de seguridad digital. La afirmación corre rápido y deja flotando una pregunta incómoda: ¿estamos creando una tecnología que destruirá nuestra seguridad? Los ordenadores cuánticos más avanzados operan hoy con poco más de un centenar de qubits físicos: ruidosos, inestables, cargados de error. Romper una clave RSA de las que usamos habitualmente exigiría miles de qubits lógicos estables, con corrección de errores muy eficiente. Ese nivel de madurez no se ha alcanzado. Las previsiones más optimistas lo sitúan alrededor de 2035.

El riesgo no es futuro. Es retroactivo. La lógica del harvest now, decrypt later consiste en interceptar y almacenar hoy tráfico cifrado para descifrarlo mañana. Significa que toda la información cuya vida útil supere la próxima década ya está expuesta, desde la historia clínica hasta el secreto industrial. Las organizaciones van a tener que migrar a la criptografía post-cuántica antes de que la amenaza se materialice.

Y esa criptografía no es una promesa. Es un estándar. ML-KEM y ML-DSA se están convirtiendo en norma internacional, con despliegues híbridos en VPN, TLS y certificados. Estados Unidos ha fijado su consolidación federal para 2035. Europa apunta a las infraestructuras críticas antes del final de la década. La industria también se ha movido. NTT Research ha presentado una suite de seguridad Zero Trust adaptada a entornos post-cuánticos, y ha desarrollado el primer sistema de transporte post-cuántico capaz de cambiar de método criptográfico sin interrumpir las comunicaciones.

Ahora bien, reducir lo cuántico a la criptografía sería quedarse con una sola cara del problema. Por eso en NTT DATA hemos construido una oferta de valor que cubre los cuatro dominios de las tecnologías cuánticas. La computación, con optimización, simulación y aprendizaje automático. La sensórica y la metrología. Las comunicaciones cuánticas, con QKD. Y la criptografía post-cuántica, desde el descubrimiento de activos hasta la migración.

En seguridad hay que pensar además en que estos algoritmos protegerán también a los malos. El cifrado resistente a lo cuántico es de doble uso y blindará por igual comunicaciones legítimas, redes criminales y mercados ilícitos.

El Foro Económico Mundial, con sus Quantum Computing Governance Principles, y la UNESCO, a través del COMEST, ya trabajan sobre principios como la transparencia, la rendición de cuentas y la prevención de usos maliciosos.

Estamos además en plena convergencia entre IA y cuántica. Cada modelo entrenado con datos sensibles amplía la superficie de lo que hay que proteger. Cada agente que opera de forma autónoma sobre sistemas corporativos, también. La confianza digital pasa a ser un problema de ciclo de vida del dato.

En esta edición de Radar hemos querido abordar lo que ya es una realidad: la criptografía post-cuántica, el gobierno de claves y la protección del dato. Y también las tendencias que están redefiniendo el ecosistema cuántico y las capacidades que conviene empezar a construir hoy. El reto es doble y urgente: prepararse y experimentar.

Hay que migrar antes de que la amenaza se materialice y, al mismo tiempo, desarrollar aplicaciones cuánticas con impacto real. Los ejemplos ya existen: NTT DOCOMO reorganizó las estaciones base de su red móvil en cuarenta segundos, frente a las veintisiete horas que requerían los métodos clásicos.

Desde NTT DATA también hemos ayudado a optimizar la gestión logística de un cliente y a mejorar el modelo de mantenimiento predictivo de otro. Nuevos fármacos, materiales más eficientes y redes con menor consumo energético completan la otra mitad de la historia, que también empieza hoy.

Lluis Quiles Ardila
Managing Director

Ransomware, terceros y parches pendientes: la cadena invisible del riesgo

Cibercrónica Marta Gonzalez Martino

Entre junio y los primeros días de julio, varios incidentes relevantes confirmaron una tendencia que atraviesa sectores y países: la exposición ya no depende únicamente de los sistemas propios de cada organización. La dependencia de terceros, el uso de infraestructuras compartidas, la falta de aplicación de parches, el abuso de credenciales y la automatización de fases del ataque ampliaron el impacto de brechas que, en muchos casos, comenzaron por un único punto vulnerable.

