

FOS

Volumen 11, número 02

Estado de la seguridad de API y aplicaciones 2025

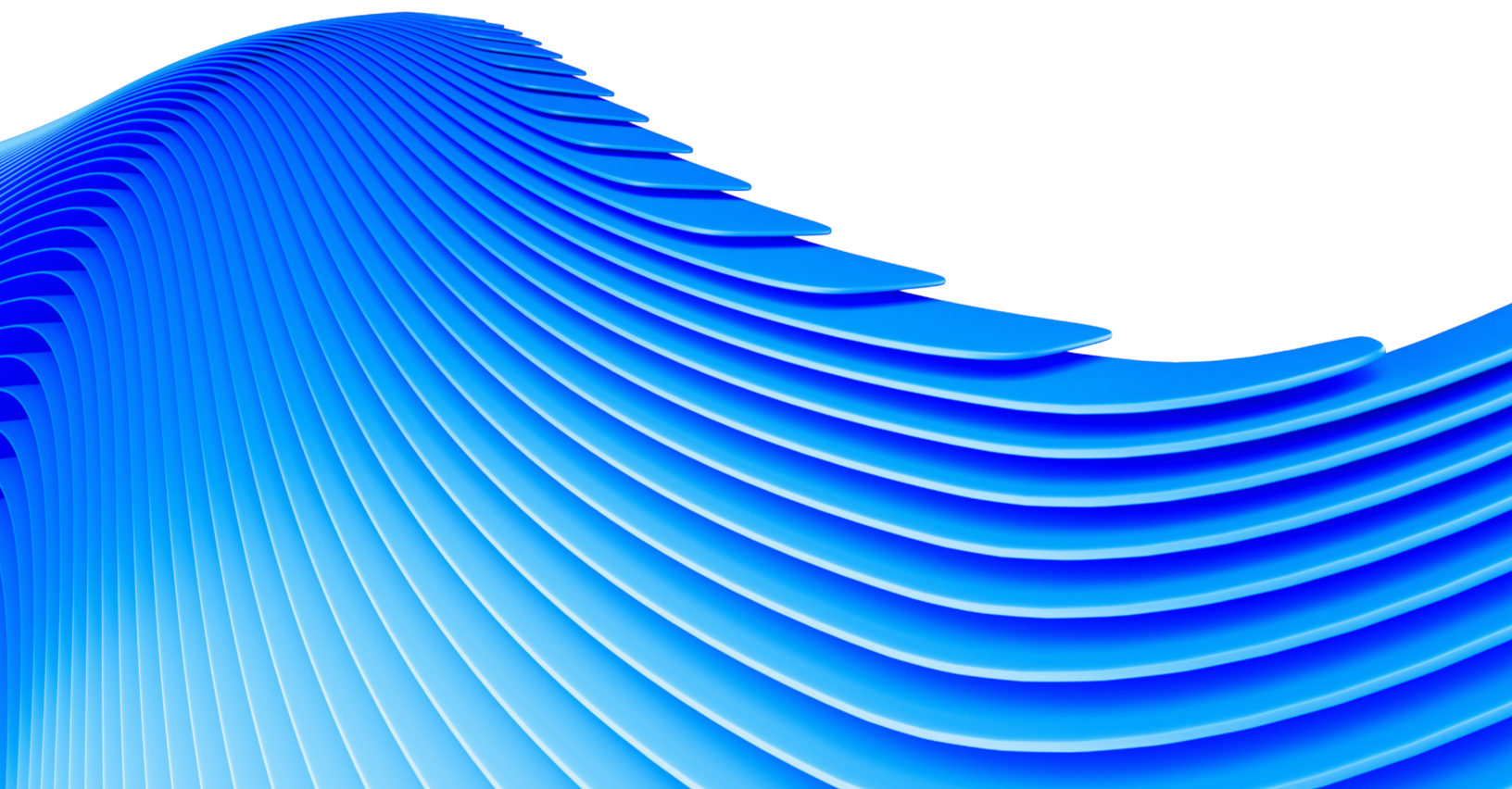
Cómo cambia la IA el panorama digital



Estado de Internet/**Seguridad**

Contenido

02	Introducción
04	Información clave del informe
06	Evolución de nuestra inteligencia sobre amenazas de API
13	Ataques web: comparación y tendencias interanuales
17	Ataques DDoS de capa 7: comparación y tendencias interanuales
21	Tendencias por sectores
27	Tendencias regionales
39	Cumplimiento
44	Mitigación
46	Metodología
47	Créditos



Introducción

El panorama de la seguridad de las aplicaciones web a principios de 2025 refleja una complejidad y una sofisticación sin precedentes en los vectores de amenaza. Las organizaciones se enfrentan a un marcado aumento de los ataques dirigidos a aplicaciones web: Akamai observó más de 311 000 millones de ataques a API y aplicaciones web solo en 2024, lo que representa un aumento interanual del 33 %. Este aumento está directamente relacionado con la rápida adopción de servicios en la nube, arquitecturas de microservicios y aplicaciones con inteligencia artificial (IA). Los **factores** geopolíticos han intensificado aún más este panorama, y son los sectores de alta tecnología, comercio y redes sociales en los que se observa el mayor volumen de ataques distribuidos de denegación de servicio (DDoS) a la capa 7 (capa de aplicación). Cabe destacar que los atacantes ahora están **implementando** métodos de intrusión generados por IA que automatizan todo el ciclo de vida de los ataques.

De forma paralela, las API se han convertido en objetivos críticos. En Akamai, hemos documentado más de 150 000 millones de ataques a estas entre enero de 2023 y diciembre de 2024. La integración de herramientas de software como servicio (SaaS) basadas en IA con plataformas clave mediante API ha ampliado considerablemente la superficie de ataque. Las **implicaciones** financieras son graves: en la actualidad, los problemas relacionados con la seguridad de las API cuestan a las organizaciones aproximadamente 87 000 millones de dólares al año, y los pronósticos indican que esta cifra podría superar los 100 000 millones de dólares en 2026 si no se interviene de forma adecuada. Las API zombis y en la sombra presentan vectores de ataque especialmente vulnerables en ecosistemas de API cada vez más complejos.



El papel de la IA en la seguridad de las API y las aplicaciones web

La IA está transformando tanto el entorno de seguridad de las API como el de las aplicaciones web al mejorar las capacidades de detección y respuesta ante amenazas, aunque también presenta nuevos desafíos. En las aplicaciones web, la IA se **utiliza** para automatizar la detección de amenazas, predecir posibles infracciones y mejorar los tiempos de respuesta ante incidentes. Sin embargo, la IA también **permite** a los atacantes generar malware basado en IA y un sofisticado scraping web, así como automatizar el ciclo de vida de los ataques con metodologías de ataque dinámicas.

En el caso de las API, la IA desempeña un **papel** fundamental a la hora de gestionar y proteger el gran número de interacciones con estas. Las herramientas basadas en IA son esenciales para detectar anomalías, identificar patrones de uso indebido y automatizar las respuestas a las amenazas en tiempo real. La gestión de API basada en IA seguirá **evolucionando** mediante la integración de análisis predictivos y medidas de seguridad automatizadas para protegerse contra ataques cada vez más sofisticados. A pesar de estos avances, los **ataques** basados en IA contra las API, como el Credential Stuffing y los ataques de lógica empresarial, siguen siendo una preocupación importante, ya que requieren marcos de seguridad sólidos para contrarrestar estas amenazas de forma eficaz.

Divergentes, pero interconectados: estrategias de ataque a API y aplicaciones web

Los ataques a API y aplicaciones web, aunque están relacionados, van dirigidos a diferentes aspectos de la infraestructura de una aplicación:



Los **ataques a aplicaciones web** se dirigen a los componentes orientados al usuario, como las páginas de inicio de sesión orientadas al público, y a menudo emplean técnicas menos sofisticadas.



Los **ataques de API** se centran en aprovechar las vulnerabilidades de los terminales de API y la lógica de back-end de una aplicación, lo que requiere un conocimiento más profundo de la estructura y el comportamiento de la API.

Las principales diferencias radican en la superficie de ataque y la complejidad. Los ataques a aplicaciones web suelen ir dirigidos a las partes visibles de una aplicación, mientras que los ataques de API van dirigidos a los canales de comunicación entre los diferentes componentes de software. Sin embargo, ambos pueden proporcionar acceso no autorizado a datos confidenciales y recursos del sistema cuando tienen éxito.

Conocer las medidas de ciberseguridad para los ataques a aplicaciones web y API simultáneamente es fundamental, ya que las aplicaciones modernas dependen cada vez más de las API para su funcionalidad. Las organizaciones prevén un **aumento** del 39 % en las aplicaciones web en los próximos dos años, por lo que la interdependencia de la seguridad web y de las API se ha vuelto más pronunciada. Si ignora cualquiera de estos aspectos, una organización puede quedar **vulnerable** a sofisticados ataques multivectoriales que aprovechan las debilidades tanto en el front-end como en el back-end de las aplicaciones.

Perspectiva única de Akamai: revelación de patrones de amenazas

El análisis que Akamai realiza de esta complejidad se beneficia de su infraestructura de red, que procesa más de un tercio del tráfico web global, lo que proporciona una visibilidad inigualable de los patrones de amenazas. Esta perspectiva, combinada con la información de sus equipos de investigación y ciencia de datos, permite a Akamai ofrecer inteligencia integral y útil. Sus conclusiones ofrecen a los responsables de seguridad la información estratégica necesaria para tomar decisiones sobre dónde centrarse a la hora de reducir los riesgos para maximizar el retorno de las inversiones en seguridad.

Información clave del informe



Las API basadas en IA son menos seguras que el resto.

La mayoría de las API basadas en inteligencia artificial (IA) son extremadamente accesibles y muchas utilizan mecanismos de autenticación inadecuados, una vulnerabilidad que se agrava con la creciente variedad de ataques con IA que las acechan.



La IA supone una ventaja técnica para los ciberdelincuentes.

Esto incluye avances como malware generado por IA, análisis de vulnerabilidades, ataques a sistemas integrados con IA y capacidades avanzadas de scraping web.

32 %

Porcentaje de crecimiento de los incidentes relacionados con los 10 principales riesgos de seguridad de API según OWASP

Los incidentes de seguridad de las API están aumentando y los 10 principales problemas de seguridad de las API según OWASP revelan fallos en la autenticación y autorización que dejan al descubierto funciones y datos confidenciales.

30 %

Aumento de las alertas relacionadas con el marco de seguridad MITRE

Los atacantes utilizan técnicas avanzadas, como la automatización y la IA, para explotar las API. El marco de trabajo MITRE puede ayudar a los defensores a identificar estos ataques de forma más rápida y precisa.

33 %

Porcentaje de aumento de los ataques web globales año tras año

El aumento de los ataques está directamente relacionado con la rápida adopción de servicios en la nube, microservicios y aplicaciones de IA, que amplían las superficies de ataque y presentan nuevos desafíos de seguridad.

230 000 millones+

Número de ataques web que afectan a las organizaciones comerciales,

lo que lo convierte en el sector más afectado, con casi el triple de ataques que el sector de la alta tecnología (el segundo más afectado).

73 %

Aumento del número total de ataques web año tras año en la región de Asia-Pacífico y Japón (APJ),

que pasó de 29 000 millones en 2023 a 51 000 millones en 2024.

37 %

Porcentaje de ataques web en la región de Europa, Oriente Medio y África (EMEA) dirigidos a API,

que tiene la mayor concentración de ataques de este tipo en todas las regiones.

94 %

Crecimiento trimestral de los ataques distribuidos de denegación de servicio (DDoS) de capa 7

entre el primer trimestre de 2023 y el cuarto trimestre de 2024.

11,9 billones

Número de ataques DDoS de capa 7 dirigidos a Norteamérica

durante el periodo de dos años comprendido entre el primer trimestre de 2023 y el cuarto trimestre de 2024.

7 billones

Número de ataques DDoS de capa 7 al sector de la alta tecnología

entre enero de 2023 y diciembre de 2024, lo que lo convierte en el que más amenazas de este tipo sufrió.

7,4 billones

Número de ataques DDoS de capa 7 dirigidos a la región APJ

durante el periodo de dos años comprendido entre el primer trimestre de 2023 y el cuarto trimestre de 2024.

20 %

Porcentaje de ataques DDoS de capa 7 relacionados con API dirigidos a la región EMEA,

que representa la mayor concentración de este tipo de ataque en todas las regiones.

Evolución de nuestra inteligencia sobre amenazas de API

La adquisición de Noname Security por parte de Akamai ha mejorado significativamente sus capacidades de análisis y generación de informes sobre las amenazas de API, lo que proporciona una nueva perspectiva sobre los riesgos específicos que afectan a tales API. Akamai utiliza este nuevo conjunto de datos (aún en las primeras etapas de la integración de datos) para mejorar nuestra inteligencia sobre amenazas existente y proporcionar una visión ampliada de los problemas relacionados con la seguridad de las API.

Asignación de alertas a marcos de seguridad

Con el tiempo, este nuevo conjunto de datos asignará detalles más minuciosos de las alertas de seguridad a los marcos de ciberseguridad críticos y a los estándares de cumplimiento, entre los que se incluyen:

- MITRE ATT&CK (Tácticas, técnicas y conocimientos comunes de los adversarios)
- Reglamento General de Protección de Datos (RGPD)
- Normas de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS)
- Organización Internacional de Normalización (ISO)
- Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP)

Estas mejoras refuerzan significativamente la capacidad de Akamai para proporcionar una protección sólida a los clientes. Al adscribirse a estos marcos, las organizaciones pueden comprender mejor su situación de seguridad, cumplir los requisitos normativos y priorizar de forma eficaz sus actividades relacionadas con la seguridad. Este enfoque integral permite a las organizaciones asignar recursos estratégicamente y desarrollar estrategias específicas para proteger sus API y sus datos confidenciales.

Análisis de una muestra de datos durante un periodo de 30 días

Para este informe, hemos analizado una muestra de datos de 30 días para destacar la actividad general de los atacantes en cada uno de los marcos de ciberseguridad y los estándares de cumplimiento (Figura 1). También ofrecemos una perspectiva más profunda de las alertas de MITRE y OWASP. Además, examinamos cómo estos riesgos e incidentes de seguridad pueden afectar a los estándares de cumplimiento.

	Actividad de 30 días	Aumento mensual
OWASP	5 907 000	32 %
MITRE	2 817 000	30 %
ISO	832 000	22 %
RGPD	669 000	21 %
PCI DSS	881 000	16 %

Fig. 1: Desglose de las alertas de seguridad según los marcos de seguridad y los estándares de cumplimiento

Alertas de MITRE

Durante un periodo de 30 días, observamos un aumento del 30 % en los incidentes relacionados con las técnicas MITRE entre nuestros clientes. En particular, los atacantes empleaban con frecuencia la técnica T1078 (Cuentas válidas), aprovechando credenciales legítimas para obtener acceso no autorizado a sistemas o redes. Dado que las API suelen depender de tokens de autorización, los adversarios que obtienen estos tokens pueden acceder a datos confidenciales sin ser detectados.

También identificamos la técnica T1566 (Phishing), en la que los atacantes lanzaron campañas de phishing para robar credenciales o tokens de API para futuros ataques. A medida que las API amplían la superficie de ataque, los atacantes las explotan cada vez más para acceder. Además, las alertas relacionadas con la técnica T1190 (Explotación de aplicación pública) revelaron que los atacantes utilizaban fallos de aplicaciones para infiltrarse en las redes. Otra técnica observada fue la T1580 (Descubrimiento de infraestructura de la nube), en la que los adversarios utilizaban API para el reconocimiento mediante el sondeo de los terminales de nube expuestos a través de llamadas de API.

Aunque MITRE no dispone de una matriz dedicada a seguridad de API, su marco sigue siendo fundamental para los equipos de seguridad y las organizaciones que buscan información sobre técnicas de atacantes dirigidas a API. Al asignar tácticas de adversarios a comportamientos específicos de API, los equipos de seguridad pueden mejorar la respuesta a incidentes y la detección de amenazas mediante la identificación de las etapas de ataque y sus respectivas tácticas, técnicas y procedimientos. Este enfoque permite a los defensores mitigar los riesgos de forma más eficaz.

Alertas de OWASP

Los 10 principales riesgos de seguridad de API según OWASP son un recurso vital que proporciona información útil sobre el impacto y la gravedad de las vulnerabilidades. Permite a los desarrolladores y a los equipos de seguridad priorizar las iniciativas de forma eficaz, con actualizaciones que mantienen la información relevante en un panorama de amenazas que evoluciona rápidamente.

Durante el periodo de muestra de 30 días, nuestro análisis reveló un aumento del 32 % en los incidentes relacionados con OWASP. Cabe destacar que vulnerabilidades como la autorización a nivel de propiedad de objeto comprometida (Broken Object Property Level Authorization, BOPLA), la autorización a nivel de función comprometida y la autenticación comprometida exponen datos confidenciales o funciones críticas directamente a los atacantes. La falta de mecanismos de autorización suficientes permiten a los adversarios derivar privilegios, apropiarse de cuentas y acceder a información confidencial, lo que los convierte en algunos de los vectores de ataque más peligrosos dirigidos a API.

