Número 110 | Enero 2026

NTT DATA

Radar

El magazine de ciberseguridad

La ciberseguridad como habilitador del negocio

Por Maria Pilar Torres Bruna

¡Bienvenido 2026! Iniciamos un nuevo ciclo marcado por un panorama tecnológico tan apasionante como desafiante. Los negocios son cada vez más dependientes de la tecnología que los sustenta, y la rápida evolución de la inteligencia artificial, que pasó de ser predictiva a generativa y, ahora, a una **era agéntica**, está impulsando la creación de agentes digitales capaces de potenciar el trabajo humano.

La computación cuántica, de la que cada día se habla más, dejará de ser un concepto lejano para convertirse en una realidad en pocos años. Muchas organizaciones ya exploran nuevos modelos de negocio y oportunidades de eficiencia basados en esta tecnología, al tiempo que se preparan para las **nuevas ciberamenazas** que traerá consigo.

Quienes trabajamos en ciberseguridad compartimos el entusiasmo de todo el sector tecnológico ante estas transformaciones. Sin embargo, también entendemos que la ciberseguridad ya no es únicamente un acelerador del negocio: hoy es un **habilitador fundamental**. Sin ciberseguridad, simplemente no hay negocio.

En este inicio de año quiero compartir los **tres grandes ejes** sobre los que un CISO concentra —o debería concentrar— su labor. Estos responden directamente a los principales puntos de dolor que cualquier organización enfrenta en materia de seguridad, y son los pilares que promovemos en NTT DATA como compañía global. Sobre ellos se articulan los servicios que ofreceremos en los próximos años:

1. Gestión de riesgos y cumplimiento proactivo

Toda iniciativa de ciberseguridad debe partir de un riesgo claramente identificado y contribuir a mitigarlo. Asimismo, es fundamental mantener una revisión continua para anticiparse a los nuevos riesgos que emergen con la aparición de técnicas de ataque cada vez más sofisticadas.

2. Potenciar un negocio seguro

El CISO debe actuar como un estratega más dentro del *C-level*, asegurando que los objetivos de ciberseguridad estén plenamente alineados con los objetivos corporativos. Su labor también implica construir **historias de valor** que refuercen la confianza de clientes, empleados y *stakeholders* en la organización.

3. Ciberresiliencia

La resiliencia es ya un concepto imprescindible. Cualquier disrupción genera pérdidas económicas, pero la verdadera diferencia está en la capacidad de una organización para **recuperarse rápidamente** ante un incidente y minimizar su impacto en el negocio.

En este 2026, seguiremos comprometidos con ayudar a las organizaciones a fortalecerse en torno a estos tres pilares. Estoy convencida de que quienes trabajamos en ciberseguridad desempeñamos un papel clave en la evolución de las compañías en los próximos años y, por ello, realizamos un trabajo fascinante.

¡El equipo de NTT DATA les desea un feliz y ciber seguro 2026!

Maria Pilar Torres Bruna
Head of Cybersecurity IBIOL

Shai-Hulud 2.0: el día en que el gusano entendió la cadena completa

Cibercrónica por Marlon Nivia Devia

Durante septiembre y noviembre de 2025, la industria del *software* descubrió que la era de los ataques a la cadena de suministro no había alcanzado su punto máximo: apenas estaba comenzando. Lo que hasta entonces se consideraba un riesgo asociado al uso de componentes de terceros se transformó en una amenaza estructural capaz de comprometer no solo el código, sino a quienes lo escriben, lo empaquetan, lo automatizan y lo despliegan.

La aparición del gusano Shai-Hulud y, pocos meses después, su variante más avanzada, Shai-Hulud 2.0, marcó un antes y un después para el ecosistema tecnológico y las plataformas de desarrollo en la nube. La industria comprendió que el problema iba más allá que npm; era la confianza delegada en un engranaje de automatismos que nadie cuestionaba.

La primera ola llegó en septiembre del 2025, cuando investigadores dieron a conocer un ataque de envenenamiento de paquetes en npm que se propagaba por sí mismo. Fue catalogado como una infección masiva, decenas de paquetes modificados, miles de descargas comprometidas y un efecto dominó que se movía rápido, pero cuyo alcance parecía limitado al repositorio. Ese diagnóstico resultó ser, en retrospectiva, un espejismo optimista. En noviembre de 2025, emergió Shai-Hulud 2.0: un gusano más sigiloso, más consciente de su entorno y con ambiciones que trascendían la distribución de código. El ataque ya no solo afectaba versiones publicadas, sino identidades digitales directamente vinculadas a GitHub, AWS, Google Cloud Platform y Azure. La superficie de ataque se había ampliado desde un package.json hasta la infraestructura donde se desarrolla, integra y despliega cada pieza de *software*.

El cambio de estrategia se reflejó en sus nuevas capacidades. Shai-Hulud 2.0 robaba *tokens* de npm, credenciales de GitHub y claves de API, pero también utilizaba estos secretos para entrar en los servicios nativos de gestión de credenciales de los tres proveedores *cloud* más relevantes: AWS Secrets Manager, Google Secret Manager y Azure Key Vault. Incluso apuntaba a sistemas heredados como Azure Pod Identity, aún presentes en numerosos *clústeres* de Kubernetes.