El segundo mayor productor de azúcar de Australia, Mackay Sugar, despertó el 10 de junio con sus sistemas paralizados. La empresa admitió haber sufrido un ciberataque que afectó a dos de sus tres ingenios principales y tuvo que activar procesos manuales para procesar la caña ya cosechada. El 15 de ese mes, el grupo The Gentlemen, identificado por Microsoft como Storm-2697, se adjudicó el ataque. El actor opera bajo un modelo RaaS heredado en parte de LockBit y utiliza un cifrador desarrollado en Go con capacidad de movimiento lateral tipo worm, además de técnicas de evasión frente a EDR mediante el framework GentleKiller. Mackay Sugar mostró que la frontera entre IT y OT es cada vez más porosa.

Casi al mismo tiempo, Google Threat Intelligence y Mandiant hicieron pública una campaña contra Oracle PeopleSoft atribuida a ShinyHunters. Entre el 27 de mayo y el 9 de junio, antes de que Oracle publicara su aviso de seguridad del día 10, los atacantes explotaron una vulnerabilidad Zero-day en PeopleSoft, software usado para gestionar funciones críticas como RR. HH., finanzas y cadena de suministro. Según Google, los atacantes desplegaron agentes MeshCentral disfrazados como endpoints legítimos en la nube para ejecutar comandos administrativos.

El 22 de junio, Tata Electronics confirmó un incidente de ciberseguridad en algunos de sus sistemas corporativos después de que World Leaks publicara en la dark web más de 200.000 archivos, con un volumen superior a 630 GB. Reuters informó de que entre los documentos había supuestos diseños, especificaciones, documentos de fabricación, correos, logs y copias de pasaportes, además de material relacionado con clientes como Apple y Tesla. La novedad posterior agravó el caso: la filtración incluía listas de componentes y proveedores, además de material sobre pruebas del iPhone 18 Pro, modelo aún no comercializado.

Tras el incidente, la compañía endureció controles internos, restringió accesos remotos a herramientas sensibles, contrató una auditoría forense y notificó a autoridades y clientes.

El 23 de junio, el foco se desplazó a Japón. KDDI Corporation, una de las grandes compañías de telecomunicaciones del país, confirmó que había detectado acceso no autorizado a un sistema de correo que prestaba servicio a seis ISP, entre ellos STNet, KDDI Web Communications, JCOM, Chubu Telecommunications, Nifty y BIGLOBE. El acceso se detectó el 17 de junio y, según KDDI, se produjo por la explotación de una vulnerabilidad en software de terceros integrado en ese sistema común. La posible exposición alcanzaba hasta 14,22 millones de direcciones de correo y contraseñas, incluyendo cuentas activas, antiguas e inactivas. KDDI aseguró que su sistema de correo móvil no se vio afectado, pero el incidente dejó una lectura clara: el efecto dominó. Una vulnerabilidad en una infraestructura compartida puede convertirse en un punto único de fallo para varios proveedores a la vez.

Desde finales de junio, el foco se desplazó hacia una zona más incómoda: credenciales, parches pendientes y automatización del ataque. BlueHammer, una vulnerabilidad de Windows Defender marcada por CISA como explotada activamente en campañas de malware y ransomware, ya había sido parcheada por Microsoft en abril. El fallo permitía escalar privilegios hasta SYSTEM mediante una condición de carrera.

A comienzos de julio apareció JadePuffer, un caso especialmente relevante para entender la automatización del ataque. Sysdig Threat Research Team lo describió como el primer caso conocido de ransomware agentic: una operación de extorsión automatizada mediante un agente basado en un modelo de lenguaje. El acceso inicial se produjo mediante la explotación de CVE-2025-3248, una vulnerabilidad crítica en Langflow que permite ejecutar código arbitrario sin autenticación en instancias expuestas.