La autorización a nivel de objeto comprometida (Broken Object Level Authorization, BOLA) sigue siendo una vulnerabilidad de seguridad de API crítica, pero su detección supone un reto debido a su dependencia de fallos en la lógica empresarial. A menudo esto genera una falta de información o bajos índices de detección. Para solucionar este problema, las organizaciones deben emplear soluciones de seguridad de API que establezcan relaciones claras entre los usuarios y los recursos a los que suelen acceder. Para ello, es necesario establecer referencias de comportamiento mediante avanzados algoritmos de aprendizaje automático capaces de reconocer patrones de acceso anómalos.

La autorización BOPLA aprovecha los problemas de acceso granular a nivel de campo en las API, que a menudo se pasan por alto durante las pruebas de seguridad. A diferencia de la autorización BOLA, que requiere cambiar los ID de objeto completos, los ataques de BOPLA se dirigen a propiedades específicas dentro de los objetos. Por ejemplo, una llamada DELETE a una API que expone información de identificación personal (PII) confidencial en su respuesta constituye una vulnerabilidad de BOPLA. Esta sutileza hace que los problemas de BOPLA sean más frecuentes que los ataques de BOLA.

Un ejemplo práctico implica una solicitud de cancelación de suscripción utilizando solo una dirección de correo electrónico, donde la respuesta de la API incluye involuntariamente el nombre completo y la dirección del usuario. Esta exposición de datos confidenciales a partes no autorizadas se produce porque las pruebas de seguridad suelen centrarse en objetos completos en lugar de en propiedades individuales. Este fallo contribuye al aumento en la detección de vulnerabilidades de tipo BOPLA en las evaluaciones de seguridad de API.

Otra vulnerabilidad crítica es el uso de recursos sin restricciones, que los atacantes pueden aprovechar para provocar interrupciones del servicio a través del agotamiento de recursos o ataques similares a DDoS. Esta vulnerabilidad plantea riesgos que van más allá del impacto en el servicio, como el aumento de los costes operativos debido al uso excesivo de los recursos en la nube y el aumento de los riesgos de ataques de fuerza bruta. Sin una limitación de velocidad adecuada, los atacantes pueden sondear rápidamente las API, lo que podría poner en peligro la seguridad. Además, estos ataques generan un tráfico considerable, lo que da lugar a un aumento significativo de los costes para las organizaciones.

El uso no seguro de API, que se deriva de una validación inadecuada, el filtrado de datos y la falta de mecanismos de seguridad durante las integraciones de API de terceros, presenta otro vector de amenaza importante. Este problema es cada vez más preocupante, ya que las organizaciones dependen más de las API de terceros para la transformación digital. Un [estudio reciente](#) reveló que más del 80 % de las organizaciones encuestadas se enfrentaban a problemas con API de terceros, lo que destacaba la importancia de adoptar un modelo de seguridad Zero Trust. Aunque esta vulnerabilidad por sí sola puede no ser inmediatamente catastrófica, puede convertirse en una amenaza de seguridad importante cuando se combina con otras debilidades, como una validación deficiente o dependencias poco seguras. Por ejemplo, una API financiera que confíe en transacciones de terceros no verificadas podría dar lugar a infracciones de seguridad.



Las alertas de seguridad relacionadas con la norma PCI DSS y el RGPD aumentaron un 16 % y un 21 %, respectivamente, mientras que las alertas relacionadas con la norma ISO 27001 aumentaron un 22 %.

Garantía de cumplimiento de las API

Entre las prácticas recomendadas para garantizar el cumplimiento de las API se incluyen etiquetar cada alerta con los estándares normativos y de cumplimiento específicos que infrinja, lo que proporciona a las organizaciones información inmediata sobre los problemas de cumplimiento críticos y proporciona orientación práctica para abordarlos. Este enfoque proactivo ayuda a las organizaciones a mantener el cumplimiento normativo, lo que reduce el riesgo de multas y otras repercusiones legales, así como daños a la reputación que pueden provocar pérdidas financieras significativas. Por ejemplo, [una aerolínea se enfrentó a una multa de 20 millones de libras](#) después de que una vulnerabilidad de API revelara los datos de 400 000 clientes, lo que pone de manifiesto las graves consecuencias de una seguridad inadecuada de las API según el RGPD.

Las normas de cumplimiento sirven como mecanismos de protección esenciales para que las organizaciones protejan tanto los datos confidenciales como a sus clientes y cumplan las obligaciones legales y normativas. Normas como la PCI DSS, el RGPD y la Ley de Transferibilidad y Responsabilidad de Seguros Médicos (HIPAA) requieren el tratamiento seguro de información confidencial, como datos de pago e información de identificación personal. Según nuestro análisis de datos, las alertas de seguridad relacionadas con la norma PCI DSS y el RGPD aumentaron un 16 % y un 21 %, respectivamente, mientras que las alertas relacionadas con la norma ISO 27001 aumentaron un 22 %.

RGPD

El RGPD hace hincapié en la integración de la protección de datos y la privacidad del cliente a lo largo de todo el ciclo de vida de las API. Esto implica un diseño seguro, una autenticación y autorización sólidas, limitación de velocidad, pruebas periódicas de vulnerabilidad, cifrado y evaluaciones de riesgos continuas, incluso durante las primeras etapas de desarrollo. Estas medidas garantizan la confidencialidad, integridad y disponibilidad de los datos.

PCI DSS

Del mismo modo, la [PCI DSS](#) hace hincapié en la protección de las API que gestionan los datos de las tarjetas de pago mediante la integración de la seguridad en las fases de diseño, codificación y prueba. Exige la protección contra vulnerabilidades web y pruebas periódicas para identificar y solucionar los fallos de seguridad.

Los requisitos 10 y 11 exigen específicamente un registro y una supervisión completos de las actividades de API, incluidas las solicitudes, las respuestas, los intentos de autenticación y los cambios en el sistema. Los registros se deben conservar durante al menos 12 meses y a los tres meses más recientes se debe poder acceder fácilmente para su análisis. Además, recomienda que las organizaciones realicen análisis externos de vulnerabilidades después de cambios significativos. Para garantizar el cumplimiento de la norma PCI, las organizaciones deben implementar controles estrictos, como la limitación de velocidad, el registro, el control de acceso por roles (RBAC) y la gestión de sesiones para garantizar que las API sean resistentes a amenazas y riesgos.



ISO 27001

La norma ISO 27001 proporciona un marco sólido para gestionar de forma eficaz los riesgos de seguridad de la información, mejorar la estrategia de seguridad de una organización y generar confianza entre compañeros y clientes. Las prácticas recomendadas incluyen:

- Implementar el control de acceso (por ejemplo, claves de API) para verificar la identidad de los usuarios
- Utilizar el cifrado de datos de extremo a extremo
- Supervisar las API para detectar comportamientos anómalos
- Llevar a cabo evaluaciones de riesgos exhaustivas para identificar posibles vulnerabilidades de API

Estos requisitos de cumplimiento resaltan la intersección crítica entre la seguridad de las API y los marcos normativos. Una implementación adecuada no solo protege los datos confidenciales, sino que también cumple varias normativas de forma simultánea. Para obtener más información sobre las normas globales existentes y emergentes, vaya a la sección [Cumplimiento](#) de este informe.

Brechas de visibilidad de las API: los pasajes ocultos a los datos

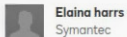
Abuso de las API

En noviembre de 2024, [Bleeping Computer informó](#) de un importante ataque contra un proveedor de soluciones de firma electrónica. Los atacantes aprovecharon un componente fundamental de la API de seguimiento y gestión de documentos del proveedor, lo que les permitió enviar facturas fraudulentas a numerosas víctimas potenciales. Si los destinatarios firmaban involuntariamente estos documentos, los atacantes podían solicitar pagos a diversas organizaciones.

Este incidente subraya el impacto pernicioso del uso indebido de API: los agentes maliciosos pueden explotar las API más allá de su diseño previsto y transformarlas en canales no intencionados de ataques. La aparición de la IA generativa ha agravado aún más estos riesgos al automatizar la detección de vulnerabilidades y las derivaciones de limitación de frecuencia, lo que facilita ataques más rápidos y sofisticados.

Fuente: BleepingComputer/Wallarm

Please Review & Act on These Documents



Elaine Harris
Symantec

Norton
Receipts & Invoice
[View More](#)

Norton
Internet Security
Powered by [docusign](#)

Please review the documents below.

[CONTINUE](#)

[OTHER ACTIONS](#)

Signature
 Initial
 Stamp
 Date Signed

Name
 First Name
 Last Name
 Email Address
 Company
 Title

- Comprehensive protection against viruses and malware
- Identity theft protection
- Performance optimization tools
- 24/7 customer support

DETAILS:

PRODUCT	TENURE	AMOUNT
Norton LifeLock 360	2 Users/1 Year	249.00 USD
	Activation Charges	49.00 USD
TOTAL		298.00 USD

POLICY:

We understand that circumstances can change and you may need to cancel your subscription. We

Desafíos en la detección del uso indebido de API

Los equipos de seguridad se enfrentan a importantes obstáculos a la hora de detectar el uso indebido de API, principalmente debido a la necesidad de establecer una referencia de comportamiento normal frente al comportamiento sospechoso. Este desafío pone de relieve la necesidad fundamental de supervisar el comportamiento en tiempo real para identificar anomalías y amenazas de forma preventiva.

Nuestro [estudio sobre el impacto de la seguridad de API de 2024](#) revela una tendencia preocupante: solo el 13 % de las organizaciones encuestadas prueban sus API a diario, lo que supone una disminución notable con respecto al 37 % de 2023. Esta disminución es especialmente alarmante dado el panorama actual de amenazas. La reducción drástica de las pruebas diarias de API expone a las organizaciones a mayores riesgos de seguridad, ya que disminuye significativamente su capacidad para detectar y responder a las amenazas en rápida evolución, lo que podría dejar sin atender vulnerabilidades críticas durante periodos prolongados.

Las pruebas automatizadas frecuentes durante los ciclos de desarrollo permiten a las organizaciones identificar y resolver los problemas con antelación, lo que evita costosas correcciones en los entornos de producción. En una época en la que la explotación de API emplea cada vez más métodos automatizados y encubiertos, las pruebas proactivas desempeñan un papel fundamental a la hora de mitigar los riesgos.

API no gestionadas: API zombis y en la sombra

La visibilidad del estado de las API sigue siendo un reto fundamental para las organizaciones, y abarca tanto el seguimiento oficial de las API como la identificación de datos confidenciales. El [estudio sobre el impacto de la seguridad de API de 2024](#) revela una importante brecha: El 47 % de los equipos responsables de la seguridad de las aplicaciones mantienen inventarios completos de API, pero no identifican las API que gestionan datos confidenciales. Los profesionales sénior de seguridad informan de limitaciones similares y el 42 % de ellos se enfrentan a este problema de supervisión. Resulta alarmante que el número de empresas con inventarios completos de API y conocimiento de la exposición de datos confidenciales ha disminuido del 40 % en 2023 al 27 % en 2024. El estudio sobre el impacto de la seguridad también destaca las API zombi y en la sombra como una de las principales causas de los incidentes de seguridad de las API.

Los inventarios incompletos suelen omitir las API zombi y en la sombra. Las API zombi (es decir, interfaces obsoletas que siguen activas debido a una retirada incompleta, a la rotación de personal o a otras razones) crean vectores de ataque vulnerables. Las API en la sombra (aquellas desarrolladas como soluciones rápidas fuera de los procesos de aprobación estándar) plantean amenazas comparables. [Según el estudio](#), un tercio de las transacciones de API maliciosas va dirigido a API ocultas.

Las medidas de seguridad tradicionales, como los firewalls de aplicaciones web (WAF), no resultan adecuadas para estas amenazas. Las organizaciones necesitan soluciones avanzadas de detección y supervisión de API para identificar los terminales vulnerables de forma eficaz.

Un inventario completo de API constituye la piedra angular de una estrategia de seguridad eficaz, ya que permite a las organizaciones supervisar los patrones de uso, realizar un seguimiento de los historiales de versiones, identificar vulnerabilidades y satisfacer los requisitos normativos y de cumplimiento. Este enfoque estratégico proporciona una visibilidad clara de la infraestructura digital de una organización, lo que en última instancia puede reforzar la gestión de riesgos y mejorar la estrategia de seguridad general.

En el punto de mira

En el primer trimestre de 2025, detectamos un ataque a una empresa de comercio electrónico a través del uso indebido de API. La API de envío de SMS de la empresa carecía de una autenticación adecuada, lo que permitía a los atacantes explotarla utilizando más de 200 direcciones IP diferentes, un solo token de autenticación, y numerosos números móviles aleatorios (tanto legítimos como falsos).

La estrategia de ataque fue sencilla, pero eficaz: saturar a la empresa registrando varios números de móvil y enviando mensajes SMS a números fraudulentos para causar directamente daños financieros. Cuando los atacantes registraban un número de móvil, la empresa afectada, que paga por un servicio de puerta de enlace SMS para facilitar la mensajería de texto entre sus aplicaciones y dispositivos móviles, incurría en gastos financieros inesperados que podían dañar su marca o su reputación. Una estrategia de defensa en profundidad con varias capas de medidas de seguridad puede contrarrestar este tipo de ataque y mitigar significativamente los riesgos asociados.

Nuestras alertas revelaron que los atacantes enviaron 11 057 solicitudes POST durante este ataque, de las cuales 5659 tuvieron éxito en las respuestas (Figura 2).

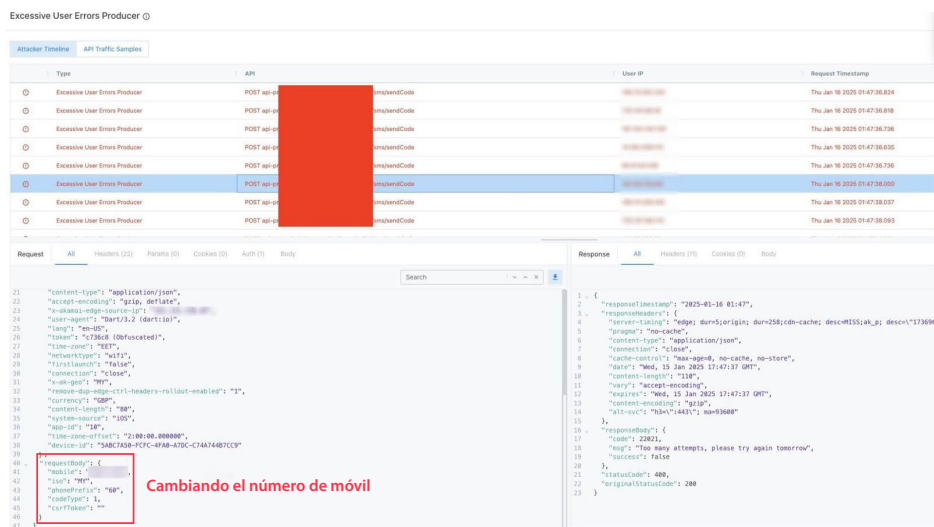


Fig. 2: Los atacantes inundan la API no segura con solicitudes

Estas solicitudes automatizadas eran idénticas, con la excepción de un parámetro crítico:

Body param **mobile**: the following pattern is detected - **<number>**

Dichas solicitudes pueden sobrecargar el servidor y provocar una denegación de servicio, o bien indicar un acceso no autorizado a la API. Los WAF tradicionales carecen de la capacidad de detectar estos sofisticados ataques. Sin embargo, las soluciones de seguridad de API avanzadas que crean una referencia de comportamiento normal de las API pueden identificar dichos ataques mediante el análisis del comportamiento, mitigar los riesgos de forma proactiva y evitar que los atacantes causen más daños.

Ataques web: comparación y tendencias interanuales

La investigación de Akamai reveló un aumento sustancial de los ataques web dirigidos a aplicaciones web y API durante el periodo analizado de enero de 2023 a diciembre de 2024 (Figura 3). El volumen mensual de ataques aumentó de casi 14 000 millones a principios de 2023 a más de 29 000 millones en octubre de 2024. Esto representa un crecimiento del 65 % en los ataques web entre el primer trimestre de 2023 y el cuarto trimestre de 2024.

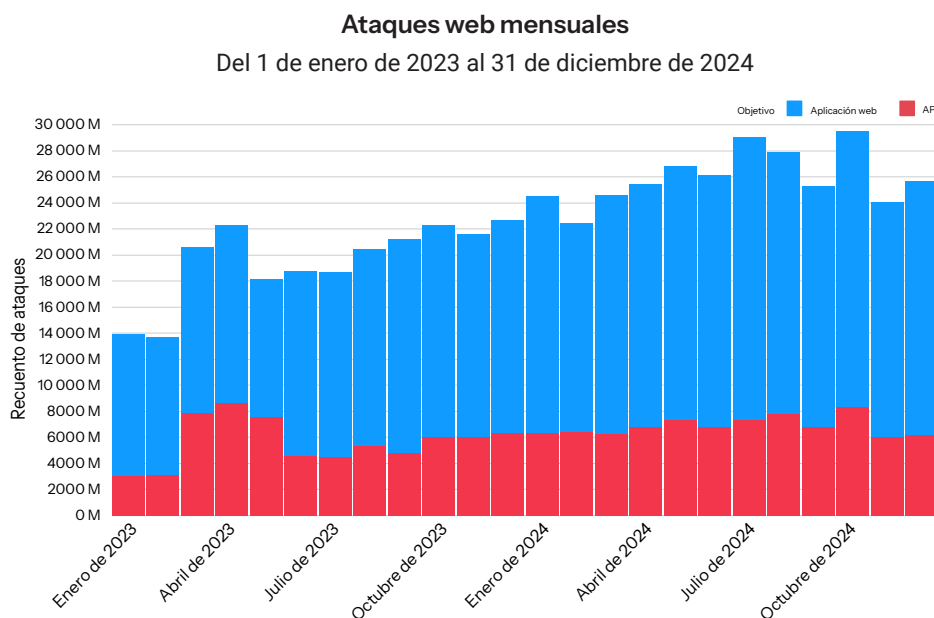


Fig. 3: Los ataques web tradicionales dirigidos a aplicaciones web y API siguen aumentando, con un crecimiento del 65 % entre el primer trimestre de 2023 y el cuarto trimestre de 2024

Principales vectores: una combinación de riesgos tradicionales y modernos basados en el comportamiento

Los profesionales de la ciberseguridad se enfrentan a una complejidad cada vez mayor al proteger la infraestructura digital de sus organizaciones frente a una serie de amenazas, que van desde ataques web tradicionales hasta ataques modernos dirigidos a vulnerabilidades y errores de configuración inherentes.