El gusano no solo obtenía lo estático; entendía lo dinámico: el permiso justo, la variable del *pipeline*, la llave que abre producción desde un entorno que nunca debió tenerla.

Y si el robo fallaba, el *malware* recurría a su última carta, un comportamiento destructivo capaz de borrar directorios completos, como si supiera que en una cadena de suministro rota, destruir puede ser comparablemente rentable a robar.

El impacto real no se midió en paquetes infectados, sino en secretos expuestos. Según investigaciones posteriores, aproximadamente 400.000 credenciales sin procesar fueron recolectadas y difundidas a través de decenas de miles de repositorios públicos, quedando abiertamente accesibles para cualquier tercero que los encontrara, analizara o reutilizara. Lo alarmante fue descubrir que muchos de estos *tokens* seguían activos cuando la campaña salió a la luz.

La industria debatía aún cuántas versiones habían sido afectadas cuando la verdadera pregunta emergió: ¿quién tenía acceso ahora a estos datos y durante cuánto tiempo? Lo que empezó como un incidente técnico en npm terminó afectando plataformas de integración continua como GitHub Actions, Jenkins, GitLab CI y AWS CodeBuild, comprometiendo *pipelines* basados en contenedores Linux que automatizaban procesos de publicación y despliegue. El ataque comprobó que no era necesario entrar a producción cuando se podía controlar la fábrica entera que producía el *software*.

Para la comunidad de desarrollo, Shai-Hulud 2.0 representó algo más que un gusano: fue una señal de que el modelo de confianza del *software* moderno necesitaba replantearse. El código abierto se sostiene en la colaboración, pero la automatización extrema se sostiene en la fe; en la suposición de que cada paquete es seguro, cada *token* está resguardado y cada *script* que se ejecuta durante una instalación fue puesto allí con buenas intenciones. El gusano demostró que, en un mundo donde instalar es equivalente a ejecutar, cada línea de código descargado es una decisión de seguridad.

Un año, dos variantes y un mensaje evidente: la amenaza ya no entra por la aplicación, entra por quien la construye.

Shai-Hulud no solo robó secretos; expuso una realidad incómoda: la cadena de desarrollo de *software* es tan fuerte como la menor de sus dependencias y tan segura como el *token* más olvidado en una variable de entorno. Protegerla exige ver más allá del repositorio y asumir que cada automatización, por útil que sea, puede convertirse en una ejecución no supervisada al servicio del atacante.

Marlon Nivia Devia
Cybersecurity Engineer

OWASP TOP 10 2025, ¿mejores programadores o mejores *frameworks*?

Artículo por Martín Bedoya Rodriguez

En los últimos años, los *frameworks* modernos para el desarrollo de aplicaciones web, móviles y APIs han mejorado significativamente, no solo en velocidad y usabilidad, sino también en seguridad. Tecnologías como Spring Boot, .NET, FastAPI, React o Flutter han incorporado mecanismos de protección que ayudan a prevenir vulnerabilidades comunes. Sin embargo, a pesar de estas mejoras, aún existe una brecha entre las herramientas disponibles y el nivel de conciencia que los equipos de desarrollo tienen sobre prácticas seguras de programación.

El cambio también se ha visto en la forma de estructurar el *software*. En lugar de aplicaciones monolíticas, ahora se opta por arquitecturas modulares que favorecen la separación de responsabilidades. Esto facilita la implementación de buenas prácticas de seguridad desde el diseño. No obstante, el hecho de usar una arquitectura moderna no garantiza por sí mismo que el *software* sea seguro. La seguridad sigue dependiendo, en gran medida, del conocimiento y criterio de quienes diseñan e implementan las soluciones.

Mediante el OWASP TOP 10 es posible entender cómo han evolucionado las amenazas en el *software*. Es una lista ordenada que agrupa las principales categorías de vulnerabilidades más explotados durante los últimos 4 años, de este modo, es una guía perfecta para que los equipos de desarrollo prioricen las actividades de seguridad durante el ciclo de vida del *software*. La versión más reciente, el OWASP TOP 10:2025 ha incluido cambios importantes que reflejan cómo han evolucionado los ciberataques y el impacto causado sobre las organizaciones.

Uno de los cambios más llamativos es la caída de las vulnerabilidades por inyección al quinto lugar. En 2017, esta categoría ocupaba el primer puesto, en 2021 descendió al puesto tres. Esto demuestra que los controles implementados por los *frameworks* han tenido un efecto positivo. La mayoría de *frameworks* incluyen controles de sanitización que previenen este tipo de vulnerabilidades sin que el programador tenga que intervenir directamente. Aun así, las aplicaciones antiguas o el uso incorrecto de las capacidades del *framework* siguen representando un riesgo.

En contraste, el primer lugar sigue ocupado por las vulnerabilidades en el control de acceso, es decir, fallos que permiten a los usuarios acceder a información o funciones que no deberían.