A partir de ahí, el agente automatizó reconocimiento, búsqueda de credenciales, extracción de datos y movimiento lateral hacia servicios internos. Según Sysdig, el ataque acabó afectando a una plataforma Nacos, donde se cifraron más de 1.300 elementos de configuración y se dejó una demanda de rescate.

El 1 de julio, España apareció en la secuencia con Indra, que confirmó la detección de ransomware en una de sus filiales. Su CSIRT activó protocolos de análisis, contención, erradicación y recuperación. Según la compañía, el incidente quedó limitado a un entorno no crítico, no se propagó al resto del grupo y no interrumpió la prestación de servicios. El ataque fue reivindicado por The Gentlemen, que incluyó a Indra en su sitio de filtraciones con una cuenta atrás antes de publicar supuestos datos robados, aunque la exfiltración y el tipo de información comprometida no estaban confirmados públicamente.

El 5 y 6 de julio apareció otro caso distinto, pero con el mismo fondo: FortiBleed. Según la información publicada por The Times y The Sun, atacantes vinculados a Rusia habrían utilizado vulnerabilidades en firewalls Fortinet, combinadas con fuerza bruta y credenciales previamente filtradas, para acceder a cuentas de organismos públicos británicos. Entre las víctimas mencionadas aparecen personal del Foreign Office, trabajadores de administraciones locales y personal técnico de embajadas británicas en Tailandia y Mauricio. El NCSC confirmó una campaña de fuerza bruta y pidió a las organizaciones revisar credenciales y configuraciones.

En conjunto, estos incidentes dejan una conclusión clara: la superficie de ataque ya no termina en los sistemas internos de una organización. Se extiende hacia proveedores, plataformas compartidas, integraciones SaaS, credenciales reutilizadas, firewalls expuestos, parches pendientes y herramientas que, si no se controlan, pueden convertirse en el primer eslabón de una intrusión mayor.

Mackay Sugar mostró cómo un ataque digital puede afectar a una operación física; KDDI evidenció el riesgo de las infraestructuras compartidas; PeopleSoft y Tata Electronics confirmaron el peso de la cadena de suministro; BlueHammer y FortiBleed recordaron que lo conocido y no corregido sigue siendo explotable; JadePuffer añadió la automatización del ataque como nueva capa de presión; e Indra mostró que incluso un incidente contenido puede ser relevante cuando la víctima forma parte de sectores estratégicos.

Marta González Martino
Cybersecurity Consultant

Seguridad postcuántica: la era de la criptoagilidad y la criptoresiliencia

Artículo por Kim Boermans

La computación cuántica está dejando atrás los laboratorios de investigación y empieza a consolidarse como una fuerza estratégica con impacto real, incluida la transformación del panorama de la ciberseguridad, especialmente por su capacidad potencial para desafiar los fundamentos criptográficos que sustentan la economía digital.

El modelo de cifrado actual se basa en la premisa de que determinados problemas matemáticos son prácticamente imposibles de resolver con las capacidades de computación disponibles hoy en día. Esta premisa se está viendo erosionada por la computación cuántica, que podría dejar obsoletos algoritmos ampliamente utilizados como RSA y ECC, reduciendo drásticamente el tiempo necesario para romperlos. El desafío ya está aquí. El concepto de "capturar ahora, descifrar después" plantea que los datos capturados hoy podrían verse comprometidos una vez que la tecnología cuántica alcance la madurez.

Las organizaciones deben actuar de forma temprana para obtener una visibilidad completa sobre dónde y cómo se implementa la criptografía en sus ecosistemas digitales. Esto incluye evaluar sistemas heredados, arquitecturas distribuidas y datos que, debido a requisitos regulatorios, deben permanecer seguros durante años o incluso décadas.

Hacia una hoja de ruta de seguridad cuántica

La transición hacia la seguridad postcuántica requiere una estrategia sostenida que combine tecnología, procesos y capacidades organizativas. No existe un "interruptor" ni una solución mágica capaz de resolver el problema de forma inmediata.