Violaciones de restricciones de solicitudes de API: una amenaza creciente

Un análisis exhaustivo de los terminales de API durante un periodo de dos años revela que las infracciones de restricciones de solicitudes de API son un motivo de preocupación para las organizaciones (Figura 4). Estas violaciones se manifiestan cuando las solicitudes o las respuestas no cumplen los parámetros predefinidos o los requisitos establecidos, como superar los límites de velocidad o enviar entradas de datos no válidas.

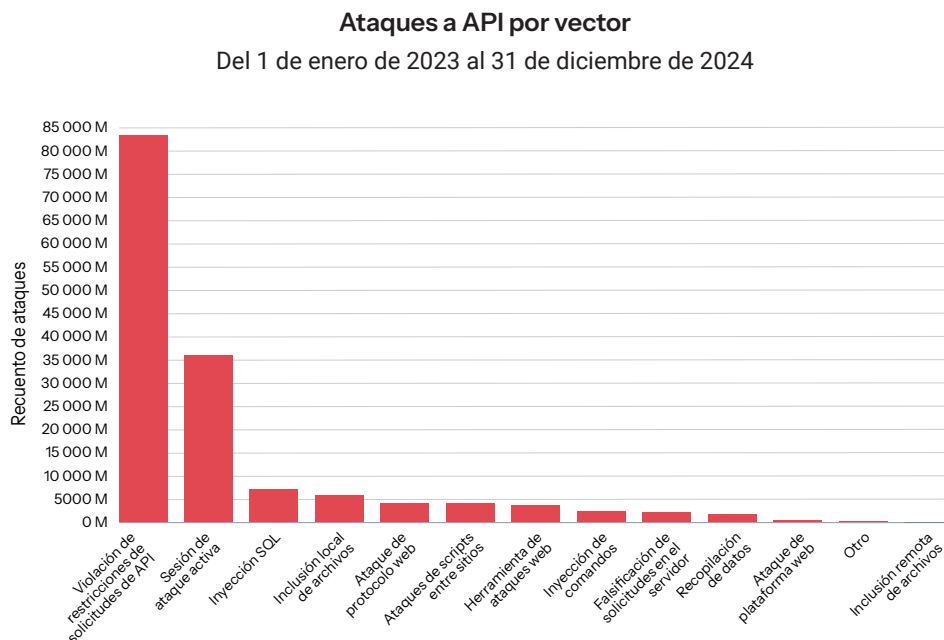


Fig. 4: En dos años se registraron más de 83 000 millones de violaciones de restricciones de solicitudes

Las violaciones de restricciones de solicitudes de API suponen una amenaza creciente, con más de 83 000 millones de ataques registrados en un periodo de dos años. Este vector de ataque experimentó un aumento sustancial del 24 % de 2023 a 2024, lo que subraya los peligros del uso indebido de API. La prevalencia de estas violaciones es un indicador crítico de un posible uso indebido de API, que puede precipitar una cascada de efectos adversos, incluida la degradación del rendimiento del sistema, las interrupciones del servicio y el aumento de la vulnerabilidad a los ataques dirigidos.

Sesiones de ataque activas: ataques únicos que requieren una solución creativa

Las soluciones de Akamai emplean herramientas de seguridad innovadoras para hacer frente a los desafíos únicos que plantean los ataques específicos a las API. La base de estas soluciones es un mecanismo patentado para detectar sesiones de ataque activas, que sirve como herramienta de defensa estratégica. Este sistema utiliza la propia inteligencia sobre amenazas de Akamai para identificar y realizar un seguimiento de comportamientos sospechosos, lo que permite a las organizaciones frustrar las amenazas de forma proactiva antes de que se conviertan en ataques a gran escala.

El sistema identifica a los atacantes y aplica un enfoque de "área de penalización". Cuando se trata de ataques modernos, los adversarios utilizan principalmente la automatización para ejecutar sus reconocimientos y ataques. Akamai identifica rápidamente estas sesiones de búsqueda de vulnerabilidades, reacciona bloqueando el cliente temporalmente y las etiqueta como sesiones de ataque activas. Esta estrategia impide de forma eficaz a los posibles atacantes realizar tareas de reconocimiento y explotar vulnerabilidades de la red.

Al limitar la oportunidad para los agentes maliciosos, las organizaciones pueden reforzar sustancialmente su estrategia de seguridad de API. Este enfoque proporciona una protección sólida contra una amplia variedad de posibles ataques y mejora significativamente la resiliencia general de la ciberseguridad.

La importancia de esta estrategia es evidente en nuestros datos. Las sesiones de ataque activas encabezaron la clasificación general tanto para aplicaciones web como para API (Figura 5). En 2023, representó más de 69 000 millones de ataques. Esta cifra aumentó a más de 113 000 millones de ataques en 2024, lo que supone un notable aumento interanual del 63 %.

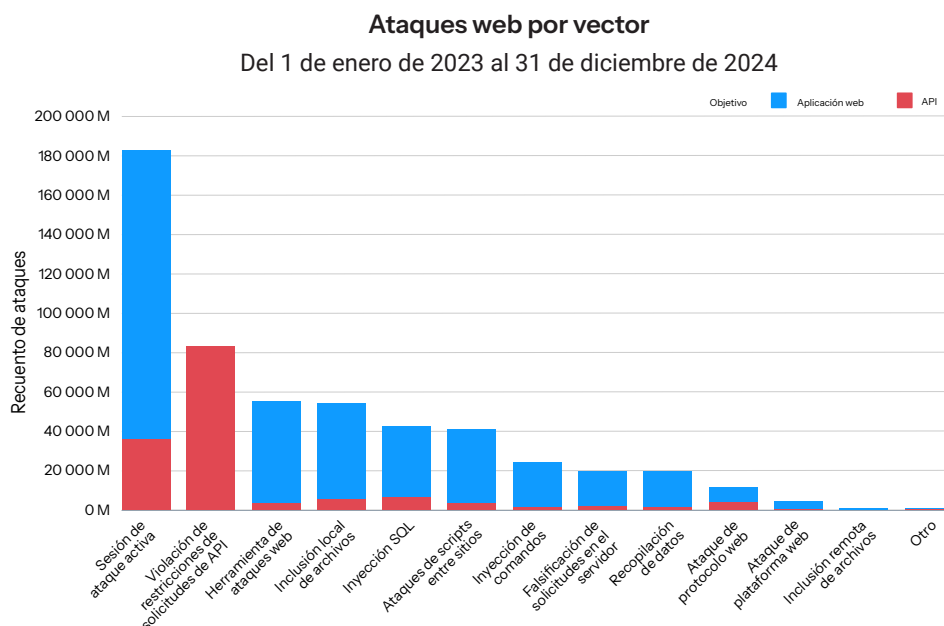


Fig. 5: La sesión de ataque activa supera con creces a los demás vectores, tanto para aplicaciones web como para API, lo que pone de manifiesto la incesante búsqueda de vulnerabilidades por parte de los atacantes en las redes de sus objetivos

Por qué no podemos ignorar las vulnerabilidades web tradicionales en la infraestructura moderna

Los ataques de inyección siguen demostrando una alta eficacia a pesar de la aparición de sofisticadas metodologías de ataque basadas en el comportamiento y una mayor concienciación sobre las vulnerabilidades web tradicionales. Nuestros datos de enero de 2023 a diciembre de 2024 indican un aumento significativo del volumen de ataques. La inyección de lenguaje de consulta estructurado (SQLi) y la inyección de comandos experimentaron un crecimiento interanual del 60 % y del 34 %, respectivamente. Estas vulnerabilidades permiten a los agentes maliciosos ejecutar comandos no autorizados, poner en peligro la integridad del sistema y acceder a datos confidenciales sin una autenticación adecuada, lo que pone de relieve su importancia continua en el dominio de la ciberseguridad.

La prevalencia duradera de las bases de datos SQL, conocidas por su almacenamiento de datos fiable y escalable, contribuye a que estos sistemas sean un objetivo persistente. En particular, las [cuatro bases de datos más utilizadas](#) emplean arquitecturas basadas en SQL, lo que subraya aún más la naturaleza crítica de este vector de ataque.

Aunque la lista de los 10 principales riesgos de seguridad de las API según OWASP se ha sometido a revisiones, como la sustitución de los ataques de inyección por errores de configuración de seguridad en su actualización de 2023, el riesgo asociado a los ataques de inyección sigue siendo primordial. Al mismo tiempo, otros vectores establecidos, como la inclusión de archivos locales (LFI) y los scripts entre sitios (XSS), siguen manifestándose en grandes volúmenes. [La guía de los defensores de 2025](#) aclara la sofisticación de las técnicas de ataques de XSS (como la inyección de recursos remotos, el robo de cookies, la desfiguración en los sitios web y la falsificación de sesiones) basándose en ataques reales observados en 2024.

Estos hallazgos subrayan el imperativo de implementar estrategias de defensa multicapa. Los profesionales de la ciberseguridad deben emplear una combinación de codificación de salida adecuada, políticas sólidas de seguridad del contenido y WAF avanzados para contrarrestar eficazmente estos ataques cada vez más sofisticados.

Ataques DDoS de capa 7: comparación y tendencias interanuales

Entre enero de 2023 y diciembre de 2024, la investigación de Akamai registró un aumento espectacular de los ataques DDoS de capa 7 (capa de aplicación) contra aplicaciones web y API (Figura 6). Los ataques mensuales aumentaron vertiginosamente de algo más de 500 000 millones a principios de 2023, a más de 1,1 billones en diciembre de 2024. Esto representa un crecimiento del 94 % en los ataques DDoS de capa 7 entre el primer trimestre de 2023 y el cuarto trimestre de 2024.

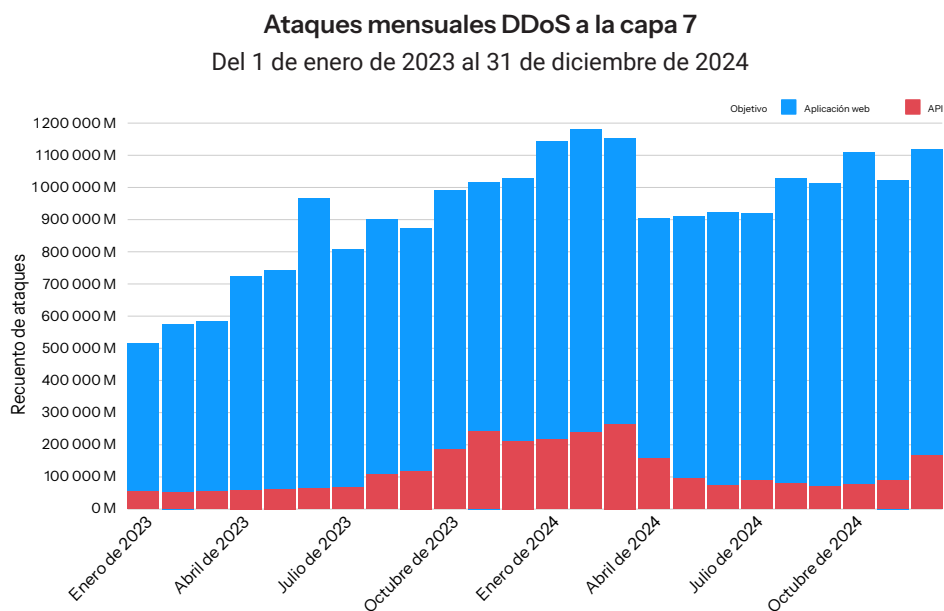


Fig. 6: El número de ataques DDoS de capa 7 dirigidos a aplicaciones web y API sigue creciendo, con un aumento del 94 % entre el primer trimestre de 2023 y el cuarto trimestre de 2024

Ataques DDoS de capa 7 a aplicaciones y API

Las [inundaciones HTTP](#) persisten como principal vector de amenaza en la evolución continua de los ataques DDoS de capa 7 dirigidos a aplicaciones web y terminales de API. Estos ataques saturan los recursos de API al inundarlos con grandes volúmenes de solicitudes aparentemente legítimas que se centran en operaciones que consumen muchos recursos. Los atacantes han perfeccionado sus técnicas, creando ataques DDoS de capa 7 que aprovechan vulnerabilidades específicas en la lógica de aplicaciones web o API, lo que complica las medidas de detección y mitigación. Además, los ataques basados en bots son cada vez más sofisticados y generan patrones de tráfico que emulan con gran precisión el uso legítimo de las API.

La transmisión de la IA de los atacantes: Conducción manual o automática por el camino de las API

Las tecnologías de IA generativa han revolucionado la integración empresarial a través de las API, lo que está "impulsando" la adopción generalizada y la aplicación práctica de las API. Se prevé una [enorme expansión](#), del mercado de API con IA, en concreto, que pase de 44 410 millones de dólares en 2025 a 179 140 millones de dólares en 2030, lo que supone una tasa de crecimiento anual compuesto del 32,2 %. No obstante, el aumento de la adopción de la IA ha coincidido con un número cada vez mayor de [ataques con IA a API](#). El aumento de las vulnerabilidades de API expuestas se puede atribuir en gran medida a los atacantes que utilizan la IA como herramienta tanto para el reconocimiento como para la explotación, ya sea manual o automáticamente.

Estrategias de ataque a API basadas en IA

-  **Selección estratégica de objetivos:** los atacantes utilizan herramientas de IA para identificar y analizar componentes específicos en las API objetivo y [generar código malicioso por IA](#) para aprovechar vulnerabilidades específicas. Este enfoque permite ataques precisos y eficaces contra las debilidades de las API.
-  **Ataques automatizados:** mediante la automatización del proceso de ataque, los ciberdelincuentes reducen considerablemente su tiempo y esfuerzo, al identificar y aprovechar rápidamente las debilidades de seguridad de las API. Esta automatización suele implicar [bots basados en IA](#) que suponen una amenaza crítica tanto para las empresas como para las personas.
-  **Ataques volumétricos:** los atacantes utilizan la IA para saturar las API con tráfico, lo que inunda los sistemas de seguridad con un volumen y una velocidad considerables. Los [ataques DDoS automatizados](#) ejemplifican esta estrategia en la que los bots basados en IA lanzan ataques continuos, al mismo tiempo que se adaptan dinámicamente a las medidas defensivas.
-  **Ataques basados en el comportamiento:** la IA analiza los patrones de tráfico para crear [ataques de actividad baja y lenta](#) que evaden la detección al mantenerse por debajo de los umbrales de alerta típicos. Estos ataques suelen tener como objetivo vulnerabilidades comunes de API, como la autenticación BOLA y la autenticación comprometida.

La ironía de las API basadas en IA

Paradójicamente, las API basadas en IA han demostrado ser notablemente inseguras. La mayoría de las [API basadas en IA](#) son accesibles externamente y una parte importante depende de mecanismos de autenticación inadecuados, lo que las hace más vulnerables a los ataques. Nuestro [Estudio sobre el impacto de la seguridad de API de 2024](#) reveló que las API de las herramientas de IA generativa eran la principal causa de los incidentes de API notificados por los equipos de seguridad de comercio electrónico y del sector retail.

Panorama de amenazas impulsadas por IA en constante cambio

Los avances en la tecnología de IA han contribuido significativamente al cambiante panorama de amenazas para las API. En el último año se han registrado [aumentos récord](#) en las vulnerabilidades de API basadas en IA, y hay fuentes que afirman que, por primera vez, la mayoría de las [vulnerabilidades explotadas](#) registradas por la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) de EE. UU. estaban relacionadas con API.

Ataques a aplicaciones web basados en IA y estrategias de defensa

La influencia de la IA en la seguridad de las aplicaciones web mediante la introducción de nuevos vectores de ataque y capacidades defensivas también ha sido profunda. Entre las áreas clave en las que la IA ha alterado considerablemente el panorama de la ciberseguridad para los ataques a aplicaciones web se incluyen el malware mejorado con IA, el análisis de vulnerabilidades basado en IA, los ataques a sistemas con IA integrada, el scraping web avanzado y los sistemas de WAF basados en IA.

Malware mejorado con IA

Los expertos en ciberseguridad han observado que el malware avanzado utiliza la IA para atacar aplicaciones web. En una campaña de correo electrónico de 2024 dirigida a usuarios franceses, los atacantes implementaron código malicioso, probablemente diseñado con ayuda de la IA generativa, para ejecutar el [malware AsyncRAT](#). Este ejemplo destaca la creciente tendencia de la creación e implementación de malware asistido por IA, que plantea nuevos desafíos para los profesionales de la seguridad de aplicaciones web.