Este tipo de vulnerabilidad es más difícil de mitigar automáticamente porque depende de cómo se definen los permisos y roles dentro del *software*. Requiere decisiones conscientes por parte de los desarrolladores, quienes deben entender bien cómo funciona el negocio para implementar controles efectivos.

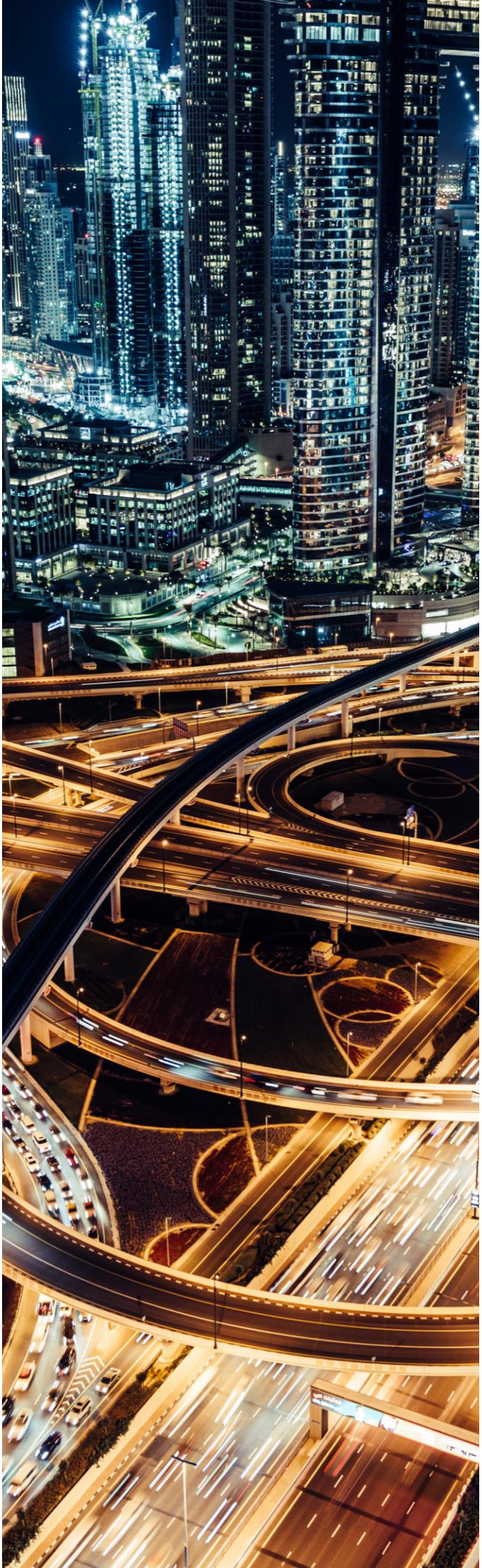
Otra novedad importante en la edición 2025 es la incorporación de la categoría “fallos en la cadena de suministro de *software*”, que refleja el riesgo de depender de librerías externas sin validación. Hoy es común que una aplicación dependa de decenas de componentes desarrollados por terceros, y basta que uno de ellos tenga una vulnerabilidad para comprometer todo el *software*. Esta categoría menciona el *typosquoatting*, técnica reciente que consiste en cambiar los nombres a librerías públicas e infectarlas con *malware* esperando que los desarrolladores incautos las importen.

OWASP TOP10:2025 refleja un avance significativo en la seguridad ofrecida por los *frameworks* de desarrollo, lo que ha permitido reducir ciertas vulnerabilidades históricas. Sin embargo, también evidencia que persisten vulnerabilidades relacionadas directamente con decisiones humanas. Errores en la lógica de autorización, malas prácticas en la gestión de dependencias o fallos por desconocimiento demuestran que el desarrollador sigue siendo un actor fundamental en la seguridad del ciclo de vida del *software*.

En síntesis, aunque los *frameworks*, herramientas, plataformas y metodologías para hacer *software*, han evolucionado para ofrecer mayor seguridad, la responsabilidad sigue siendo compartida. Es esencial que los equipos de desarrollo incorporen buenas prácticas desde el principio del proceso de *software*, y que comprendan que la seguridad no es solo un asunto técnico, sino una necesidad estratégica del negocio.

OWASP TOP10:2025 no solo muestra las vulnerabilidades más explotadas en los últimos 4 años, sino que también invita a repensar cómo se construye *software* en un entorno cada vez más complejo. En lugar de reaccionar ante vulnerabilidades, la tendencia es clara: prevenir desde el inicio, con diseño seguro, equipos capacitados y una cultura de desarrollo responsable.

Martín Bedoya Rodriguez
Cybersecurity Expert Engineer



OWASP Top Ten 2025: del código seguro al ecosistema seguro

Artículo por Evelyn Terrones Romero

La seguridad en el desarrollo de aplicaciones ha evolucionado a gran velocidad. Lo que antes era una disciplina centrada en corregir errores en el código, hoy se ha convertido en una gestión integral que abarca todo el ecosistema de *software*. Este artículo muestra la evolución del OWASP Top Ten, analiza las principales novedades en su edición 2025 y compara los cambios más relevantes respecto a la versión anterior (2021), con el objetivo de entender mejor los riesgos actuales y cómo prepararnos para mitigarlos.