A lo largo de este camino, deben desarrollarse dos capacidades clave. La primera es la criptoagilidad: la capacidad de adaptarse dinámicamente a nuevos estándares sin interrumpir las operaciones del negocio y de priorizar las acciones de manera eficaz.

Los primeros pasos esenciales incluyen identificar los activos criptográficos, mapear dependencias y comprender qué datos están en riesgo. A partir de ahí, las organizaciones pueden diseñar una hoja de ruta que facilite la transición hacia algoritmos resistentes a la computación cuántica, junto con modelos de gestión más eficientes y escalables.

La segunda capacidad es la criptoresiliencia: la capacidad de responder rápidamente ante vulnerabilidades emergentes, mantener el cumplimiento regulatorio y preservar la confianza en un entorno en constante evolución.

Convergencia con tecnologías emergentes

La convergencia con otras tecnologías emergentes, como la inteligencia artificial, los gemelos digitales y blockchain, amplifica tanto las oportunidades como las exigencias de seguridad. Los datos utilizados para entrenar modelos, optimizar operaciones o simular escenarios deben permanecer protegidos, incluso durante su procesamiento, elevando así el estándar de protección requerido.

Como resultado, están surgiendo enfoques más integrales que combinan asesoramiento estratégico, experimentación aplicada y modelos de implementación por fases. Evaluar tecnologías, desarrollar prototipos y validar casos de uso específicos ayuda a reducir la incertidumbre y acelerar la adopción con menor riesgo.

Al mismo tiempo, la evolución hacia modelos de criptografía como servicio está transformando las dinámicas operativas: centralizando capacidades, automatizando la gestión de claves y adaptando continuamente los algoritmos sin interrumpir las operaciones del negocio.

Este enfoque refuerza la seguridad, simplifica las operaciones, reduce costes y permite respuestas más ágiles. La computación cuántica abre la puerta a nuevos niveles de optimización y eficiencia en múltiples industrias. Sin embargo, capturar este valor requiere construir hoy una base sólida de confianza digital. El proceso comienza con una pregunta sencilla: ¿qué algoritmos criptográficos protegen nuestros datos más valiosos y cuál es su nivel de exposición en un futuro cuántico?

Kim Boermans
Head of Cybersecurity NTT DATA Benelux & France

Siete tendencias que están redefiniendo el ecosistema de las ciencias y tecnologías cuánticas

Tendencias por María Gutierrez

Durante años, el debate sobre las tecnologías cuánticas se ha centrado casi exclusivamente en la computación cuántica. Sin embargo, el verdadero cambio es mucho más amplio. La denominada segunda revolución cuántica está impulsando un ecosistema que integra computación, comunicaciones, criptografía, algoritmia, sensórica y metrología, con implicaciones estratégicas para la industria, la seguridad y la competitividad. Estas son las principales tendencias, que pensamos, marcarán su evolución en los próximos años:

1. Del número de qubits al rendimiento útil. El sector ha dejado atrás la carrera por incrementar el número de qubits como principal indicador de progreso. La atención se dirige ahora a métricas como la fiabilidad de las operaciones, la corrección de errores, la escalabilidad de las arquitecturas y la capacidad de ejecutar algoritmos con valor práctico, en paralelo, el sector está evolucionando hacia la denominada era NISQ (Noisy Intermediate-Scale Quantum), caracterizada por dispositivos con un número limitado de qubits y todavía susceptibles al ruido. El reto ya no es construir procesadores más grandes, sino sistemas fiables y utilizables.

2. La sensórica cuántica emerge como la primera gran aplicación comercial. Mientras la computación cuántica continúa madurando, los sensores cuánticos se perfilan como la tecnología con mayor impacto a corto plazo. Su extraordinaria sensibilidad permitirá mejorar la navegación sin dependencia del GPS, la monitorización de infraestructuras críticas, la exploración geológica, el diagnóstico biomédico y la observación de la Tierra con una precisión sin precedentes.