Análisis de vulnerabilidades basado en IA

La IA ha revolucionado el [análisis de vulnerabilidades](#) de las aplicaciones web, ya que ofrece capacidades defensivas y ofensivas, tanto para uso beneficioso como malicioso. Estas herramientas basadas en IA ahora automatizan las búsquedas de vulnerabilidades comunes, como SQLi, XSS, falsificación de solicitudes entre sitios y falsificación de solicitudes en el servidor (SSRF). Además, realizan análisis basados en IA de posibles impactos y generan recomendaciones basadas en IA para los pasos de corrección.

Ataques a sistemas con IA integrada

La integración de la IA, en particular los modelos de lenguaje de gran tamaño (LLM), en las aplicaciones web ha introducido [nuevas vulnerabilidades de seguridad](#). *Los ataques de inyección de instrucciones* se dirigen a los sistemas de IA para anular las protecciones del modelo. Un ejemplo destacado es una [vulnerabilidad de la IA de Slack](#) (ya corregida) que permitió la recopilación de datos de canales privados a través de la inyección indirecta de instrucciones. *Los ataques de envenenamiento de datos* corrompen el comportamiento del modelo de IA mediante la manipulación de un pequeño porcentaje de conjuntos de datos, lo que podría comprometer la integridad del sistema. *Las técnicas de jailbreak* eluden las medidas de protección de LLM, lo que permite a los atacantes anular las restricciones, extraer datos confidenciales y producir resultados perjudiciales. Estos vectores de ataque emergentes requieren una mayor vigilancia y nuevas estrategias de defensa.

Scraping web sofisticado

La IA ha mejorado las capacidades de scraping web, lo que crea nuevos desafíos para la seguridad de las aplicaciones web. Estas herramientas de scraping basadas en IA ahora ofrecen métodos de extracción de datos más eficaces y una evasión mejorada de las medidas antiscraping. Desde principios de la década de 2020, el [scraping web sofisticado](#) ha estado utilizando la IA para procesar datos, pero recientemente ha habido un aumento sustancial en la frecuencia del scraping de LLM. Gran parte de esto se debe al aumento de las consultas basadas en agentes, que está impulsando la demanda de fuentes de datos en tiempo real (no estáticas).

Lamentablemente, esto ha llevado a que una solicitud de una aplicación web (en función de factores como la complejidad de la solicitud, la infraestructura de alojamiento, etc.) cueste, de media, entre 0,01 y 0,50 dólares. Y aunque el comercio fue el sector más afectado inicialmente por el aumento del scraping de LLM, la tendencia ha cambiado: otros sectores (por ejemplo, servicios financieros, juegos de apuestas, medios digitales y medios audiovisuales) han sufrido ahora la peor parte de este cambio.

Sistemas de WAF basados en IA

Un aspecto positivo es que los sistemas de WAF avanzados se basan en la IA para identificar y mitigar de forma más eficaz una serie de ciberamenazas, como bots, ataques DDoS, scrapers y análisis. Los [sistemas de WAF basados en IA](#) ayudan a combatir los ciberataques sofisticados, ya que los WAF tradicionales con conjuntos de reglas estáticas se enfrentan a amenazas de día cero y requieren actualizaciones manuales.

La estrategia de aprendizaje automático multicapa permite el reconocimiento de patrones, el aprendizaje adaptable, la detección de anomalías y la mejora del tiempo de respuesta. Con el aprendizaje basado en miles de millones de eventos diarios y la implementación de un enfoque por capas con una supervisión continua, los sistemas de WAF basados en IA tienen como objetivo prevenir de forma proactiva las amenazas en constante evolución y mantener a los clientes protegidos.

Tendencias por sectores

Entre los sectores, el comercio superó con creces a los demás en cuanto al número de ataques web en general registrados entre el primer trimestre de 2023 y el cuarto trimestre de 2024, y triplicó las cifras del sector de la alta tecnología (el segundo sector más atacado) (Figura 7). Además, el número de ataques de API experimentados por el sector del comercio durante el mismo periodo superó en gran medida al total de ataques de API de los otros 10 sectores principales.

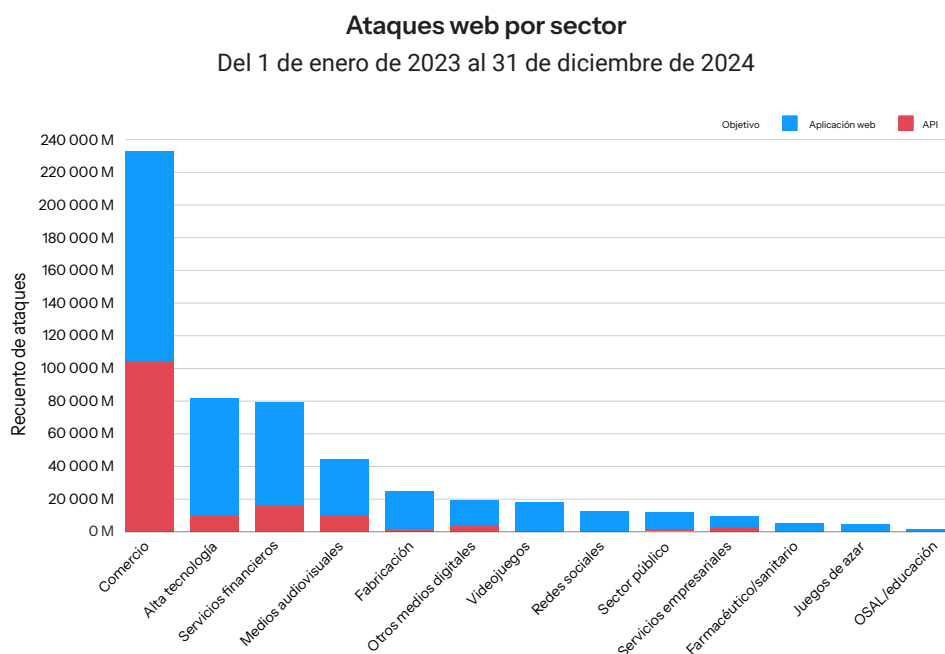


Fig. 7: El comercio, la alta tecnología y los servicios financieros fueron los tres sectores más afectados por los ataques web

En el caso de los ataques DDoS de capa 7 (capa de aplicación), el sector de la alta tecnología se vio más afectado que cualquier otro, con más de 7 billones de ataques durante el periodo comprendido entre el primer trimestre de 2023 y el cuarto trimestre de 2024. A la alta tecnología le siguieron las redes sociales y el comercio (Figura 8). Sin embargo, durante el mismo periodo de tiempo, el número de ataques DDoS de capa 7 dirigidos a API en el sector del comercio una vez más superó considerablemente al de todos los demás sectores juntos.

Ataques DDoS de capa 7 por sector

Del 1 de enero de 2023 al 31 de diciembre de 2024

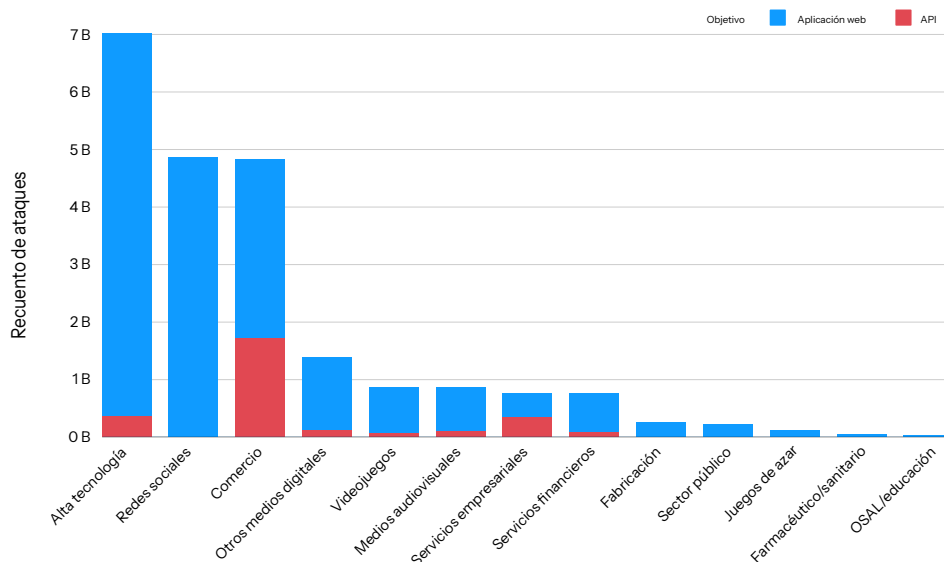


Fig. 8: Ataques DDoS de capa 7 por sector

Comercio

Además de sufrir más de 230 000 millones de ataques web (más del 40 % del total) entre 2023 y 2024, el sector del comercio se enfrentó a una escala sin precedentes de ataques DDoS de capa 7, y los datos de Akamai revelaron más de 4,8 billones de ataques durante 2023 y 2024.

Este volumen combinado representa un patrón de selección estratégica en el que las aplicaciones web absorben aproximadamente el 64,25 % de los ataques, mientras que las API representan el 35,75 % restante. Esta distribución refleja los vectores duales que utilizan los atacantes para atentar contra las plataformas comerciales y resalta la naturaleza polifacética del panorama de amenazas actual.

Las entidades comerciales representan objetivos especialmente lucrativos debido a su concentración de datos confidenciales de clientes, información de pago y transacciones financieras. El camino directo hacia la monetización a través del robo de credenciales de pago, cuentas de clientes comprometidas y PII confidencial crea incentivos financieros inmediatos para los atacantes. A diferencia de algunos sectores en los que los datos comprometidos requieren pasos adicionales para convertirlos en beneficios financieros, las plataformas comerciales suelen proporcionar a los atacantes activos directamente explotables.

El sector del retail como objetivo principal

El sector del retail es el segmento más afectado dentro del sector del comercio en general y se enfrenta a volúmenes de ataques desproporcionados debido a varias características distintivas.

Las operaciones de retail suelen mantener ecosistemas digitales complejos, que incorporan varias plataformas y sistemas. Sus agresivas iniciativas de transformación digital a menudo priorizan la velocidad de comercialización en lugar de la seguridad integral, lo que crea brechas de seguridad. La adopción de estrategias omnicanal aumenta involuntariamente la complejidad de la superficie de ataque. Además, la amplia dependencia de proveedores externos crea una compleja cadena de suministro con numerosos vectores de riesgo potenciales.

Según el Internet Crime Complaint Center del FBI, los patrones de tráfico estacionales crean periodos predecibles de gran volumen que los atacantes aprovechan para lanzar sus ataques. Los incidentes de ciberdelincuencia se disparan **entre un 25 % y un 30 %** durante la temporada navideña. Las plataformas de comercio electrónico también se enfrentan a mayores amenazas, con un aumento del **31 %** en los ciberataques durante diciembre en comparación con la media anual.

La evolución de los ataques a aplicaciones web

Los ataques a aplicaciones web están experimentando una importante transformación, impulsada por los avances tecnológicos y las cambiantes metodologías de los atacantes. Los atacantes utilizan técnicas cada vez más sofisticadas para aprovechar las vulnerabilidades de las aplicaciones web y adaptan sus estrategias para eludir las medidas de seguridad en constante evolución. El auge de las herramientas de ataque automatizadas, junto con la integración de algoritmos de aprendizaje automático, ha permitido a los atacantes lanzar campañas más precisas y dirigidas contra las aplicaciones web de los retailers.

Además, el cambio hacia arquitecturas de microservicios y hacia el desarrollo basado en API ha ampliado la superficie de ataque, lo que ha obligado a replantearse los paradigmas de seguridad tradicionales. Esta evolución exige un enfoque proactivo por parte de los profesionales de la ciberseguridad, que haga hincapié en la supervisión continua, los mecanismos de defensa adaptable y un profundo conocimiento de los vectores de ataque emergentes en el panorama de las aplicaciones web.

El panorama de amenazas de bots

El panorama de amenazas de bots está evolucionando rápidamente con los avances tecnológicos, especialmente en el caso de los atacantes que integran capacidades de IA generativa. Esta evolución ha mejorado las estrategias de ataque mediante ataques de día cero más rápidos y sofisticadas técnicas de evasión que eluden las defensas tradicionales. Las pruebas demuestran que los ataques de fraude de bots basados en IA contra los retailers **aumentaron** de forma constante entre agosto de 2022 y abril de 2024, con un impresionante aumento del 137 % en enero de 2024. Los desafíos que supone la detección agravan aún más estas amenazas, ya que las empresas suelen tardar cuatro meses en identificar los ataques de bots, tiempo durante el cual sufren pérdidas financieras y daños a la reputación.



Los bots ahora funcionan como vectores centrales en el panorama de las ciberamenazas al sector del retail, lo que facilita el robo de cuentas, el fraude con tarjetas de crédito y el uso indebido de tarjetas regalo. Actúan como facilitadores en campañas de ataque más amplias, ya que utilizan datos robados de un sitio afectado para impulsar ataques de Credential Stuffing contra otros, lo que crea un efecto multiplicador en los ecosistemas de retail. Esta actividad contribuye a la "industrialización" del fraude online, ya que las redes criminales globales utilizan herramientas automatizadas para ampliar las operaciones mucho más allá de lo que los métodos manuales podrían lograr.

Para obtener una lista de recomendaciones sobre cómo proteger mejor las API y las aplicaciones web de su negocio de retail frente a ataques relacionados con la IA y los bots, vaya a la sección [Mitigación](#).

Servicios financieros

El sector de los servicios financieros se ha convertido en uno de los principales objetivos de los ataques web y sigue registrando ataques DDoS de capa 7. Los ataques web ascendieron a más de 79 000 millones entre enero de 2023 y diciembre de 2024, mientras que los ataques DDoS de capa 7 sumaron más de 761 000 millones, tanto contra aplicaciones web como contra API, durante el mismo periodo.

Este volumen sin precedentes pone de relieve la vulnerabilidad y el atractivo del sector para los atacantes. Varios factores impulsan este aumento, entre ellos el papel crítico del sector en la infraestructura económica global, el alto valor de los datos financieros y el potencial de causar [interrupciones](#) significativas.

Digitalización de los servicios financieros

La digitalización de los servicios financieros ha ampliado la superficie de ataque para los ciberdelincuentes. La adopción de soluciones de personalización basadas en IA, banca como servicio y finanzas integradas ha introducido nuevas vulnerabilidades. Los conflictos geopolíticos, en particular la guerra entre Rusia y Ucrania, han impulsado actividades hacktivistas [dirigidas a](#) las instituciones financieras. Los factores económicos, como el auge de las criptomonedas y la posible implementación de una reserva de estas, han aumentado el [interés](#) de los atacantes por el sector financiero.

Los ataques a aplicaciones web se están transformando rápidamente, adaptándose a las nuevas tecnologías y explotando las vulnerabilidades emergentes. Los atacantes utilizan ahora sofisticados algoritmos de inteligencia artificial y aprendizaje automático para eludir las medidas de seguridad tradicionales y lanzar ataques más dirigidos y persistentes. El aumento de las arquitecturas sin servidor y los microservicios ha creado nuevos vectores de ataque, mientras que el creciente uso de API ha ampliado los posibles puntos de entrada de los agentes maliciosos. Además, el cambio hacia las aplicaciones móviles y basadas en la nube ha requerido replantearse las estrategias de seguridad, ya que estas plataformas presentan desafíos únicos en cuanto a la protección de datos y el control de acceso.

Prominencia del segmento bancario como objetivo de ataque

Dentro del sector de los servicios financieros, la banca destaca como el segmento que sufre más ataques web (Figura 9). Al igual que en el sector del comercio, los ataques de [Credential Stuffing](#) también están surgiendo como uno de los principales vectores de amenazas en el sector bancario.

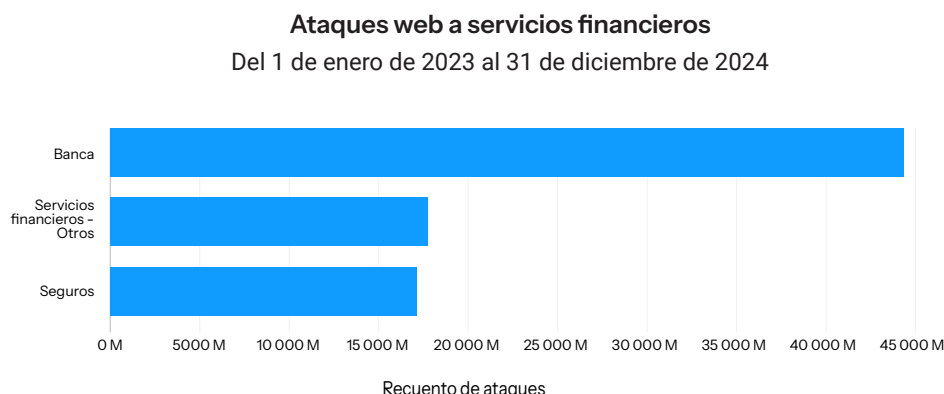


Fig. 9: La banca es el segmento que recibe más ataques web en el sector de los servicios financieros

La prevalencia de los servicios de banca online, junto con la naturaleza crítica del acceso a las cuentas, atrae a los ciberdelincuentes. Los incentivos financieros asociados a los ataques en este sector son considerables: incluso un pequeño número de cuentas comprometidas puede generar ganancias significativas. La reticencia del segmento bancario a implementar medidas de seguridad estrictas que podrían crear fricciones en la experiencia de los usuarios, como la autenticación multifactorial, ha [contribuido](#) involuntariamente a su vulnerabilidad.