OWASP Top Ten

El OWASP Top Ten es un proyecto abierto y global que identifica las principales vulnerabilidades de seguridad en aplicaciones y se ha consolidado como un estándar de facto en la gestión de riesgos para el desarrollo seguro. Su enfoque prioriza los riesgos con mayor impacto y la frecuencia de explotación, convirtiéndose en una de las referencias más influyentes en materia de seguridad en aplicaciones.

OWASP 2025: Novedades destacadas

El OWASP Top Ten 2025, es la octava edición desde su lanzamiento en 2003 y continúa siendo el documento de referencia mundial sobre los diez riesgos más críticos en aplicaciones web. Esta versión trae consigo un cambio de enfoque: si bien mantiene la atención en problemas estructurales, amplía la mirada hacia riesgos que surgen del entorno operativo, la cadena de suministro de *software* y el manejo de condiciones excepcionales.

¿Qué incorpora la nueva versión 2025?

- Dos categorías nuevas.
- Cambios de nombre y alcance en varias categorías existentes.
- Consolidación de riesgos para agruparlos por causa raíz y no solo por su manifestación.

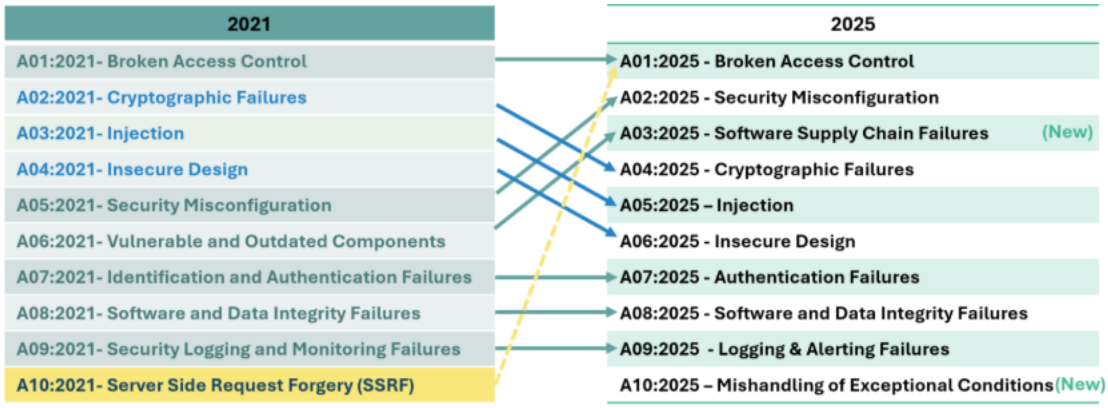
A continuación, destacan los principales cambios para esta nueva edición:

A03: Fallos en la cadena de suministro de *software*

Este nuevo riesgo ocupa el tercer lugar y reemplaza al antiguo “Componentes vulnerables y desactualizados” de 2021. Ahora no solo contempla el uso de librerías inseguras, sino todo el ecosistema de dependencias: paquetes maliciosos, *scripts* contaminados, *pipelines* comprometidos y errores en la gestión de secretos. El foco está en fortalecer la gestión de terceros.

A10: Manejo incorrecto de condiciones excepcionales

Esta nueva categoría aborda fallos en el manejo de errores, *time-outs* no controlados, errores lógicos en estados anómalos, filtración de información sensible a través de mensajes de error y excepciones mal gestionadas que pueden abrir brechas críticas de seguridad. Estos problemas, que antes se consideraban operativos, hoy son vectores reales de ataque que permiten la exposición de datos confidenciales o la ejecución de lógica maliciosa. En 2025, OWASP deja claro que una aplicación puede ser técnicamente correcta y, aun así, vulnerable si no responde de forma segura ante lo inesperado.



Fusión de SSRF con Pérdida de Control de Acceso

El Server Side Request Forgery (SSRF), anteriormente ubicado en la categoría A10:2021, se incorpora ahora dentro de A01:2025 “Pérdida de Control de Acceso”. Este cambio refleja que SSRF debe entenderse como un problema de control de acceso y no como una vulnerabilidad aislada. Así, se refuerza el enfoque en el acceso a recursos internos, APIs y servicios de *backend*, que actualmente representan uno de los principales vectores de ataque en entornos *cloud*.

Ascenso de la categoría Configuración de Seguridad Incorrecta

La categoría A05:2021 “Configuración de Seguridad Incorrecta”, asciende al puesto A02:2025, reconociendo que muchos fallos actuales no se encuentran en el código en sí, sino en cómo se implementan los entornos: credenciales por defecto, permisos mal configurados, servicios expuestos, políticas inseguras o cabeceras de seguridad ausentes, entre otros.