3. La metrología será un habilitador silencioso de la economía digital. Los avances en relojes atómicos ópticos e interferometría cuántica están redefiniendo los estándares de medida y sincronización. Esta capacidad resulta esencial para redes eléctricas inteligentes, telecomunicaciones avanzadas, sistemas financieros, navegación de precisión y futuras infraestructuras 6G, donde la exactitud temporal será un activo estratégico.

4. Las comunicaciones cuánticas avanzan hacia infraestructuras seguras. La distribución cuántica de claves (QKD), las redes cuánticas metropolitanas y los primeros experimentos con repetidores cuánticos están sentando las bases de una futura Internet cuántica. Aunque todavía existen importantes desafíos tecnológicos, numerosos países consideran ya estas capacidades como infraestructuras críticas para proteger comunicaciones gubernamentales, financieras y de defensa. Y desde luego es una de las grandes apuestas de Europa para estos próximos años.

5. La criptografía postcuántica pasa de la investigación a la planificación. La estandarización de nuevos algoritmos resistentes a ataques cuánticos marca el inicio de una transición que afectará a todas las organizaciones. El desafío no es únicamente tecnológico, sino también organizativo: identificar activos críticos, planificar la migración y garantizar la protección de información cuyo ciclo de vida se extienda durante décadas. Este punto es uno de los mas inminentes, de echo podríamos decir que deja de ser “tendencia” para empezar a ser ya “moda”.

5. La inteligencia artificial acelera el desarrollo cuántico. La convergencia entre IA y tecnologías cuánticas constituye una de las tendencias más prometedoras. La inteligencia artificial ya optimiza el diseño de materiales, el control experimental de dispositivos cuánticos y la calibración de sensores, mientras que, a medio plazo, la computación cuántica podría potenciar determinados algoritmos de optimización y aprendizaje automático.

6. La ventaja competitiva dependerá del ecosistema, no solo de la tecnología. La competencia internacional ya no se limita al desarrollo de hardware. Europa, Estados Unidos y China están desplegando estrategias que combinan inversión pública, colaboración industrial, formación de talento, normalización e infraestructuras de investigación. Para las empresas, el reto consiste en identificar casos de uso, desarrollar capacidades internas y participar en estos ecosistemas antes de que la tecnología alcance su plena madurez.

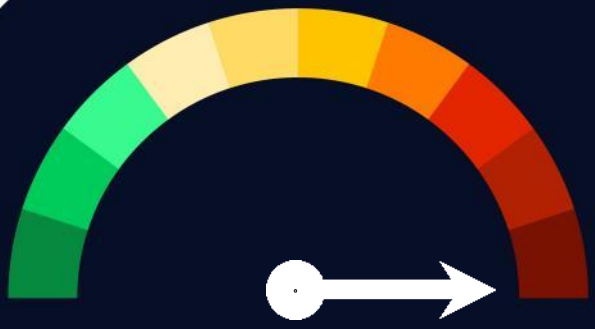
La ciencia y las tecnologías cuánticas han dejado de ser una promesa lejana para convertirse en un elemento estratégico de las políticas industriales y de innovación. Su adopción será gradual y desigual, pero las organizaciones que comiencen hoy a desarrollar conocimiento, alianzas y capacidades estarán mejor posicionadas para capturar el valor de una revolución tecnológica que ya ha comenzado.

María Gutierrez
Cybersecurity Expert

Vulnerabilidades

Google Chrome Sandbox Escape

Fecha: 30 de junio de 2026
CVE: CVE-2026-13782



CVSS: 10

CRÍTICA

Descripción

CVE-2026-13782 es una vulnerabilidad crítica causada por un error de tipo *Use-After-Free* (CWE-416) en el navegador de Chrome, mediante el cual se reutiliza o hace referencia a memoria después de que esta haya sido liberada.

En este contexto, un atacante que haya comprometido previamente el proceso de renderizado puede aprovechar este error para escapar de la *sandbox* de Chrome mediante una página HTML especialmente diseñada.

Este tipo de vulnerabilidad es especialmente crítica, ya que el *sandbox* constituye una de las principales barreras de seguridad del navegador, motivo por el cual tiene una puntuación CVSS de 10.

