

# Comercio electrónico y sector retail

## Cómo perciben y experimentan las empresas de su sector la creciente amenaza para las API

Las API que impulsan las iniciativas digitales de las empresas de comercio electrónico y del sector retail están en el punto de mira. Los atacantes, valiéndose de métodos cada vez más innovadores, acceden a datos en API desprotegidas para robar información de tarjetas de crédito, desviar fondos de programas de fidelización y lanzar ataques de Credential Stuffing. Los equipos de seguridad están al tanto de estos ataques y sus consecuencias, por lo que buscan constantemente formas de mejorar la protección. Afrontar otro vector de ataque puede antojarse desalentador, especialmente en el caso de las API, cuya mala configuración o cuyos fallos en la lógica empresarial pueden descubrirse y explotarse con facilidad.

¿Cómo disponemos de esta información? Akamai ha encuestado a más de 1200 profesionales de TI y seguridad, desde directores de seguridad de la información hasta personal de seguridad de las aplicaciones, para conocer sus experiencias con las amenazas relacionadas con las API.

Este informe desvela los resultados de su sector, donde el 68 % de los encuestados afirma haber experimentado incidentes de seguridad relacionados con las API en los últimos 12 meses. ¿Cuáles fueron las consecuencias? Las principales respuestas de las empresas que operan en su sector incluyeron el aumento de los niveles de estrés en sus equipos y el deterioro de la credibilidad entre la alta dirección y los miembros de la junta directiva. Se trata de una respuesta comprensible, dados los costes notificados; los profesionales de comercio electrónico y del sector retail citan un gasto medio de 526 531 USD por incidente de API.

Siga leyendo para obtener información sobre el sector en el [Estudio sobre el impacto de la seguridad de API de 2024](#).

## La visibilidad disminuye conforme aumentan los ataques

Si bien la notable mayoría de los encuestados pertenecientes al comercio electrónico y al sector retail experimentó incidentes de seguridad de API, su media del 68 % fue inferior al 84 % registrado en los ocho sectores encuestados. Mientras tanto, las principales prioridades en materia de seguridad de empresas similares del sector, de cara a los próximos 12 meses, son "defenderse de los ataques impulsados por IA generativa" y "proteger las API de los atacantes".

¿Existe alguna relación entre priorizar las API y prevenir los ataques? Es posible que los equipos de seguridad de las empresas de comercio electrónico y del sector retail hayan reconocido la importancia que tiene proteger las API y que las medidas adoptadas hayan contribuido a reducir los incidentes. No obstante, nuestros hallazgos también sugieren que estos equipos no están detectando todos los casos de abuso de las API.

Distinguir entre actividades de API genuinas y maliciosas, o fraudulentas, sigue siendo un reto para las empresas de comercio electrónico y del sector retail. Además, la visibilidad del riesgo les supone otro desafío. Aunque el 67 % de sus homólogos en el sector afirma tener inventarios de API completos, *tan solo el 29 %* de este subconjunto sabe cuáles de sus innumerables API devuelven datos confidenciales. Esto incluye información de identificación personal (PII) o datos de tarjetas de crédito.

Piense en lo que puede suceder con una API que implemente una unidad de negocio sin colaboración ni supervisión por parte de los equipos centrales de seguridad o TI del retailer. Esta API podría:

- Haberse creado para devolver datos de clientes sin unos controles de autorización adecuados y sin las pruebas oportunas para detectar errores de configuración.
- Haberse sustituido por una nueva versión sin desactivarse previamente la anterior, la cual sigue expuesta a Internet.
- Haber pasado desapercibida ante las herramientas tradicionales, que no pueden detectar las API no administradas.
- Ser explotada por estafadores que acceden a las cuentas de fidelización de clientes reales y canjean efectivo.

**68 %** de las empresas de comercio electrónico y del sector retail sufrió algún incidente de seguridad de API en los últimos 12 meses<sup>1</sup>

**Tan solo el 29 %** de las empresas de comercio electrónico y del sector retail con inventarios de API completos saben cuáles devuelven datos confidenciales<sup>1</sup>

**526 531 USD** = impacto financiero medio de un incidente de seguridad de API para las empresas de comercio electrónico y del sector retail en los últimos 12 meses<sup>1</sup>

## 3 consecuencias principales<sup>1</sup>

1. **Aumento del estrés** o la presión para mi equipo
2. **Asunción de gastos** para solucionar el problema
3. **Daños a la reputación de nuestro departamento**, sobre todo frente a la alta dirección y ante la junta directiva

**44 %** de los ataques web dirigidos contra las organizaciones de comercio tenían como objetivo a las API<sup>2</sup>

Fuentes:

1. Akamai, "Estudio sobre el impacto de la seguridad de API", 2024
2. Informe sobre el estado de Internet (SOTI) de Akamai, "Al acecho en las sombras: las tendencias de ataque ponen de relieve las amenazas a las API", 2024



Esto no es una mera hipótesis. Según el estudio True Cost of Fraud™ (El verdadero coste del fraude) de 2023 de LexisNexis® Risk Solutions, el 50 % de las pérdidas por fraude pueden atribuirse al abuso en la apertura de nuevas cuentas, para lo cual los estafadores abusan de las API con el propósito de abrir cuentas a gran escala. Además, nuestro escenario refleja lo que los equipos de TI y seguridad reales citan como las principales causas de sus incidentes de API.