Inyección y Fallos Criptográficos bajan algunos puestos

Estas categorías descienden en el OWASP Top Ten 2025, no porque hayan perdido relevancia en cuanto a su severidad, sino porque el contexto de amenazas ha cambiado. Actualmente, otros riesgos se presentan con mayor frecuencia y representan vectores de ataque más explotados.

Lo que esta nueva edición nos enseña:

- **La seguridad ya no es solo responsabilidad del equipo de desarrollo:**

Las nuevas categorías reflejan que los equipos de DevOps, infraestructura y seguridad deben trabajar de manera conjunta. Un buen código desplegado en un entorno mal configurado, sigue siendo vulnerable.

- **Las dependencias son tu responsabilidad:**

Es fundamental escanear y gestionar las dependencias, monitorizar vulnerabilidades y aplicar principios de confianza cero desde el diseño.

- **Los errores también son puertas de entrada a ataques:**

El nuevo foco en el manejo de excepciones y condiciones no esperadas muestra que la resiliencia del sistema no es solo operativa. Un error mal gestionado puede convertirse fácilmente en una vulnerabilidad, por eso, anticipar y controlar estos fallos es parte esencial de una estrategia de seguridad efectiva.

El **OWASP Top Ten 2025** marca una nueva etapa en la madurez de la seguridad en aplicaciones. Hoy el riesgo no está únicamente en el código fuente, sino en cómo integramos, desplegamos, configuramos y operamos nuestro *software*. Este enfoque más holístico exige una verdadera cultura DevSecOps, basada en la colaboración entre distintas áreas.

En una era de desarrollo acelerado, dependencias externas y despliegues continuos, conocer y aplicar el OWASP Top Ten no es solo una buena práctica: **es una necesidad.**

Evelyn Terrones Romero
Cybersecurity Expert Analyst

La evolución del ecosistema OWASP

Tendencias por Diego Carreño

OWASP ha dejado de ser esa lista de vulnerabilidades que vemos en cada presentación de informes de *pentest* para convertirse en el sistema operativo silencioso que orquesta la seguridad del *software* moderno. Ya no se trata solo del Top 10, sino de un ecosistema de estándares (ASVS, MASVS, SAMM, API Security, LLM Top 10, AI Testing Guide, entre otros) que estructura cómo diseñamos, desarrollamos, probamos y gobernamos aplicaciones, APIs y sistemas de IA.

Hoy, hablar de OWASP es hablar de un "sistema operativo" para la seguridad del *software*: un conjunto de estándares, controles, prácticas y metodologías que articulan desde la planificación de un *backlog* hasta las auditorías técnicas de cumplimiento. No se trata solo de proteger el código: se trata de diseñar organizaciones que piensen, construyan y aseguren el *software* de forma integral.

De *checklist* a "sistema operativo" de AppSec

La primera señal importante de este cambio fue OWASP ASVS (para aplicaciones web y servicios) y MASVS (para aplicaciones móviles), que definen niveles de seguridad (L1, L2, L3) y requisitos claros que se trasladan a políticas, historias de usuario, criterios de aceptación y alcance de pruebas. A su alrededor se ha ido formando un ecosistema cada vez más denso:

- SAMM, como modelo de madurez de los programas de seguridad de *software* con enfoque evolutivo.
- La Web Security Testing Guide (WSTG) y la Mobile Application Security Testing Guide (MASTG), como catálogos de pruebas de seguridad que se convierten en *suites* de regresión para web y móvil.
- Guías como Cheat Sheet Series y Proactive Controls, que aterrizan en recetas concretas de codificación defensiva.
- El Threat Modeling Project, junto con herramientas como Threat Dragon y enfoques como Cornucopia, para llevar el análisis de amenazas al *backlog* desde el diseño.
- Los laboratorios intencionalmente vulnerables como Juice Shop, WebGoat, usados para entrenar equipos y validar reglas de análisis estático y dinámico.
- Además de los distintos Top 10 especializados (API Security Top 10, Top 10 for LLM Applications, etc.), que ya están estructurando cómo probar sistemas basados en IA generativa.

La tendencia de fondo es clara: las organizaciones ya no consumen estos proyectos de forma aislada. Los ensamblan como módulos de un mismo sistema, coherente y transversal al negocio.

El resultado práctico es que OWASP deja de ser una lista que se consulta al final para revisar vulnerabilidades y pasa a ser la capa que estructura desde la idea hasta producción.

OWASP como "lenguaje común" entre negocio, desarrollo y riesgo

Uno de los avances más visibles es el uso de OWASP como lenguaje común entre áreas que históricamente hablaban dialectos distintos. Negocio se mueve en términos de riesgos y KPI, desarrollo habla de *bugs* y deuda técnica, riesgo y cumplimiento miran controles y normativas. OWASP está empezando a actuar como traductor entre todos. Algunos ejemplos que hemos visto en 2025:

- Los *product owners*, junto a los analistas de seguridad, fijan el nivel de seguridad objetivo de cada iniciativa en términos de ASVS o MASVS y lo incorporan como requisito no funcional en el *backlog*.
- Riesgo y cumplimiento mapean marcos como PCI-DSS, NIS2 o regulaciones locales a familias de requisitos OWASP (autenticación, *logging*, criptografía, etc.).
- Auditoría interna utiliza SAMM para evaluar capacidades, *roadmap* y evidencia de mejora continua, más allá de controles puntuales.
- Las fábricas de desarrollo y *testing* estandarizan plantillas de historias de usuario seguras, criterios de aceptación y casos de prueba apoyándose en ASVS, WSTG, MASTG y las Cheat Sheets.