Solución

Se recomienda:

- Actualizar a Chrome 150.0.7871.47 o posterior.
- Mantener activadas las actualizaciones automáticas.

Productos afectados

- Google Chrome de Windows, Linux o macOS anteriores a la versión 150.0.7871.47.

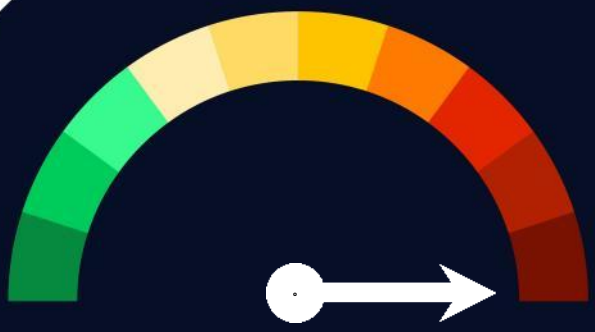
Referencias

- nvd.nist.gov
- rapid7.com
- incibe.es
- cvedetails.com

Vulnerabilidades

Adobe ColdFusion Path Traversal

Fecha: 30 de junio de 2026
CVE: CVE-2026-48282



CVSS: 10

CRÍTICA

Descripción

Adobe ColdFusion es afectado por una vulnerabilidad de *path traversal* en el componente *Remote Development Services* (RDS). Este problema permite que un atacante sin necesidad de ser autenticado manipule rutas de archivos enviadas al servidor mediante peticiones HTTP, de forma que pueda salir de los directorios permitidos y acceder a ubicaciones arbitrarias del sistema o guardar código CFML (*ColdFusion Markup Language*) malicioso en directorios accesibles por la aplicación web, obtenido una ejecución remota de código.

La causa raíz está en que ColdFusion no valida ni restringe, adecuadamente, la ruta de archivo, proporcionada por el usuario, en ciertas operaciones del servicio RDS.

Solución

Se recomienda:

- Actualizar las versiones a ColdFusion 2025 Update 10 y ColdFusion 2023 Update 21.

Productos afectados

- ColdFusion 2025 Update 9 y anteriores.
- ColdFusion 2023 Update 20 y anteriores.

Referencias

- adobe.com
- nvd.nist.gov
- sentinelone.com
- cvereports.com

Parche de seguridad de BMC para vulnerabilidad crítica de Control-M/Server

Fecha: 01 de julio de 2026
CVE: CVE-2026-10539

Crítica

Descripción

Debido a una validación insuficiente de comandos, la vulnerabilidad CVE-2026-10539 podría permitir que un atacante remoto no autenticado pudiese ejecutar comandos no autorizados en el servidor Control-M, facilitando un posible movimiento lateral dentro de la infraestructura.

Control-M es un planificador de cargas de trabajo (*workload automation*) desplegado en grandes empresas de telecomunicaciones, banca, seguros, administraciones públicas e industria. Por ello, el impacto potencial de esta vulnerabilidad es elevado, ya que podría comprometer un sistema que afecta a múltiples procesos de negocio y sistemas dependientes.

Productos afectados

Los productos afectados son:

- Control-M/Server desde la versión 9.0.20.x hasta la versión 9.0.21.200 incluida.

Solución

Se recomienda:

- Actualizar Control-M/Server a la versión 9.0.21.300 o posterior.
- Restringir el acceso a Control-M/Server únicamente a redes de confianza

Referencias

- incibe.es
- nvd.nist.gov
- bmcapps.my.site.com

 |

BeyondTrust corrige múltiples vulnerabilidades en Remote Support y Privileged Remote Access

Fecha: 6 de julio de 2026
CVE: CVE-2026-40138 y 3 más

Crítica

Descripción

BeyondTrust ha solucionado múltiples vulnerabilidades relacionadas con los programas *BeyondTrust Remote Support* (RS) y *Privileged Remote Access* (PRA), dos productos usados para acceso remoto, soporte remoto y gestión de accesos privilegiados.