La prominencia del segmento bancario como objetivo de ataque se ve agravada por varios factores. La sensibilidad al tiempo de inactividad presenta una oportunidad de extorsión, ya que los atacantes aprovechan el [temor](#) a las interrupciones de los servicios. Además, la creciente sofisticación de las técnicas de ataque (como el uso de la IA y el aprendizaje automático para evadir la detección) plantea importantes [desafíos](#) para los mecanismos de defensa tradicionales. El panorama normativo, con estrictos requisitos de cumplimiento y posibles multas por infracciones de seguridad, aumenta la complejidad de los desafíos de ciberseguridad del segmento bancario.

Alta tecnología

La alta tecnología sigue siendo uno de los principales sectores atacados tanto en el ámbito de los ataques web como de los ataques DDoS de capa 7. En el contexto de este informe, la alta tecnología incluye los segmentos del sector de las telecomunicaciones, el software y hardware de empresa, y el software y hardware de consumo. Nuestros datos mostraron que este sector era el segundo en el número de ataques web en general, con más de 81 700 millones de ataques durante el periodo de 2023 a 2024. Además, el sector de la alta tecnología fue el que recibió más ataques DDoS de capa 7: más de 7 billones durante el periodo de dos años.



Las aplicaciones web de alta tecnología suelen emplear consultas complejas de bases de datos y contenido dinámico, lo que crea vulnerabilidades que los atacantes aprovechan para [saturar fácilmente los servidores](#). Estas vulnerabilidades contribuyen a la alta tasa de ataques DDoS de capa 7 que sufre el sector. En particular, las [redes de blockchain](#) han experimentado un aumento considerable de ataques DDoS, ya que los atacantes utilizan métodos como la inundación HTTP y las transacciones de spam para impedir las transacciones legítimas, a pesar de la arquitectura descentralizada del blockchain. El impacto financiero crítico del tiempo de inactividad operativo en el sector de la alta tecnología motiva a los atacantes a desplegar ataques DDoS capaces de inhabilitar servicios esenciales. El desarrollo de software moderno depende de arquitecturas centradas en API, lo que supone un riesgo adicional, ya que los atacantes a menudo aprovechan terminales codificados de manera insegura en ataques de inundación HTTP.

El segmento de las telecomunicaciones se enfrenta a retos similares

El segmento de las telecomunicaciones, que se ve afectado por un número considerable de ataques a API, se enfrenta a retos de ciberseguridad similares. Entre las amenazas a API y aplicaciones web en este segmento del sector de la alta tecnología se incluyen las filtraciones de datos, los ataques DDoS y las vulnerabilidades de la cadena de suministro. Estas vulnerabilidades han dado lugar a varias filtraciones de datos de gran repercusión.

Por ejemplo, en enero de 2025, los investigadores descubrieron vulnerabilidades críticas de las API en una [importante red de telecomunicaciones](#) que expusieron a 3000 empresas a riesgos de seguridad. La investigación reveló importantes brechas de seguridad, como puntos débiles en el proceso de verificación Conozca a su cliente y una vulnerabilidad de cruce de rutas en una API de back-end que permitía el acceso a los sistemas internos.

El Internet de las cosas introduce nuevos vectores de ataque

El sector de la alta tecnología sigue lidiando con las vulnerabilidades de API y aplicaciones web en constante evolución en una era de rápidos avances tecnológicos. Esta evolución abarca la adopción generalizada de dispositivos del Internet de las cosas (IoT), que introduce nuevos vectores de ataque porque muchos dispositivos carecen de medidas de seguridad sólidas. La adopción acelerada de infraestructuras multinube suele dar lugar a entornos mal configurados, lo que crea posibles puntos de entrada que los atacantes pueden aprovechar.

Las vulnerabilidades de los dispositivos IoT y los sistemas en la nube creados de forma no segura son cada vez más presa de [sofisticados ataques con IA](#). Las [plataformas de SaaS](#) se enfrentan a riesgos elevados de ataques a API debido a su amplia superficie de ataque. La proliferación de soluciones de IA y el aumento de la dependencia de plataformas de SaaS de terceros han ampliado considerablemente la superficie de ataque general a API en el sector de la alta tecnología. A medida que las organizaciones siguen adoptando estas tecnologías, aumenta la posibilidad de ser objeto de ataque, lo que exige medidas de seguridad sólidas y una supervisión vigilante.

Tendencias regionales

NOTA: Hemos cambiado el formato de nuestros informes regionales para que los lectores puedan acceder a los datos y resaltar fácilmente las tendencias de ataque en distintas regiones: Norteamérica, Asia-Pacífico y Japón (APJ), Europa, Oriente Medio y África (EMEA) y Latinoamérica (LATAM). También hemos incluido un gráfico de referencia rápida para visualizar a los datos que tratamos en esta sección (Figura 10).

Datos de ataques webDatos de ataques DDoS de capa 7

Región	Recuentos de ataques web	Recuentos de ataques DDoS de capa 7	Principales vectores de ataques web	Principales áreas objetivo	Principales sectores objetivo
APJ	80 000 M, 14 % API	7,4 B, 6 % API	Sesión de ataque activa, LFI, XSS	Australia (20 300 M), India (17 300 M), Singapur (15 900 M)	Servicios financieros, comercio, redes sociales
				Singapur (4,7 B), India (607 000 M), Corea del Sur (283 000 M)	Redes sociales, otros medios digitales, comercio
EMEA	116 000 M, 37 % API	2,6 B, 20 % API	Sesión de ataque activa, violación de restricciones de solicitudes de API, LFI	Reino Unido (30 300 M), Países Bajos (19 500 M), España (14 200 M), Alemania (12 800 M)	Comercio, medios audiovisuales, servicios financieros
				Alemania (569 000 M), Reino Unido (506 000 M)	Comercio, otros medios digitales, medios audiovisuales
Latinoamérica	3 000 M, 12 % API	258 000 M, 18 % API	Sesión de ataque activa, WAT, SSRF	Brasil (19 300 M), México (2 000 M)	Comercio, servicios financieros
				Brasil (175 000 M), México (39 000 M)	Comercio, servicios financieros
Norteamérica	327 000 M, 29 % API	11,9 B, 16 % API			

Fig. 10: Resumen de regiones, de enero de 2023 a diciembre de 2024 (LFI indica inclusión de archivos locales; XSS, scripts entre sitios; WAT, herramienta de ataque web, y SSRF, falsificación de solicitudes en el servidor)



Dos tendencias de ataques a aplicaciones y API

Nuestro análisis de comparaciones regionales de ataques a aplicaciones web y API y ataques DDoS de capa 7 durante el periodo de 24 meses del informe, desde enero de 2023 hasta diciembre de 2024, revela dos tendencias generales (Figura 11).

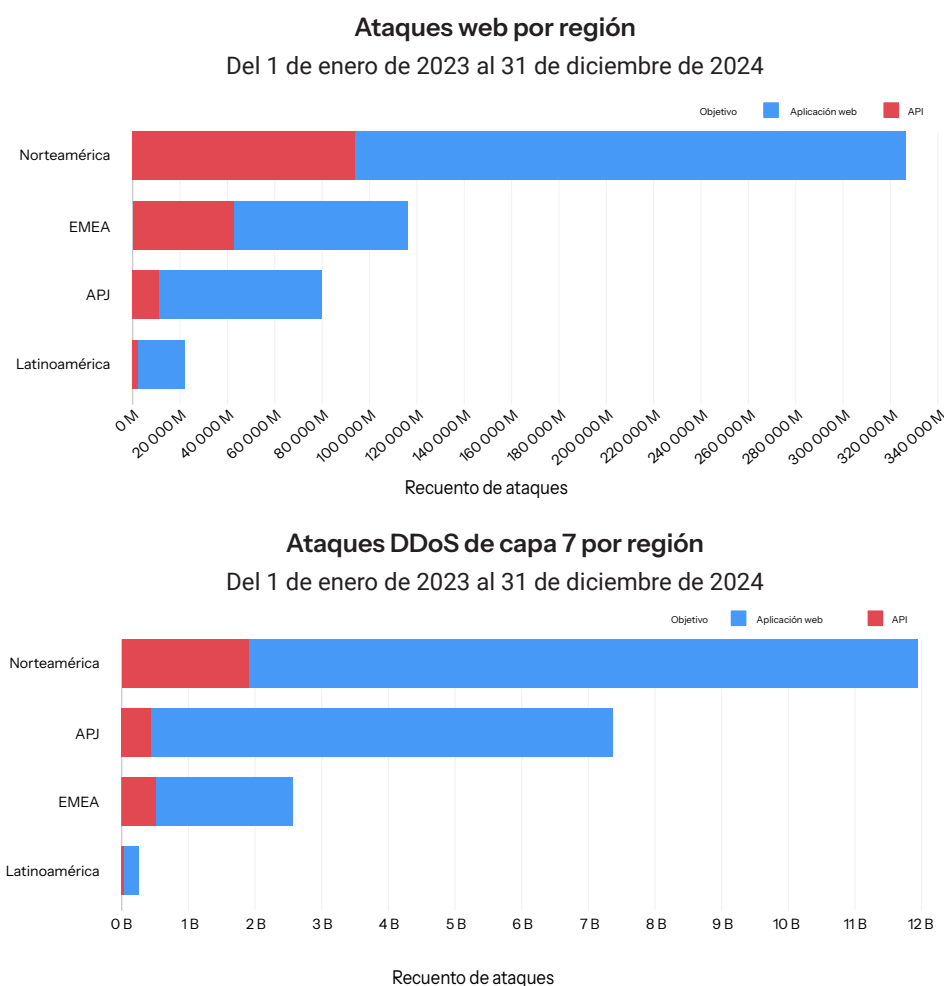


Fig. 11: Durante el periodo analizado, en todo el mundo, EMEA experimentó el mayor porcentaje de ataques a API, mientras que APJ experimentó el segundo número más alto de ataques DDoS de capa 7

Tendencia de ataque 1: los ataques a API se generalizaron en EMEA, lo que podría atribuirse a [tasas de adopción de API más altas que en otras regiones](#), así como a la banca abierta y a la [norma PCI DSS v 4.0](#), que están impulsando el uso de API y pueden introducir riesgos de seguridad. (Consulte la sección [Evolución de nuestra inteligencia sobre amenazas de API](#) para obtener información detallada sobre los riesgos específicos que afectan a las API).

En sintonía con la tendencia que [observamos por primera vez en 2023](#), EMEA experimentó la mayor concentración de ataques web contra API durante el periodo de 24 meses: del total de 116 000 millones de ataques web en la región, el 37 % fue dirigido a API. Por el contrario, Norteamérica registró un total de 327 000 millones de ataques web, un 29 % contra API. En APJ, el 14 % de los 80 000 millones de ataques web fue dirigido a API, seguido de LATAM, con un 12 % de los 3 000 millones de ataques.

EMEA también experimentó la mayor concentración de ataques DDoS de capa 7 dirigidos a API (20 %), seguida de LATAM (18 %), Norteamérica (16 %) y APJ (6 %). En general, los intentos de ataque DDoS de capa 7 contra API representaron un porcentaje relativamente pequeño del total de ataques web en cada región. Preveemos que estos porcentajes aumentarán con el tiempo por diversos motivos, como ataques basados en bots más avanzados y un aumento de ataques basados en IA contra vulnerabilidades de API.

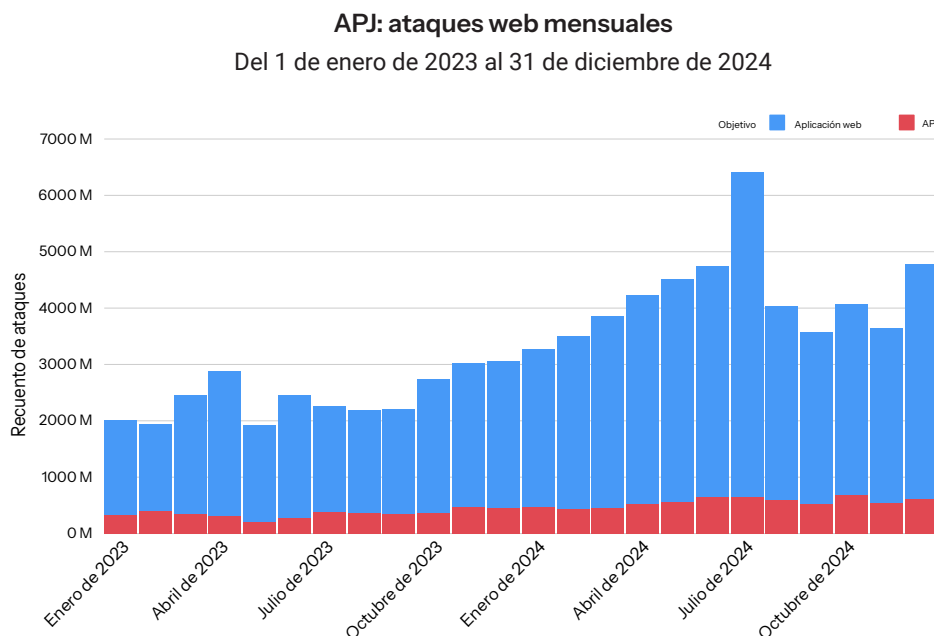
Tendencia de ataque 2: APJ experimentó el segundo nivel más alto de ataques DDoS de capa 7 a nivel mundial, con 7,4 billones (frente a los 11,9 billones en Norteamérica). La región EMEA alcanzó los 2,6 billones y la de Latinoamérica, los 258 000 millones. Esta tendencia se observó inicialmente en nuestro [informe sobre el estado de Internet \(SOTI\) Fortalezas digitales en peligro](#) y seguimos atribuyéndola a una alta concentración de intentos de ataque contra las redes sociales en APJ.

Un análisis más profundo de APJ, EMEA y LATAM

En esta sección, destacamos algunas tendencias clave en APJ, EMEA y LATAM. También incluimos datos específicos de áreas dentro de estas regiones donde tenemos suficientes datos de eventos de ataque para proporcionar información estadísticamente significativa.

Ataques a API y aplicaciones web: análisis del tráfico

La comparación de las tendencias mensuales de ataques web entre regiones revela un marcado contraste (Figura 12).



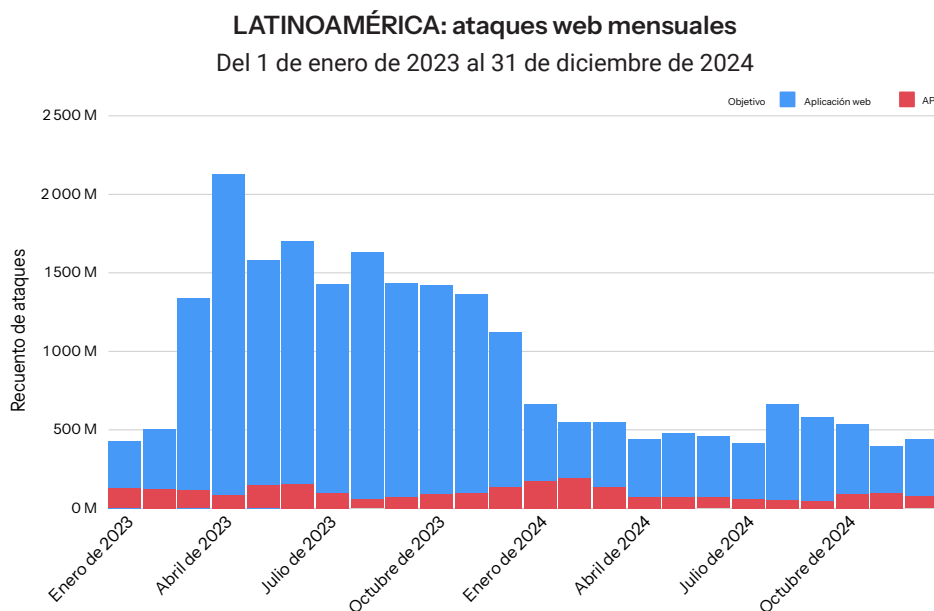
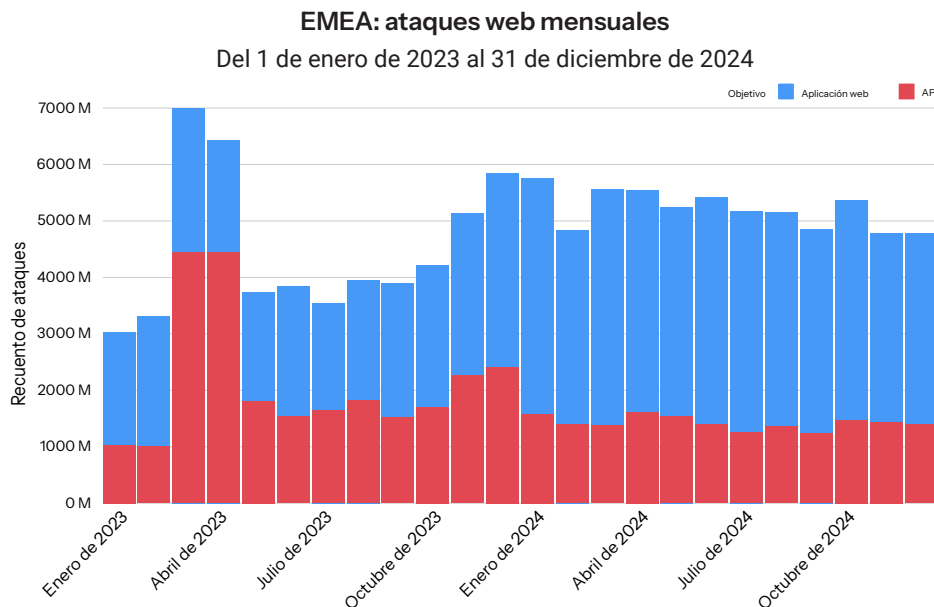


Fig. 12: La actividad de ataques a aplicaciones web provocó un aumento en el número total de ataques web en APJ y EMEA, mientras que los ataques en LATAM disminuyeron considerablemente

APJ experimentó un considerable aumento interanual del 73 % en el total de ataques web: de 29 000 millones en 2023 a 51 000 millones en 2024. En EMEA, el aumento interanual fue moderado, un 16 % (de 54 000 millones a 62 000 millones), pero este menor aumento se ve afectado por un evento atípico registrado en los datos que, si se elimina, aumentaría el número hasta acercarse al 33 %. En Latinoamérica, los ataques web disminuyeron considerablemente, ya que pasaron de un total de 16 000 millones en 2023 a 6 millones en 2024, lo que supone un descenso interanual del 61 %.