El resultado es que una conversación que antes se daba en tres idiomas distintos empieza a tener un diccionario compartido. Cuando se dice "vamos a llevar esta API a un nivel de ASVS L2 y cubrir el Top 10 de API Security", todos entienden qué implica y lo más importante: pueden medir si se está cumpliendo.

OWASP como columna vertebral de la automatización

La otra gran palanca de cambio es la automatización. OWASP se ha convertido en la taxonomía que muchas organizaciones usan para orquestar sus *pipelines* de DevSecOps, la correlación de hallazgos y la priorización de remediación.

Los escáneres SAST, DAST e IAST etiquetan vulnerabilidades con referencias a OWASP (ASVS, API Top 10 2023, Top 10 LLM, etc.). En muchas organizaciones, todos esos resultados se consolidan en un único panel de seguridad de aplicaciones que los agrupa bajo ese mismo esquema y, a partir de ahí, los *pipelines* CI/CD aplican "perfiles OWASP" distintos según el tipo de aplicación y su criticidad.

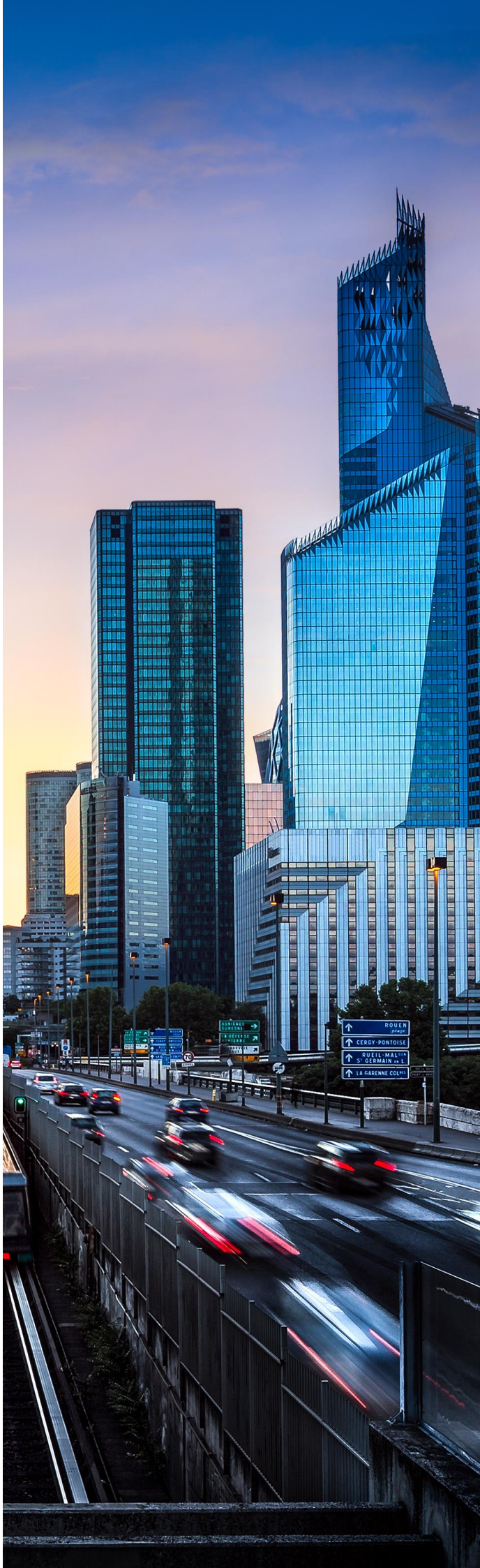
Incluso los asistentes de IA generativa para desarrollo seguro se están entrenando con controles y guías OWASP: ASVS, MASVS, Cheat Sheets, WSTG, MASTG o el propio AI Testing Guide, recién lanzado. De este modo, las recomendaciones de diseño, codificación defensiva y pruebas salen alineadas desde el minuto uno con estándares reconocidos.

Conclusión: la próxima ventaja competitiva será hablar OWASP con fluidez

Las organizaciones que abracen esta ola como una decisión estratégica (y no como "otra referencia más") serán las que consigan alinear negocio, desarrollo, riesgo y auditoría en un único lenguaje; industrializar controles y pruebas sin perder trazabilidad; e incorporar nuevas tecnologías sin tener que reinventar el modelo de seguridad desde cero cada vez.

OWASP deja así de ser solo lo que miramos cuando algo sale mal y se convierte en el sistema operativo de seguridad que define cómo construimos lo que queremos que salga bien. Y eso, lejos de ser una moda, es la tendencia que probablemente marcará la próxima década del desarrollo seguro.