Estas vulnerabilidades permiten a un atacante no autenticado eludir controles de acceso, obtener acceso no autorizado al sistema o provocar una denegación de servicio.

Además, una de las vulnerabilidades permitía a usuarios autenticados con privilegios limitados acceder a recursos o datos fuera de su alcance autorizado. El riesgo es especialmente relevante en entornos donde estas soluciones estén expuestas a red o Internet.

Productos afectados

Los productos afectados son:

- BeyondTrust Remote Support (RS) versión 25.3.2 o anteriores
- BeyondTrust Privileged Remote Access (PRA) versión 25.3.2 o anteriores

Solución

Se recomienda:

- Actualizar los programas a la versión 25.3.3.
- En entornos que no puedan actualizar inmediatamente, aplicar el *Security Rollup* de abril de 2026.

Referencias

- beyondtrust.com
- thehackernews.com
- nvd.nist.gov
- cybersecuritynews.com
- csirt.telconet.net

 |

Eventos

Black Hat USA 2026
1 de agosto - 6 de agosto

El evento de ciberseguridad más destacado del año regresa al Mandalay Bay con un programa rediseñado de seis días, concebido para impulsar la innovación, romper límites y reunir a la comunidad global de seguridad como nunca antes.

La edición de este año contará con cuatro días de formaciones inmersivas dirigidas por expertos, del 1 al 4 de agosto, seguidas del Summit Day el martes 4 de agosto, y de una conferencia principal de dos días con briefings innovadores, demostraciones de herramientas open source en Arsenal, un dinámico Business Hall y múltiples oportunidades de aprendizaje y networking.

Enlace

DEF CON 34
6 de agosto – 9 de agosto

DEF CON es la conferencia hacker más grande y con mayor trayectoria del mundo, conocida por su modelo de “villages”, en el que comunidades de interés organizan talleres prácticos y charlas. El Car Hacking Village de DEF CON es el principal punto de encuentro para investigadores de seguridad en automoción, con demostraciones en vivo de hacking de vehículos, competiciones CTF dirigidas a sistemas reales de automoción y ponencias sobre las vulnerabilidades más recientes en vehículos conectados.DEF CON es el lugar donde se revelan por primera vez muchos de los principales descubrimientos en seguridad del automóvil.

Enlace

SANS Security Awareness & Culture Summit 2026
19 de agosto – 28 de agosto

Es la 13ª edición de este encuentro, enfocado en profesionales de concienciación, comportamiento humano y cultura de ciberseguridad. El evento busca compartir conocimiento, experiencias y herramientas prácticas para impulsar cambios reales en la cultura de seguridad de las organizaciones.

El programa incluye charlas especializadas, casos de uso, sesiones prácticas y workshops presenciales, con foco en cómo influir no solo en los comportamientos, sino también en las actitudes y creencias de los empleados frente a la ciberseguridad. Además, ofrece espacios de networking con expertos y otros profesionales del sector.

Como complemento, SANS ofrece cursos asociados sobre liderazgo en ciberseguridad y gestión del riesgo humano, orientados a reforzar capacidades en programas de awareness, formación y cambio cultural. Es un evento especialmente relevante para organizaciones que quieren evolucionar desde campañas puntuales de concienciación hacia modelos más maduros de Human Risk Management

Enlace

Recursos

➢ Cyber Frontier 2026

Publicación anual de NTT DATA que reúne perspectivas de expertos, investigadores y profesionales de ciberseguridad. La edición 2026 aborda temas como la brecha de talento, la defensa frente a brechas, las amenazas de desinformación impulsadas por IA y la preparación ante la disrupción de la computación cuántica.