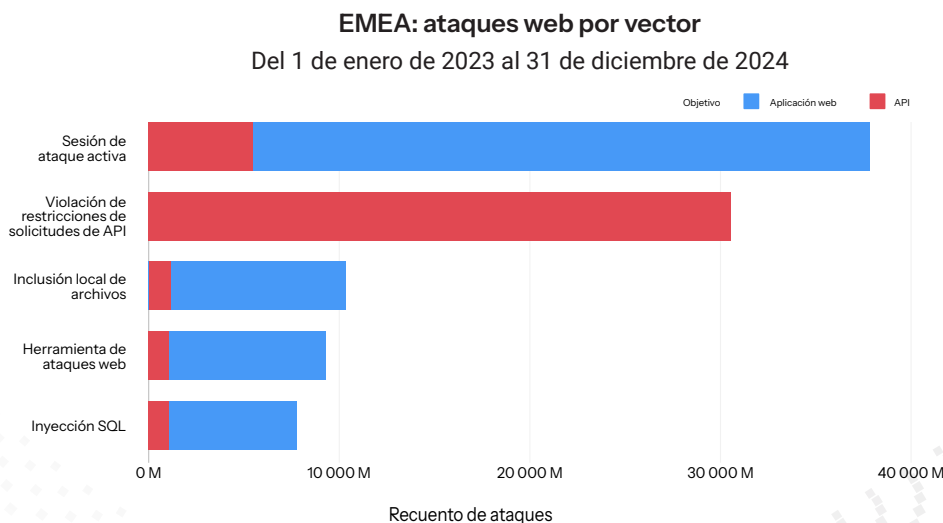
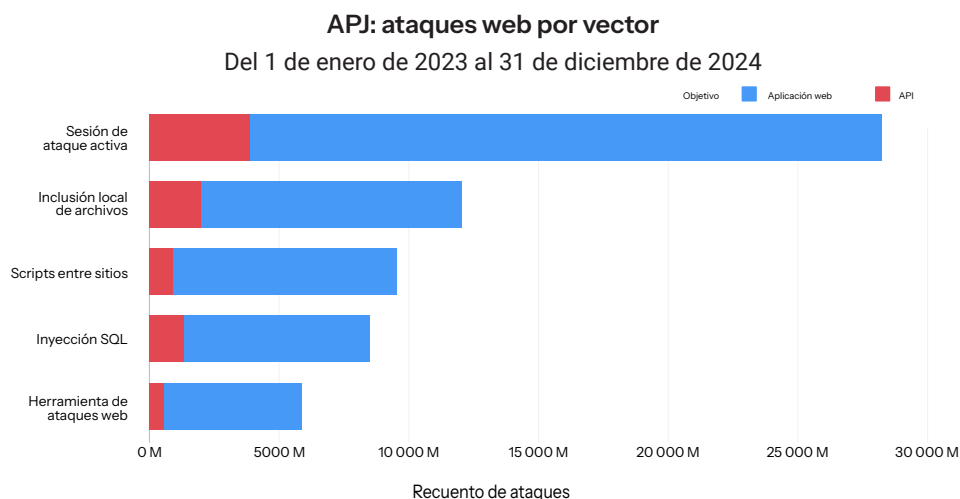
El crecimiento de los ataques a aplicaciones web parece estar impulsando un aumento en el número total de ataques web, ya que los ataques a API se mantuvieron en niveles bajos, especialmente en APJ y LATAM.

En EMEA, tras el pico registrado en el primer semestre de 2023 (relacionado con [ataques dirigidos a gran escala al sector del comercio en España](#)), los niveles de ataque a API disminuyeron y permanecieron en niveles inferiores a lo largo de 2024, aunque siguieron siendo relativamente altos con respecto a otras regiones.

En LATAM, los ataques web disminuyeron, ya que los atacantes redirigieron su atención del sector comercial a otros sectores, como el farmacéutico y el de los servicios empresariales, así como a otros tipos de ataques, como el [ransomware](#).

Ataques a API y aplicaciones web: tácticas en tendencia

En los últimos dos años, los atacantes siguieron recurriendo a métodos tradicionales de eficacia probada, pero el uso de vectores de ataque web modernos y basados en el comportamiento también fue elevado (Figura 13).



LATINOAMÉRICA: ataques web por vector

Del 1 de enero de 2023 al 31 de diciembre de 2024

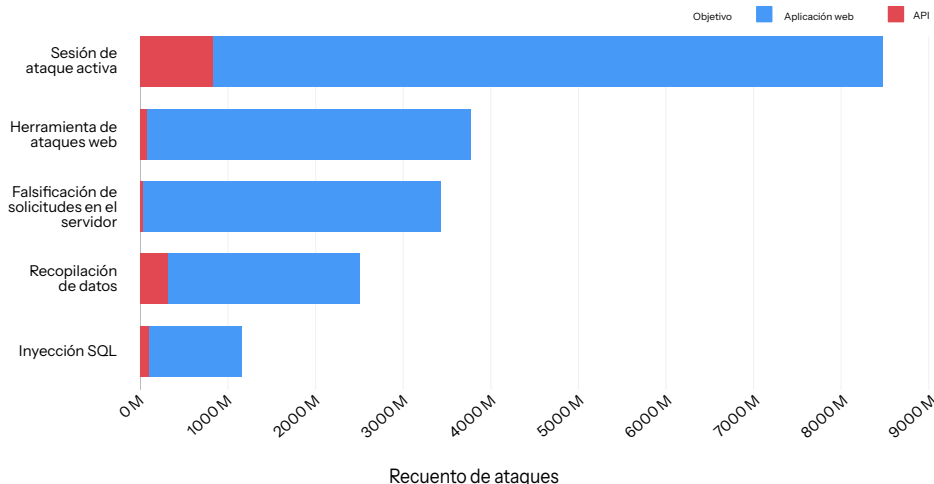


Fig. 13: En todas las regiones, los principales vectores de ataque incluyeron métodos tradicionales y modernos basados en el comportamiento dirigidos específicamente al uso indebido de API

En consonancia con las tendencias globales, en todas las regiones persisten los vectores de ataque tradicionales, como LFI, SQLi y XSS, junto con SSRF, que se observó en LATAM. Destacamos la capacidad de permanencia de XSS y su continua relevancia para la protección contra las vulnerabilidades web tradicionales en [La guía de los defensores de 2025](#).

Lo que es diferente durante este periodo, dado que los atacantes se centran cada vez más en el uso indebido de API, es el aumento de los problemas con los vectores de ataque modernos basados en el comportamiento. Los atacantes utilizan estos vectores para descubrir vulnerabilidades que puedan aprovechar. Tras el seguimiento de estos vectores a nivel regional, los investigadores de Akamai observaron lo siguiente:

- El principal vector de ataque en cada región fue la sesión de ataque activa, para la que se utilizan nuestros controles inteligentes a fin de bloquear de forma proactiva las solicitudes de atacantes conocidos durante un periodo de tiempo.
- La violación de restricciones de solicitudes de API fue el segundo vector más frecuente en EMEA, donde la concentración de ataques centrados en API es mayor. Los atacantes intentan realizar un uso indebido de las API eludiendo requisitos como los límites de velocidad y la entrada de datos.
- En cada región, la herramienta de ataque web se encontraba entre las cinco principales. Los atacantes utilizan este vector para investigar el objetivo y solicitar información sobre su seguridad, configuraciones o posibles vulnerabilidades que se podrían aprovechar con fines malintencionados.

Para obtener más información sobre estos vectores principales, consulte la sección [Ataques web](#).

Ataques a API y aplicaciones web: Principales objetivos

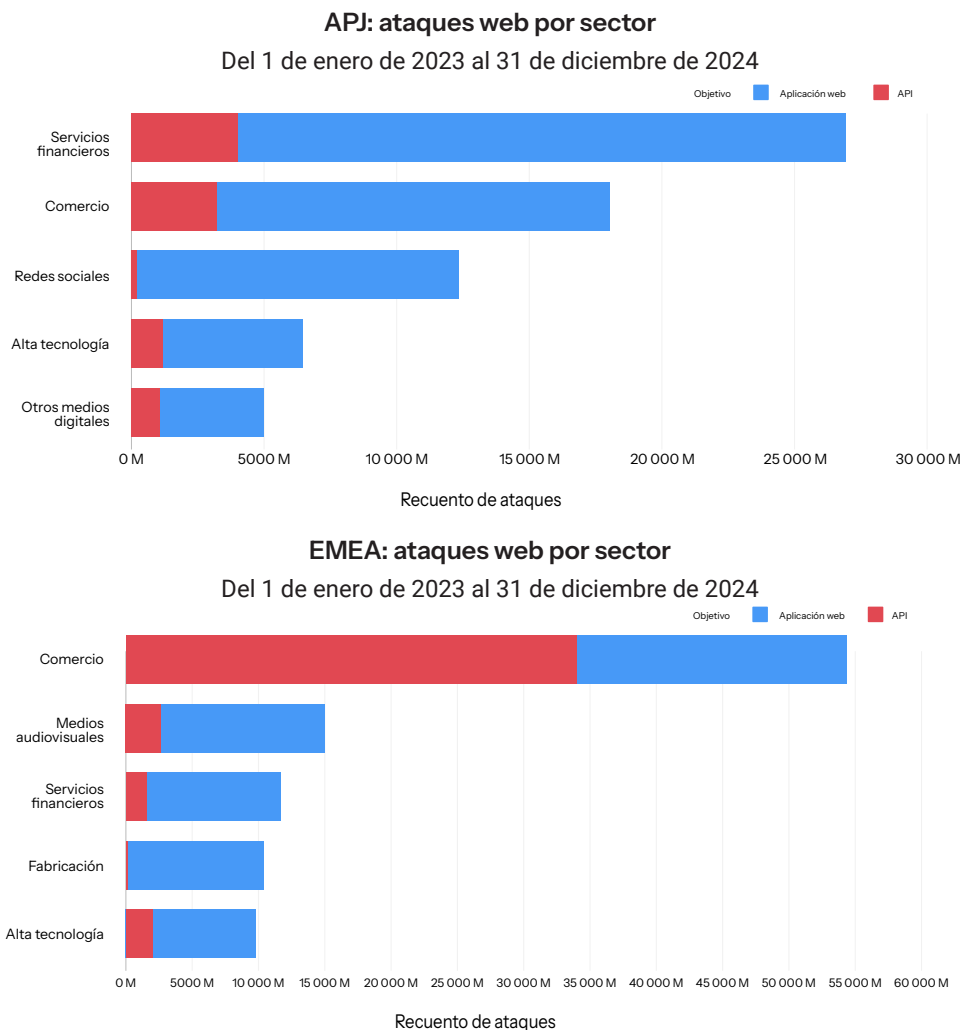
Al analizar específicamente dónde se concentraron los atacantes en cada región, observamos que, en APJ, Australia (20 300 millones), India (17 300 millones) y Singapur (15 900 millones) fueron los más afectados por ataques a aplicaciones web y API, seguidos de Japón (6300 millones), China (6200 millones), Corea del Sur (4900 millones), Nueva Zelanda (2900 millones) y la RAE de Hong Kong (2200 millones).

En EMEA, los países más afectados por los ataques a aplicaciones web y API fueron Reino Unido (30 300 millones), Países Bajos (19 500 millones), España (14 200 millones) y Alemania (12 800 millones). Austria le siguió con 8200 millones, junto con Francia (7500 millones), Italia (4100 millones), Suiza (3700 millones), Bélgica (3500 millones) e Israel (3300 millones).

En LATAM, el volumen de ataques a aplicaciones web y API se concentró en Brasil (19 300 millones), y los siguientes países más cercanos, México (2000 millones) y Chile (400 millones), sufrieron solo una parte relativamente pequeña de los ataques en la región.

Objetivos por sector

El análisis por tendencias del sector reveló que, en APJ, EMEA y LATAM, el comercio y los servicios financieros se encontraban sistemáticamente entre los tres sectores más afectados por los ataques web (Figura 14).



LATINOAMÉRICA: ataques web por sector

Del 1 de enero de 2023 al 31 de diciembre de 2024

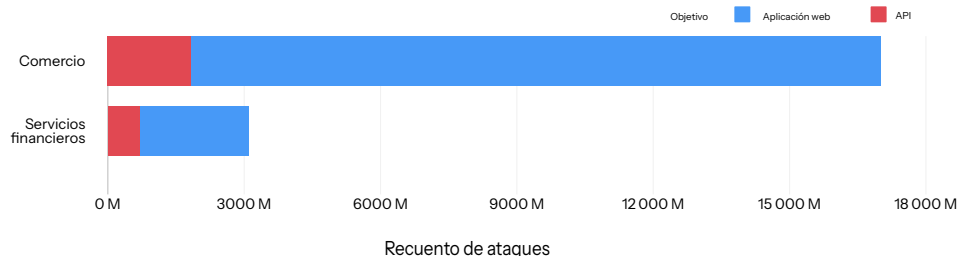


Fig. 14: El comercio y los servicios financieros se encontraban entre los tres sectores objetivo principales en las regiones de APJ, EMEA y LATAM

En APJ, el sector de los servicios financieros registró el mayor número total de ataques web, con 27 000 millones; el comercio quedó en segundo lugar, con 18 000 millones. Esto representa un crecimiento interanual del 52 % y del 161 %, respectivamente. Otros medios digitales fueron el sector más afectado por los ataques a API, con un 22 %, seguido del comercio (18 %) y los servicios financieros (15 %).

En EMEA, el comercio fue el sector más afectado por ataques web, con 54 000 millones, más del triple que el siguiente sector más cercano. A pesar de la alta concentración, el total de ataques web contra entidades comerciales disminuyó un 10 % interanual debido a un pico en 2023 que sesgó los datos de la región. Sin embargo, EMEA sigue registrando un aumento interanual del 16 % en el total de ataques web, debido al repunte de los ataques contra otros sectores, como los servicios financieros (152 %) y la fabricación (96 %). Al analizar más de cerca los ataques dirigidos a API en la región, vemos que el 63 % del total de ataques web contra el comercio se dirigió a API.

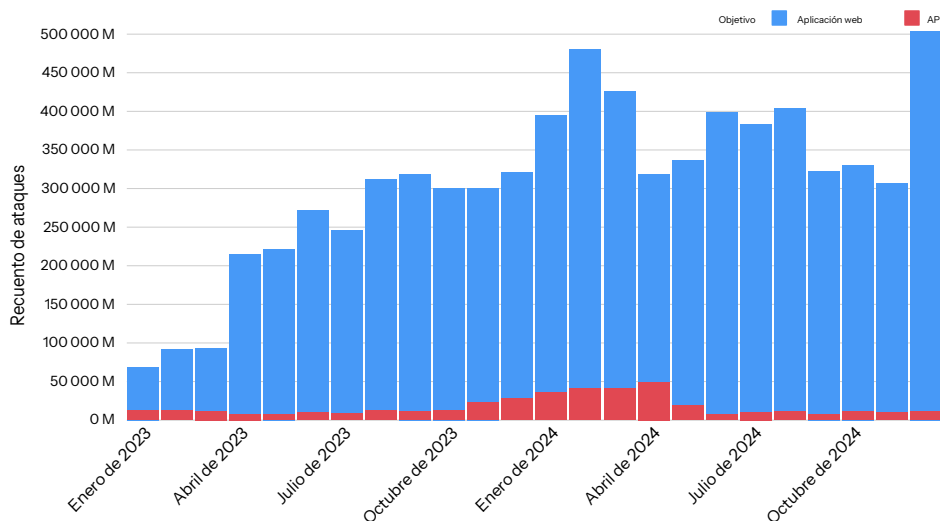
Vemos una tendencia similar en LATAM, donde el número total de ataques web contra el comercio alcanzó los 17 000 millones, por lo que superó a otros sectores. Sin embargo, año tras año, los ataques contra el sector del comercio disminuyeron un 76 %. Por su parte, los sectores farmacéutico y de servicios empresariales experimentaron aumentos interanuales del 107 % y el 129 %, respectivamente. Además, el 11 % de los ataques dirigidos al comercio se centraban en API y los servicios financieros tenían una concentración aún mayor de ataques contra API, con un 23 %.