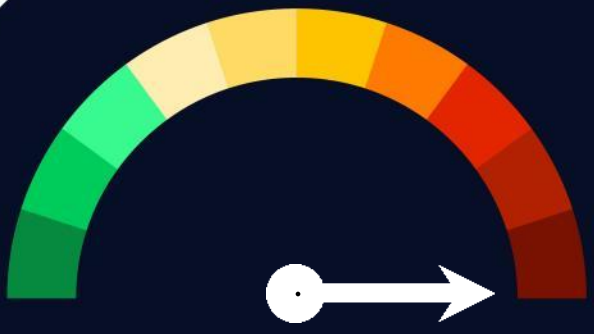
Diego Carreño
Cybersecurity Lead Analyst



Vulnerabilidades

Vulnerabilidad crítica en React Server Components

Fecha: 3 de diciembre de 2025
CVE: CVE-2025-55182



CVSS: 10

CRÍTICA

Descripción

Se ha informado acerca de una vulnerabilidad de severidad crítica presente en las funciones de servidor de React.

React proporciona herramientas e integraciones que los empaquetadores y *frameworks* utilizan para ejecutar código, tanto en clientes como en servidores.

React traduce las peticiones realizadas por el cliente a peticiones HTTP que se reenvían al servidor. Este, a su vez, las traduce en llamadas a una función y devuelve los resultados.

Un atacante no autenticado podría elaborar una petición HTTP maliciosa dirigida a un servidor React, de modo que al ser traducida se ejecute código en el sistema.

Solución

Se recomienda actualizar inmediatamente a las versiones con parches:

- React Components Server versiones 19.0.1, 19.1.2 y 19.2.1.
- Si se dispone de una aplicación que utilice el *framework* @vitejs/plugin-rsc se recomienda actualizar a: @vitejs/plugin-rsc@0.5.3 o posteriores.
- Para Next.js, las versiones 15.x y 16.x, se deben actualizar a las versiones: 15.0.5, 15.1.9, 15.2.6, 15.3.6, 15.4.8, 15.5.7 y 16.0.7.
- Para 14.3.0-canary.77 o posterior, bajar a la versión estable 14.x o a la 14.3.0-canary.76.

Productos afectados

Algunos de los productos son:

- paquete web react-server-dom (react-server-dom-webpack);
- paquete dom del servidor react (react-server-dom-parcel)
- react-server-dom-turbopack

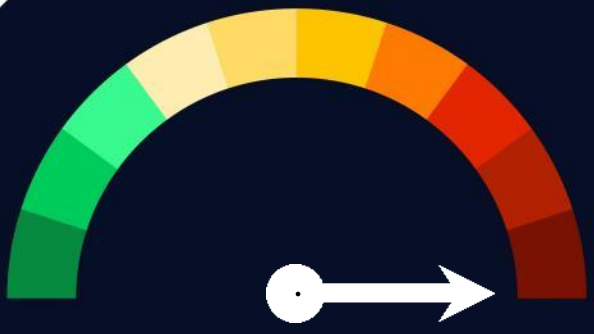
Referencias

- nvd.nist.gov
- www.incibe.es

Vulnerabilidades

Vulnerabilidad crítica en Apache Tika

Fecha: 4 de diciembre de 2025
CVE: CVE-2025-66516



CVSS: 10

CRÍTICA

Descripción

Una vulnerabilidad crítica de inyección XEE ha sido identificada en varios componentes de Apache Tika.

Este fallo permite que un archivo PDF manipulado mediante contenido XFA malicioso provoque la carga de entidades XML externas durante su procesamiento. Esto provoca la exposición de archivos del sistema lo que, en determinados entornos, facilita ataques de mayor gravedad.

La vulnerabilidad amplía el alcance del fallo previamente identificado (CVE-2025-54988), ya que también afecta a módulos adicionales y a versiones de Tika en las que el código vulnerable residía en paquetes internos diferentes, dificultando así su detección.

Solución

Se aconseja actualizar inmediatamente las versiones afectadas por aquellas en las que se han aplicado correcciones:

- Tika-core: versión 3.2.2
- Tika-parser-pdf-module: versión 3.2.2
- Tika-parsers: versión 2.0.0

Productos afectados

Los paquetes afectados incluyen las versiones:

- Tika-core: versiones 1.13 a 3.2.1
- Tika-parser-pdf-module: versiones 2.0.0 a 3.2.1
- Tika-parsers: versiones 1.13 hasta anteriores a 2.0.0

Referencias

- thehachernews.com
- incibe.es

Android corrige 107 vulnerabilidades en su parche de seguridad de diciembre

Fecha: 1 de diciembre de 2025
CVE: CVE-2025-48631 y 106 más

Crítica

Descripción

Android ha publicado el parche de seguridad correspondiente al mes de diciembre, donde corrige un total de 107 vulnerabilidades. Entre ellas, se encuentran 7 vulnerabilidades de severidad crítica y 98 de severidad alta.