Enlace

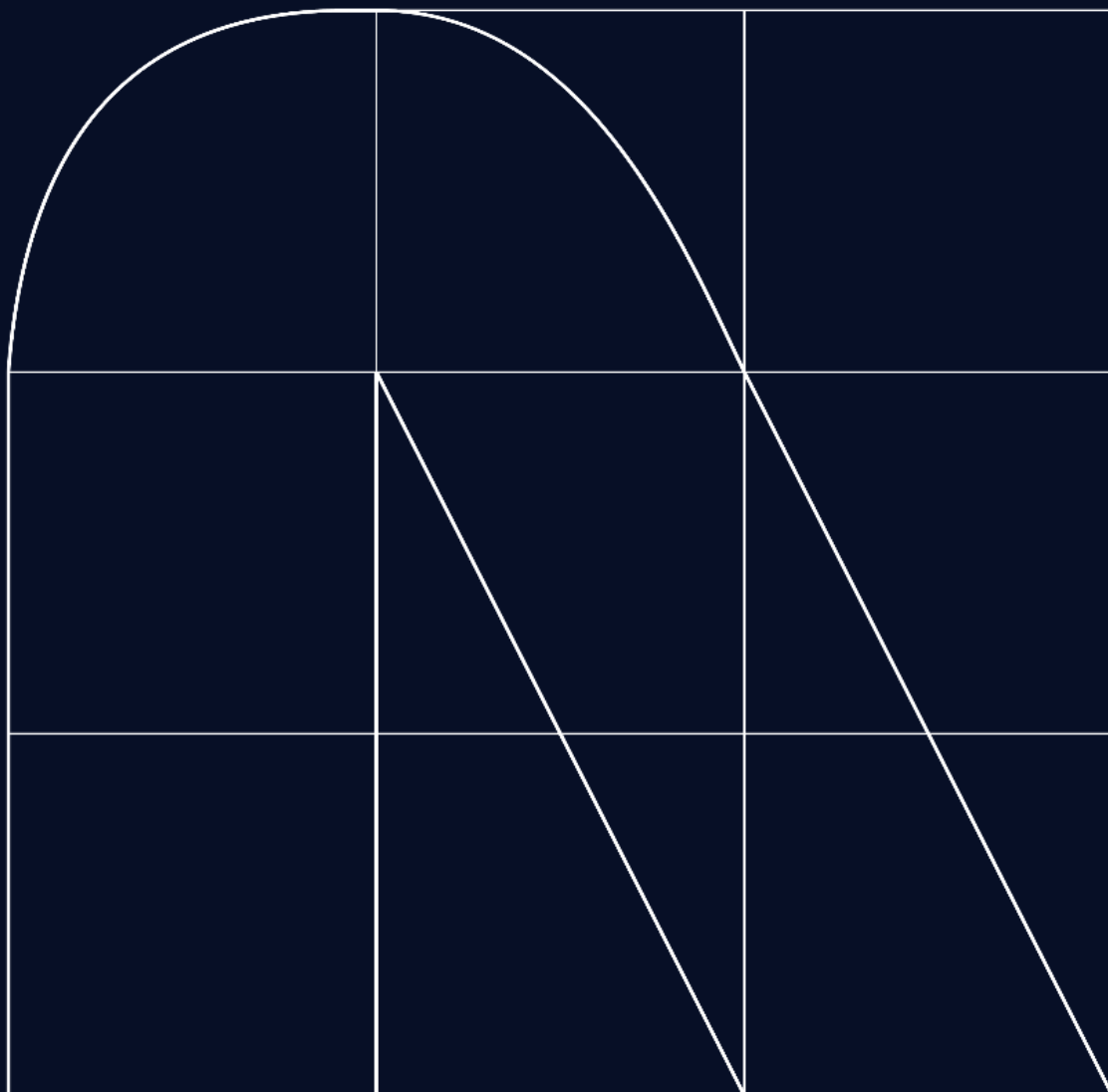
➢ Verizon 2026 Data Breach

Uno de los informes más reconocidos sobre brechas de seguridad e incidentes reales. La edición 2026 ofrece insights para responder a ataques potenciados por IA, presión financiera, ransomware, vulnerabilidades y riesgos por sectores. También incluye resumen ejecutivo, infografías y recursos por industria.

Enlace

NTT DATA

Suscríbete a RADAR
up.nttdata.com/suscribetearadar



Powered by the cybersecurity NTT DATA team

es.nttdata.com