Los sectores de los servicios financieros y el comercio comparten atributos que contribuyen a su atractivo como objetivo de los ataques a aplicaciones web y API: ambos operan en ecosistemas complejos, dependen en gran medida de las API y poseen datos valiosos. Los atacantes utilizan una combinación de técnicas de ataque tradicionales y emergentes para alcanzar sus objetivos.

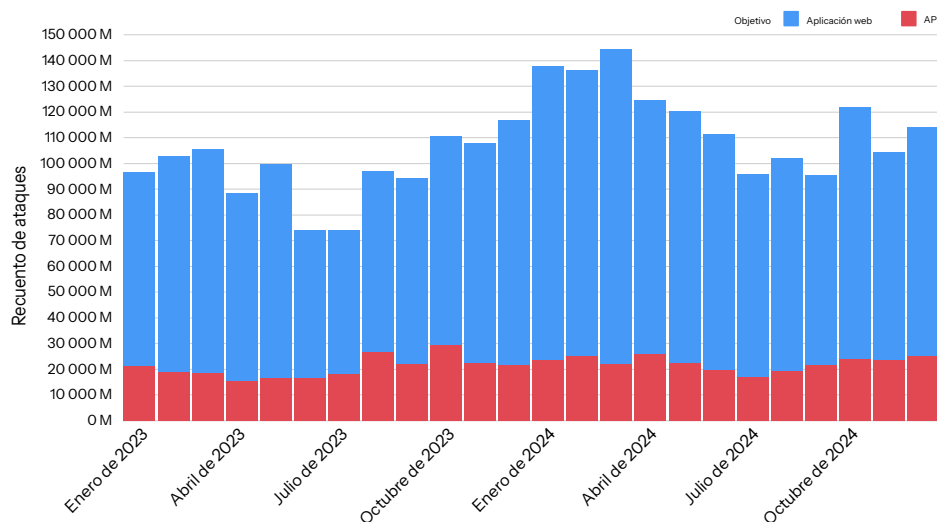
Ataques DDoS de capa 7: análisis del tráfico

Una comparación de las tendencias mensuales de los ataques DDoS de capa 7 entre las regiones revela que APJ era un punto de acceso, y que EMEA y LATAM experimentaron una fluctuación en el volumen de ataques (Figura 15).

APJ: ataques mensuales DDoS a la capa 7
Del 1 de enero de 2023 al 31 de diciembre de 2024



EMEA: ataques mensuales DDoS a la capa 7
Del 1 de enero de 2023 al 31 de diciembre de 2024



LATINOAMÉRICA: ataques mensuales DDoS a la capa 7

Del 1 de enero de 2023 al 31 de diciembre de 2024

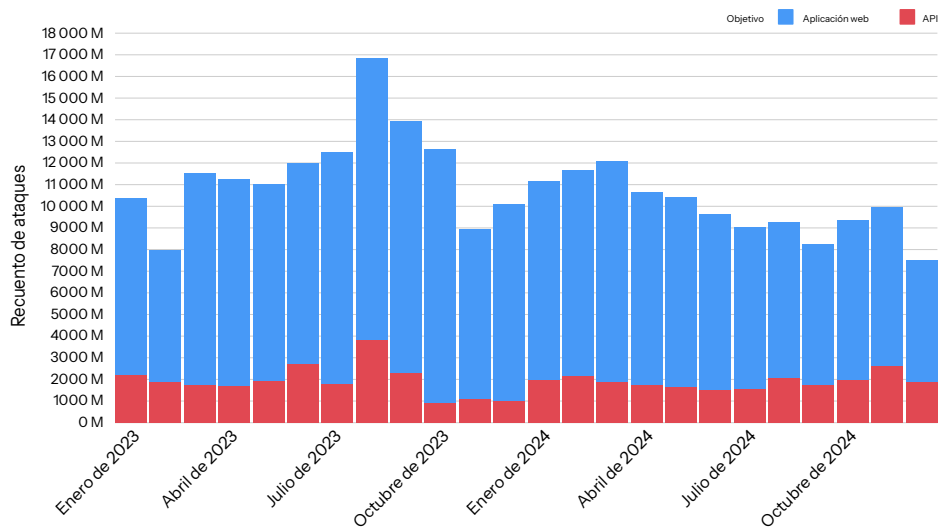


Fig. 15: Los ataques DDoS de capa 7 aumentaron en APJ y EMEA, mientras que los ataques en LATAM disminuyeron en 2024

APJ experimentó un crecimiento interanual del 66 % en los ataques DDoS de capa 7 y alcanzó un máximo de 24 meses, al llegar a un pico de 504 000 millones en diciembre de 2024. El crecimiento se debió principalmente a los ataques dirigidos al sector de las redes sociales.

En EMEA, los ataques DDoS de capa 7 alcanzaron su máximo en marzo de 2024 con casi 145 000 millones y, tras una caída, reanudaron su aumento y observaron un crecimiento interanual del 20 %. Esto puede atribuirse a una confluencia de factores geopolíticos y tecnológicos. Las continuas tensiones en la región han impulsado las actividades hacktivistas. Esta tendencia se ve agravada por el aumento de las herramientas mejoradas con IA y las plataformas de DDoS como servicio, que han reducido la barrera de entrada para los ciberdelincuentes.

LATAM experimentó un considerable aumento de los intentos de ataque DDoS de capa 7 a principios del periodo analizado, que coincidió con un aumento de los [ataques de inundación HTTP](#) dirigidos a la abrumadora cantidad de recursos de API (un vector de ataque que se analiza con más detalle en la sección [Ataques DDoS de capa 7: comparación y tendencias interanuales](#)). La actividad alcanzó su máximo en agosto de 2023, con 16 800 millones, y luego disminuyó durante el resto del periodo hasta llegar a los 7500 millones, lo que supone una disminución interanual del 15 % en los ataques.

Ataques DDoS de capa 7: principales objetivos

En cada región, observamos pocos cambios o ninguno en las áreas y sectores objetivo de los atacantes en comparación con [nuestro análisis anterior de ataques DDoS de capa 7](#).

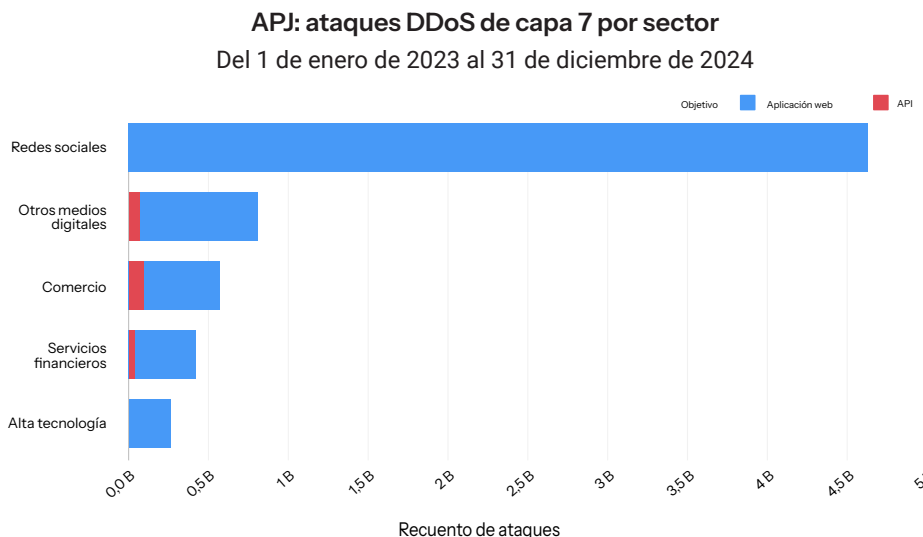
En APJ, Singapur experimentó la mayor concentración de ataques, con 4,7 billones, seguida de la India (1,1 billones), Corea del Sur (607 000 millones), Indonesia (283 000 millones), China (246 000 millones), Japón (111 000 millones), Australia (108 000 millones) y Taiwán (81 000 millones).

En EMEA, los países con el mayor número de ataques DDoS de capa 7 fueron Alemania (569 000 millones) y Reino Unido (506 000 millones), seguidos de Israel (205 000 millones), Suecia (193 000 millones) y Malta (160 000 millones). Italia (158 000 millones), Suiza (147 000 millones), Francia (129 000 millones), Países Bajos (111 000 millones) y España (96 000 millones) completaron los 10 primeros puestos.

En Latinoamérica, Brasil experimentó la mayor concentración de ataques DDoS de capa 7, con 175 000 millones, seguido de México (39 000 millones) y Costa Rica (19 000 millones).

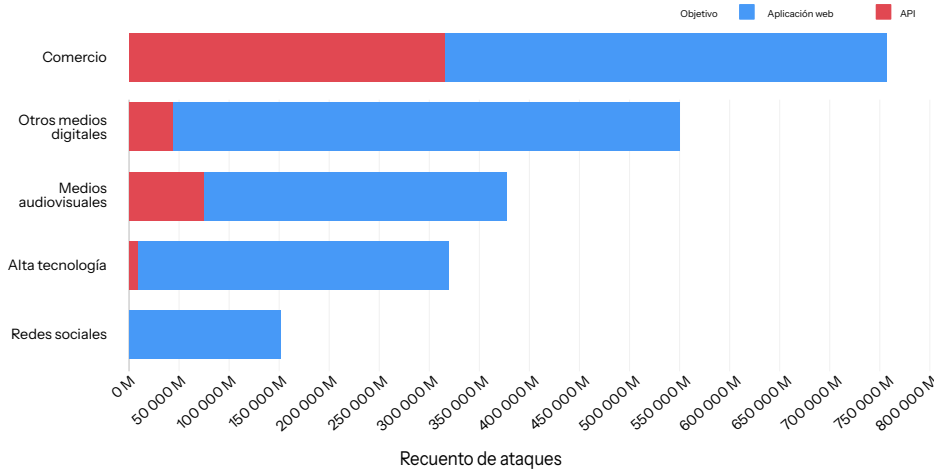
Objetivos por sector

Los principales sectores afectados por ataques DDoS de capa 7 en APJ y EMEA (Figura 16) no han cambiado desde nuestro [anterior informe SOTI en materia de seguridad de las aplicaciones](#). Como comentamos con más detalle en dicho informe, los ataques DDoS de capa 7 en plataformas de redes sociales en APJ aumentaron desde enero de 2023 hasta junio de 2024 en correlación con conflictos militares más amplios y eventos electorales de alta cobertura mediática en todo el mundo, lo que no es sorprendente, ya que las plataformas de redes sociales reciben grandes volúmenes de tráfico durante tiempos de agitación geopolítica. Como se había previsto, la tendencia se intensificó durante el resto de 2024 debido a las elecciones celebradas tanto en APJ como en los Estados Unidos. Estos factores contribuyeron al crecimiento interanual del 130 % de los ataques al sector.



EMEA: ataques DDoS de capa 7 por sector

Del 1 de enero de 2023 al 31 de diciembre de 2024



LATINOAMÉRICA: ataques DDoS de capa 7 por sector

Del 1 de enero de 2023 al 31 de diciembre de 2024

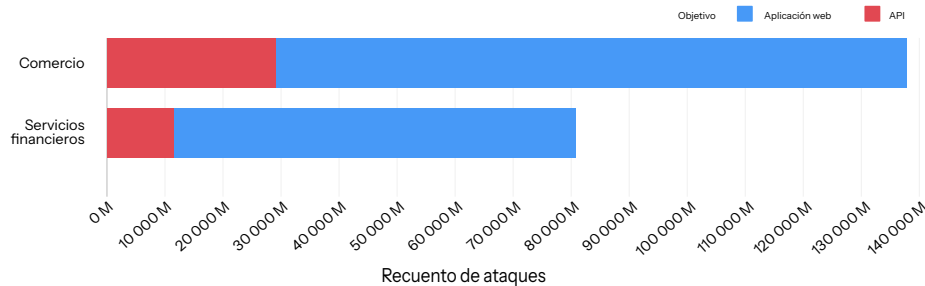


Fig. 16: Los sectores más afectados por región no han cambiado desde nuestro análisis anterior; el comercio fue el sector más afectado por los ataques DDoS de capa 7 a API

En EMEA, el comercio siguió siendo el sector más afectado por los ataques DDoS de capa 7, seguido de otros medios digitales y medios audiovisuales. Entre los sectores que experimentaron el mayor crecimiento interanual en estos ataques se encuentran la alta tecnología (70 %), las redes sociales (23 %) y el comercio (14 %). Estos cambios muestran la rapidez con la que los atacantes pueden cambiar su interés entre regiones y sectores e ilustran que merece la pena realizar un seguimiento de las tendencias más amplias.

El comercio también fue el sector objetivo principal de los ataques DDoS de capa 7 en LATAM, seguido del sector de los servicios financieros. Durante el periodo analizado, los niveles de actividad de los ataques DDoS de capa 7 se mantuvieron bastante constantes en todos los sectores.

Como reflejo de la tendencia global, entre los sectores más afectados por los ataques DDoS de capa 7, el sector del comercio experimentó la mayor concentración de ataques a las API en cada región. En EMEA, el 43 % de los ataques contra el comercio fueron dirigidos a API, el 21 % en Latinoamérica y el 16 % en APJ.

Por motivos como la inestabilidad geopolítica y el posible impacto económico de las interrupciones en servicios con una alta visibilidad, el comercio, los medios de comunicación y los servicios financieros han sido los principales objetivos de los ataques DDoS de capa 7 en EMEA y LATAM durante los últimos dos años. Consulte la sección [Tendencias por sectores](#) para obtener una explicación detallada de los factores y métodos que impulsan el alto nivel de actividad frente a los sectores del comercio y los servicios financieros.

Cumplimiento

Perspectiva global y de Norteamérica

El panorama mundial de la ciberseguridad en 2025 se caracteriza por una complejidad y volatilidad sin precedentes. Las tensiones geopolíticas, especialmente los conflictos que están teniendo lugar en Ucrania y Oriente Medio, han intensificado las ciberamenazas y los ataques financiados por los estados. El auge del hacktivismo, especialmente de grupos prorrusos que atacan a naciones occidentales, ha complicado aún más el panorama de amenazas. Desde el punto de vista económico, la rápida transformación digital en todos los sectores ha ampliado la superficie de ataque, ya que los ciberdelincuentes se centran cada vez más en infraestructuras críticas y utilizan tecnologías avanzadas, como la IA, para mejorar sus capacidades.

Estos factores, combinados con las presiones económicas globales y los cambios políticos en países clave, han creado una tormenta perfecta para los profesionales de la ciberseguridad de todo el mundo. La protección de las aplicaciones web y las API es un reto fundamental para las organizaciones. Los esfuerzos de hackers éticos, profesionales de la ciberseguridad y organizaciones como Akamai para abordar el imperativo de proteger estos puntos de entrada complementan las crecientes consideraciones sobre cumplimiento.

Los organismos reguladores de todo el mundo están imponiendo requisitos más estrictos en materia de ciberseguridad de las aplicaciones. En Norteamérica, el enfoque ha cambiado a estrategias integrales de gestión de riesgos y la notificación obligatoria de incidentes. La [Ley de Notificación de Incidentes Cibernéticos en Infraestructuras Críticas](#) de Estados Unidos, que se prevé entre en vigor en 2026, exige que las organizaciones que cuentan con infraestructuras críticas realicen un inventario de sus sistemas de información, categoricen los riesgos cibernéticos y evalúen su estrategia de ciberseguridad al menos una vez al año. Esta ley hace hincapié en la necesidad de adoptar medidas de seguridad sólidas en las aplicaciones, especialmente en las que se utilizan en sectores críticos como la energía, la fabricación de productos químicos y la tecnología de la información.

Asimismo, Canadá y México están adaptando sus normativas a las normas internacionales y se están centrando en la protección de datos y la seguridad de las infraestructuras críticas. Si bien las normativas específicas varían, la tendencia global se centra en requisitos de seguridad más rigurosos para las aplicaciones, como la validación de entradas mejorada, las prácticas de desarrollo seguro y las auditorías de seguridad periódicas.

El panorama de la seguridad de las API se enfrenta a desafíos paralelos y las API se están convirtiendo en el objetivo principal de los ciberdelincuentes debido a su papel fundamental a la hora de habilitar la integración de servicios y el intercambio de datos. Los organismos reguladores de todo el mundo están respondiendo mediante la introducción de [normativas más estrictas](#) que exigen a las organizaciones la implementación de medidas de seguridad de API sólidas.

Entre ellas se incluyen la detección de API continua y obligatoria, así como su supervisión y protección frente a las amenazas en constante evolución. En Norteamérica, el enfoque se centra en evaluaciones de riesgos exhaustivas de los ecosistemas de API, haciendo hincapié en prácticas de desarrollo seguras, mecanismos de autenticación sólidos y capacidades de detección de amenazas en tiempo real. La rápida adopción de herramientas de SaaS basadas en IA, a menudo integradas a través de API, ha ampliado considerablemente la superficie de ataque, lo que ha llevado a los reguladores a exigir enfoques de seguridad más sofisticados.

A medida que aumenta la complejidad de los entornos de API, especialmente con el auge de las aplicaciones de inteligencia artificial y aprendizaje automático, los requisitos de cumplimiento evolucionan para mitigar los riesgos asociados a las filtraciones de datos, el acceso no autorizado y las interrupciones del servicio. Aunque regiones como APJ, LATAM y EMEA están desarrollando sus propias normativas específicas, la tendencia global es la armonización de las normas de seguridad de API para adaptarlas a la naturaleza interconectada de la arquitectura digital moderna.