El fabricante ha comunicado que existen indicios de explotación activa de las vulnerabilidades CVE-2025-48572 y CVE-2025-48633.

La primera podría permitir a un atacante llevar a cabo una escalada de privilegios, mientras que la segunda corresponde a una vulnerabilidad de divulgación de información.

Entre las vulnerabilidades destaca la crítica CVE-2025-48631, ubicada en el componente *framework*, podría permitir un ataque remoto de denegación de servicio sin requerir privilegios adicionales.

Productos afectados

Los productos afectados por la actualización son los siguientes:

- Android Open Source Project (AOSP): versiones 13, 14, 15 y 16.
- Componentes de Arm, MediaTek, Unisoc y Qualcomm.

Solución

Se recomienda aplicar los parches de seguridad publicados por el fabricante.

Referencias

- source.android.com
- incibe.es

Sneeit Framework corrige una vulnerabilidad de ejecución de código remoto (RCE)

Fecha: 8 de diciembre de 2025
CVE: CVE-2025-6389

Crítica

Descripción

Se ha identificado una vulnerabilidad crítica en Sneeit Framework, un componente ampliamente utilizado por múltiples temas y plantillas premium de WordPress.

La vulnerabilidad permite a un atacante remoto no autenticado ejecutar funciones PHP arbitrarias a través de una llamada manipulada al *framework.*

El fallo se encuentra en una función que procesa entradas de usuarios sin validación, lo que permite ejecutar funciones arbitrarias en el servidor pudiendo derivar en: instalación de *backdoors*, creación de cuentas de administrador no autorizadas o compromiso de sitios web.

Productos afectados

Los productos afectados por la actualización son los siguientes:

- Todas las versiones del Sneeit Framework hasta la 8.3 incluida
- Cualquier tema o plantilla WordPress que incorpore esta versión del *framework*

Solución

El desarrollador recomienda:

- actualizar a Sneeit Framework 8.4
- Además, revisar configuraciones, usuarios administrativos y posibles señales de compromiso.

Referencias

- techradar.com
- nvd.nist.gov

Eventos

NIST Small Business Cybersecurity Webinar
20 de enero

El NIST ofrecerá un webinar virtual, vía Zoom for Government, enfocado en ayudar a pequeñas y medianas empresas a proteger *Controlled Unclassified Information*. Durante la sesión, se presentará el nuevo "Small Business Primer" para la SP 800-171 Revisión 3, explicando sus requisitos clave. Expertos de NIST orientarán sobre cómo empezar a implementar estas prácticas de seguridad y responderán preguntas de los asistentes.

Enlace

II Jornada DORA
21 de enero

La cita se presenta como un foro de referencia para compartir experiencias, evaluar avances, exponer principales dificultades y anticipar próximos pasos. Todo ello, de la mano de mesas redondas compuestas por los principales actores implicados en dicha normativa: reguladores, CISO y representantes de la Administración Pública. En concreto, participarán representantes del Ministerio para la Transformación Digital y de la Función Pública, Incibe, Agencia de Ciberseguridad de Madrid, Banco de España, Banco Santander, BBVA, CaixaBank, Mapfre, ING Bank, Allianz, Abanca, Sabadell Digital, Bankinter Group, Unicaja, Singular Bank, Santalucia, AXA Seguros, Triodos Bank.

Enlace

IA Expo Internacional 2026
31 de enero

IA Expo Internacional 2026 tendrá lugar el 31 de enero de 2026 en el The Westin Santa Fe, Ciudad de México. El evento reunirá a líderes, emprendedores, desarrolladores, investigadores y ejecutivos para analizar casos reales de adopción de inteligencia artificial, sus aplicaciones prácticas en distintos sectores, así como temas clave como ética, seguridad, automatización, transformación digital e innovación con IA.

Enlace

Recursos

➢ Guidelines for Media Sanitization

El NIST, a través de su publicación “Guidelines for Media Sanitization” (NIST Special Publication 800-88 Revision 1), establece un marco técnico claro y estandarizado para la sanitización segura de medios de almacenamiento, con el fin de garantizar que la información sensible sea eliminada de forma efectiva y no pueda ser recuperada por actores no autorizados.

El documento detalla métodos de limpieza lógica, depuración y destrucción física aplicables a distintos tipos de dispositivos (HDD, SSD, USB, equipos móviles, cintas, etc.), proporciona criterios para seleccionar la técnica adecuada según el nivel de sensibilidad de los datos y el ciclo de vida del medio, y define responsabilidades organizacionales para asegurar una gestión segura y trazable.

Enlace

➢ NIST Investments 2025

El documento “NIS Investments 2025” de ENISA analiza en profundidad cómo los Estados miembros de la Unión Europea y los operadores de servicios esenciales están invirtiendo en capacidades de ciberseguridad para cumplir con los requisitos de la Directiva NIS2 y fortalecer su resiliencia frente a amenazas crecientes. El informe presenta datos y tendencias sobre prioridades de inversión, madurez de las capacidades nacionales, evolución de riesgos, así como desafíos regulatorios y operativos que enfrenta el ecosistema europeo.

Enlace

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com