Perspectiva de APJ

La región APJ está experimentando un cambio importante en su panorama normativo, con nuevas leyes que afectan a organizaciones de diversos sectores. En Singapur, las recientes enmiendas a su [proyecto de ley de ciberseguridad](#) han ampliado el alcance para incluir sistemas de infraestructura de información crítica físicos y virtuales, incluidos los alojados en plataformas de nube y ubicados [en el extranjero](#). Japón ha actualizado su legislación a través del [Centro Nacional de Preparación para Incidentes y Estrategia de Ciberseguridad](#), mientras que India ha reformado su Ley de TI con la aprobación del [Proyecto de Ley de Protección de Datos Personales Digitales](#). Australia ha lanzado su Estrategia de Ciberseguridad 2023–2030, que reafirma el compromiso de la región con el fortalecimiento de las medidas de ciberseguridad. Como parte de esa estrategia, a finales de 2024 se realizaron enmiendas a la Ley Australiana de Seguridad de las Infraestructuras Críticas y se promulgó una nueva [Ley de Ciberseguridad de 2024](#); la aplicación de la ley ahora incluirá activos secundarios, como dispositivos IoT, aplicaciones y API que procesan datos confidenciales. Estos cambios normativos obligan a las organizaciones a reevaluar y mejorar sus prácticas de seguridad de aplicaciones web, con especial énfasis en la protección de la infraestructura crítica y los datos confidenciales.

Se prevé que la norma [PCI DSS v4.0.1](#) tenga un impacto significativo en las organizaciones que gestionan datos de tarjetas de pago; la fecha límite de cumplimiento era el 31 de marzo de 2025. Esta nueva versión introduce requisitos más estrictos para las aplicaciones web, como la implementación de controles para todos los scripts de páginas de pago ejecutados en los navegadores de los consumidores y el uso de soluciones técnicas automatizadas para detectar y prevenir continuamente los ataques basados en web. Las organizaciones de la región APJ ahora deben realizar análisis exhaustivos de brechas, actualizar sus políticas de seguridad e implementar los cambios técnicos necesarios para cumplir estas normas de seguridad mejoradas para sus aplicaciones web.

En cuanto a las API, la región APJ se está centrando cada vez más en la seguridad de las API, en parte debido a la creciente adopción de iniciativas de banca abierta. Aunque en la región aún no se han adoptado plenamente las normativas sobre banca abierta, como en EMEA, los países de APJ tienen la oportunidad de resolver de forma proactiva los [problemas en torno a la seguridad de las API](#). Una [encuesta realizada en agosto de 2024](#) sobre la seguridad de las API de esta región pone de manifiesto que las API internas son las más utilizadas, pero el acceso de usuarios externos sigue siendo la principal preocupación en el ámbito del control de acceso a las API. Esto indica la necesidad de que las organizaciones implementen medidas sólidas de seguridad de las API, como protocolos de autenticación y autorización sólidos, cifrado de datos y detección y supervisión continuas. A medida que la región avanza hacia directivas de [banca abierta](#), las organizaciones tendrán que priorizar la seguridad de las API para garantizar el cumplimiento de las normativas en constante evolución y protegerse contra las amenazas emergentes.

Perspectiva de EMEA

El panorama de la ciberseguridad en EMEA está experimentando una importante transformación, impulsada por una compleja interacción de tensiones geopolíticas, avances tecnológicos y cambios normativos. La región se enfrenta a desafíos únicos y los conflictos que están teniendo lugar en Ucrania y Oriente Medio intensifican las ciberamenazas y los ataques financiados por los Estados. Además, el aumento del hacktivismo, especialmente de grupos prorrusos que atacan a países europeos, ha hecho de la región un foco prioritario para las operaciones cibernéticas con motivaciones políticas.

El panorama de las API en EMEA se está enfrentando a desafíos paralelos. Las API se han convertido en el objetivo principal de los ciberdelincuentes debido a su papel fundamental a la hora de permitir la integración de servicios y el intercambio de datos. Además, la rápida adopción de herramientas de SaaS basadas en IA, a menudo integradas a través de API, ha ampliado considerablemente la superficie de ataque.

En respuesta a estas crecientes amenazas, la Unión Europea ha publicado toda una serie de normativas sobre ciberseguridad. La [Directiva actualizada relativa a la Seguridad de las Redes y Sistemas de Información \(NIS2\)](#), que entró en vigor en enero de 2025, amplía considerablemente su ámbito de aplicación al incluir 18 sectores críticos, y exige la aplicación de estrictas medidas de ciberseguridad a entidades medianas y grandes.

Para el sector financiero, la [Ley de Resiliencia Operativa Digital \(DORA\)](#), en vigor desde el 17 de enero de 2025, sustituye a la directiva NIS2 e impone marcos sólidos de gestión de riesgos para las tecnologías de la información y las comunicaciones, mecanismos de notificación de incidentes y programas digitales de pruebas de resiliencia operativa para aplicaciones utilizadas en servicios financieros. Además, la norma [PCI DSS v4.0.1](#), que pasó a ser obligatoria el 31 de marzo de 2025, introduce nuevos requisitos de cumplimiento centrados en las necesidades de seguridad en evolución, los procesos de seguridad continuos, las metodologías flexibles y los procedimientos de validación mejorados. La tercera [Directiva sobre Servicios de Pago de la UE \(PSD3\)](#) pretende abordar las deficiencias de la directiva PSD2 mediante mecanismos más estrictos de intercambio de datos, el refuerzo de los requisitos de seguridad y la mejora de la supervisión en el sector de los servicios financieros.



La Ley de Resiliencia Cibernética ([CRA](#)), que entró en vigor el 10 de diciembre de 2024, establece estándares obligatorios en materia de ciberseguridad para los productos con elementos digitales vendidos en la Unión Europea, lo que exige a los fabricantes que implementen medidas de seguridad a lo largo del ciclo de vida de un producto conectado. Para los desarrolladores de aplicaciones y los usuarios, la CRA considera a los smartphones y las tablets como vectores de riesgo importantes. Esta inclusión requiere que las organizaciones traten los terminales móviles como componentes fundamentales de su estrategia general de ciberseguridad e implementen rigurosas medidas de seguridad a lo largo del ciclo de vida de las aplicaciones.

En el Reino Unido, el próximo [Proyecto de Ley sobre Ciberseguridad y Resiliencia](#) mejorará las ciberdefensas del país y protegerá los servicios públicos esenciales. Las actualizaciones fundamentales del proyecto de ley en el marco regulatorio heredado ampliarán el alcance para proteger más servicios digitales y cadenas de suministro, fortalecer la aplicación y aumentar los requisitos de notificación.

Perspectiva de LATAM

El panorama de la ciberseguridad en LATAM está evolucionando rápidamente, conformado tanto por las tendencias tecnológicas globales como por los desafíos económicos y políticos propios de la región. En este contexto, la rápida transformación digital en los países de Latinoamérica, junto con las vulnerabilidades de los sistemas cada vez más interconectados, ha convertido a la región en un objetivo atractivo tanto para los ciberdelincuentes como para los atacantes financiados por los Estados. Los sectores del comercio y los servicios financieros han surgido como objetivos principales de los ciberataques. Los retailers online, los procesadores de pagos, los bancos, las compañías de seguros, las startups de tecnología financiera y los intercambios de criptomonedas son especialmente [vulnerables](#) a las amenazas que afectan a su infraestructura digital, especialmente a sus aplicaciones web y API.

Los países de Latinoamérica reconocen estos desafíos y están realizando importantes avances en el desarrollo y la implementación de normativas de ciberseguridad, con un enfoque cada vez mayor en la seguridad de las API y las aplicaciones web. Brasil ha asumido un papel de liderazgo con la implementación de la Lei Geral de Proteção de Dados Pessoais (LGPD), que entró en vigor con estrictos [requisitos](#) de protección y seguridad de datos. Aunque no aborda específicamente las aplicaciones web o las API, la LGPD ha impulsado a las organizaciones a mejorar su estrategia de ciberseguridad general, incluida la seguridad de sus interfaces digitales.

De manera similar, Chile ha promulgado su [Ley Marco de Ciberseguridad](#), que entró en vigor el 1 de enero de 2025. Esta ley crea la Agencia Nacional de Ciberseguridad y establece medidas completas para prevenir, notificar y resolver incidentes de ciberseguridad en varios sectores, incluidos los que dependen en gran medida de aplicaciones web y API. También en enero de 2025, Argentina publicó su [Plan Federal de Prevención de Ciberdelitos y Gestión Estratégica de la Ciberseguridad \(2025–2027\)](#).

Existen avances prometedores en el ámbito de las normativas específicas de las API. México, por ejemplo, ha implementado una [legislación](#) centrada en el sector financiero (incluida la tecnología financiera), con requisitos detallados para que las agencias de crédito y las cámaras compensadoras desarrollen API seguras. Este enfoque refleja un creciente reconocimiento del papel fundamental que desempeñan las API en los ecosistemas digitales modernos y la necesidad de adoptar medidas de seguridad específicas. Además, la [Ley Federal de Protección de Datos Personales en Posesión de los Particulares](#) de México regula el tratamiento de datos personales y establece obligaciones para empresas y organizaciones.

Colombia también ha estado avanzando en su [marco](#) normativo al ampliar su alcance legal mediante la publicación de políticas públicas sobre ciberseguridad para instituciones públicas y la creación de un sistema digital de gestión de riesgos de seguridad con diferentes niveles de informes de respuesta a incidentes. Aunque no se centran exclusivamente en las API, estas medidas afectarán inevitablemente a las prácticas de seguridad de las API dentro de las organizaciones.

En toda la región, existe una tendencia creciente hacia la adopción de [iniciativas](#) específicas del sector, como marcos de financiación abierta, que establecen normas de seguridad de API para proteger los datos de los consumidores. Estos marcos son especialmente relevantes en el sector financiero, donde la seguridad de las API es fundamental para mantener la integridad de las transacciones y proteger la información confidencial de los clientes. A medida que los países de Latinoamérica siguen dando prioridad a los avances en seguridad y alinean sus normativas de ciberseguridad con las normas internacionales, cabe esperar que surjan directrices más completas y específicas para la seguridad de las API y las aplicaciones web.

Mitigación

En un panorama de amenazas en constante evolución con técnicas de ataque más sofisticadas en auge, la protección de las aplicaciones web y las API es un desafío esencial para las organizaciones. Algunas de las técnicas de protección y mitigación que recomendamos son:

- **Establecer un plan de seguridad de API completo:** implemente un enfoque de "shift-left" y DevSecOps, que integre la seguridad desde el diseño de las API hasta la posproducción. Garantice una [detección](#) y visibilidad continuas para comprender toda la superficie de ataque, incluidas las API ocultas (API en la sombra, heredadas y zombis). Refuerce la seguridad con medidas estrictas de autenticación y autorización (OAuth 2.0, mTLS, control de acceso por roles/control de acceso por atributos), limitación de velocidad y mitigación de bots para evitar el uso indebido. Implemente la detección de amenazas en tiempo real, la supervisión de anomalías y la protección del tiempo de ejecución para identificar y detener los ataques a medida que se producen. Garantice el cumplimiento de normativas como DORA, RGPD, HIPAA, NIS2 y PCI DSS, al tiempo que aplica políticas de gobernanza de las API para mantener la seguridad a gran escala.
- **Implementar medidas sólidas de ciberseguridad:** utilice un [motor de seguridad adaptable](#) que supervise y responda continuamente a las amenazas en tiempo real y proporcione inteligencia sobre amenazas y [protección en tiempo de ejecución](#). Utilice también [herramientas de prueba de API](#), como pruebas de seguridad de aplicaciones dinámicas (DAST), para asegurarse de que se cumplen los requisitos de seguridad, como el acceso seguro, el cifrado y la autenticación.
- **Adoptar una defensa proactiva contra las amenazas:** utilice [herramientas especializadas de protección contra DDoS](#), configure la limitación de velocidad y el almacenamiento en caché de CDN e implemente medidas como la gestión de parches, las políticas de control de acceso y la segmentación de la red. Proteja también la infraestructura de DNS con la supervisión continua del tráfico y las plataformas híbridas.
- **Mitigar las vulnerabilidades de las API:** siga las directrices de seguridad establecidas, como las proporcionadas por [OWASP](#), para garantizar una sólida seguridad de las API y abordar los riesgos de prácticas de codificación deficientes y errores de configuración en la arquitectura de API, que pueden crear vulnerabilidades explotables que permiten a los hackers obtener acceso no autorizado o manipular datos.

- **Defenderse de las amenazas de ransomware:** utilice un enfoque por capas para combatir el ransomware. Implemente soluciones Zero Trust para bloquear el tráfico malicioso, utilice la microsegmentación para obtener una visibilidad detallada y un control de acceso preciso, y aproveche el [marco de trabajo de MITRE ATT&CK](#) para comprender los patrones de ataque y mejorar las estrategias de respuesta.
- **Prepararse para la IA:** emplee una estrategia de defensa integral que incluya [soluciones de defensa contra bots](#), herramientas de seguridad basadas en IA, firewalls especializados y medidas proactivas, como evaluaciones continuas y modelos Zero Trust, para hacer frente a los nuevos riesgos de seguridad que presenta el [creciente uso de la IA](#). Proteja los sistemas de IA con un enfoque multifacético: combata amenazas específicas, como la inyección de instrucciones y el envenenamiento de datos, mediante el conocimiento de modelos y conjuntos de datos; realice pruebas proactivas de vulnerabilidades; y utilice defensas sólidas, como la supervisión del comportamiento, la validación de contenido y las respuestas a ataques automatizadas que están integradas en entornos de desarrollo y tiempo de ejecución.

Metodología

Ataques DDoS de capa 7 y ataques a aplicaciones web

Estos datos describen las alertas en la capa de aplicación sobre el tráfico observado a través de nuestro firewall de aplicaciones web (WAF). Las alertas de ataques contra aplicaciones web se activan cuando detectamos una carga maliciosa en una solicitud a un sitio web, una aplicación o una API protegidos. Las alertas DDoS de capa 7 se activan cuando detectamos anomalías volumétricas en el número de solicitudes a un sitio web, una aplicación o una API protegidos. Estas alertas las pueden activar tanto bots maliciosos como bots legítimos. Normalmente, las solicitudes son legítimas, pero el gran volumen de solicitudes indica intenciones maliciosas. Las alertas no indican que un ataque haya conseguido su objetivo. Aunque estos productos permiten un alto nivel de personalización, recopilamos los datos presentados aquí de una manera que no tiene en cuenta las configuraciones personalizadas de las propiedades protegidas.

Los datos se extrajeron de una herramienta interna de análisis de eventos de seguridad detectados en Akamai Cloud, una red de aproximadamente 340 000 servidores repartidos en más de 4000 centros, casi 1300 redes y más de 130 países. Nuestros equipos de seguridad utilizan estos datos, medidos en petabytes mensuales, para investigar ataques, detectar comportamientos maliciosos y proporcionar información adicional a las soluciones de Akamai.

Estos datos cubren el periodo de 24 meses que abarca desde el 1 de enero de 2023 hasta el 31 de diciembre de 2024.

Datos de los ataques contra la seguridad de las API

Con la adquisición de Noname Security, Akamai ha mejorado sus capacidades de investigación y generación de informes sobre las amenazas de API. Este conjunto de datos aún se encuentra en las primeras etapas de integración y análisis. Para este informe, tomamos una muestra de datos de un periodo de 30 días del primer trimestre de 2025 para analizar el desglose de las alertas de seguridad de las API según sus marcos de seguridad y normas de cumplimiento correspondientes. Este conjunto de datos seguirá avanzando y proporcionará una vista ampliada de los problemas de seguridad de las API en el futuro.



Créditos

Director de investigación

Mitch Mayne

Editorial y redacción

Charlotte Pelliccia

Lance Rhodes

Badette Tribbey

Maria Vlasak

Revisión y expertos en la materia

Tom Emmons

Reuben Koh

Richard Meeus

Stas Neyman

Steve Winterfeld

Análisis de datos

Chelsea Tuttle

Materiales promocionales

Barney Beal

Ashley Linares

Marketing y publicación

Georgina Morales Hampe

Emily Spinks

Estado de Internet/seguridad

Lea números anteriores del aclamado informe sobre el estado de Internet en materia de seguridad de Akamai y entérese de cuándo se publican los siguientes números.

akamai.com/soti

Investigación de Akamai sobre amenazas

Conozca los últimos análisis de inteligencia frente a amenazas, informes de seguridad e investigación sobre ciberseguridad.

akamai.com/security-research

Acceda a los datos de este informe

Vea versiones de alta calidad de los gráficos a los que se hace referencia en este informe. Puede usar estas imágenes y hacer referencia a ellas libremente, siempre que se cite debidamente a Akamai como fuente y que se conserve el logotipo de Akamai.

akamai.com/sotidata

Investigación sobre seguridad de Akamai

Lea el blog de investigación sobre seguridad de Akamai para obtener una perspectiva de respuesta rápida sobre la investigación más importante de hoy en día.

akamai.com/blog/security-research



La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Gracias a la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en [X](#), antes conocido como Twitter, y [LinkedIn](#). Publicado en abril de 2025.