### Principales causas de los incidentes de API, según el testimonio de los equipos de seguridad de comercio electrónico y del sector retail

- |  |  |
|--|--|
| 1. Las API en herramientas de IA generativa; por ejemplo, LLM: <b>24,7 %</b> | 7. Una herramienta o un servicio tecnológicos muy conocidos: <b>20,0 %</b> |
| 2. La API tuvo una exposición accidental a Internet: <b>24,0 %</b>           | 8. El firewall de red no lo detectó: <b>18,7 %</b>                         |
| 3. Configuración incorrecta de API: <b>22,0 %</b>                            | 9. Vulnerabilidades de autorización: <b>17,3 %</b>                         |
| 4. El firewall de aplicaciones web (WAF) no lo detectó: <b>21,3 %</b>        | 10. Solución de software descargada de Internet: <b>16,7 %</b>             |
| 5. La puerta de enlace de API no lo detectó: <b>20,7 %</b>                   | 11. Falta de controles de autenticación de API: <b>16,0 %</b>              |
| 6. Vulnerabilidad debida a errores de codificación de API: <b>20,0 %</b>     | 12. Solución de software de nivel intermedio: <b>14,7 %</b>                |
|  | 13. API no gestionadas (por ejemplo, API zombies): <b>13,3 %</b>           |




P. ¿Cuáles cree que son las causas de los incidentes de seguridad de API que ha experimentado su organización? (Seleccione un máximo de 3); n=1207

## Impacto de los incidentes de API en el cumplimiento, los costes empresariales y el estrés del equipo

El informe Gartner® Market Guide for API Protection de mayo de 2024 expone lo siguiente: "Según datos actuales, se estima que cada vez que se ataca una API, se filtran de media 10 veces más datos confidenciales que con cualquier otro tipo de vulneración".<sup>3</sup> No es de extrañar que la normativa PCI DSS v4.0, ampliamente seguida, haya añadido requisitos en torno a la seguridad de las API. Tanto las empresas como sus reguladores necesitan saber qué tipos de datos se transmiten, no solo a través de sus propias API, sino también mediante las API de sus partners y proveedores, lo que añade otro reto a la gestión del riesgo de terceros en el sector del comercio electrónico.

La pérdida de la confianza de los reguladores puede resultar en un mayor escrutinio, lo que a su vez supondría más trabajo para los equipos, que ya atraviesan dificultades para satisfacer las exigencias en materia de cumplimiento. Además, esto podría acarrear la imposición de multas cuantiosas. Habida cuenta de los costes, no cabe duda de que las empresas de comercio electrónico y retail son plenamente conscientes de las consecuencias financieras de las amenazas de API. Por primera vez, solicitamos a los encuestados de los tres países participantes que divulgaran el impacto financiero estimado de los incidentes de seguridad de las API que han experimentado en los últimos 12 meses.

<sup>3</sup> GARTNER es una marca comercial registrada y una marca de servicio de Gartner, Inc. o sus afiliados en EE. UU. y otros países, y se usa aquí con permiso. Todos los derechos reservados.

	Retail y comercio electrónico	Media del sector
 EE. UU.	<b>526 531 \$</b>	<b>591 404 \$</b>
 Reino Unido	<b>258 815 £</b>	<b>420 103 £</b>
 Alemania	<b>348 467 €</b>	<b>403 453 €</b>

P. Si ha sufrido algún incidente de seguridad de API, ¿cuál ha sido el impacto financiero total estimado de estos incidentes combinados? Incluya todos los costes relacionados, como reparaciones del sistema, tiempo de inactividad, honorarios legales, multas y cualquier otro gasto asociado. n=1207

Si bien los impactos financieros son significativos, los participantes del estudio afirmaron con seguridad que los costes no solo afectan a los resultados empresariales. Cuando se les pidió que enumeraran el impacto principal de un incidente de seguridad de API, este no era un coste económico. Nuestros encuestados de comercio electrónico y del sector retail hicieron hincapié en la carga para los trabajadores: el estrés y la presión sobre sus equipos.

#### Las 5 principales repercusiones de los incidentes de seguridad de API para las empresas de comercio electrónico y del sector retail

1. Aumento del estrés o la presión para mi equipo o departamento: **28,7 %**
2. Costes para intentar solucionar el problema: **28,0 %**
3. Daños a la reputación de nuestro departamento ante los altos puestos y la junta directiva: **25,3 %**
4. Mayor escrutinio interno de nuestro equipo o departamento por parte de la empresa: **23,3 %**
5. Sanciones por parte de los reguladores: **25,3 %**

P. ¿Qué costes o impactos han tenido en su empresa los incidentes de seguridad de API? (Seleccione un máximo de 3); n=1207

## Siguientes pasos: Reducción del riesgo y el estrés mediante la seguridad proactiva de API

Los ataques de API contra empresas de comercio electrónico y retail aumentan en alcance, escala y sofisticación. Esto incluye los ataques de bots impulsados por IA generativa, que se adaptan rápidamente para eludir las herramientas de seguridad de API tradicionales y otras defensas perimetrales. Muchos equipos de seguridad de su sector están experimentando estas amenazas de primera mano y padecen las consecuencias, tanto en términos financieros como humanos. Con todo, incluso cuando las organizaciones comprenden la importancia de las amenazas de API, se plantean la siguiente pregunta: ¿Qué podemos hacer?

Tomar medidas ya para proteger mejor sus API, así como los datos que intercambian, puede permitir a su organización proteger sus ingresos y aliviar la carga de los equipos de seguridad; todo ello al tiempo que se mantiene la confianza que tanto les ha costado ganarse de las juntas directivas y los clientes. Entre estos pasos se incluye el desarrollo de los conocimientos de su equipo sobre las amenazas de API avanzadas y las capacidades necesarias para defenderse ante ellas.



Para leer el informe completo y obtener más información sobre las prácticas recomendadas en materia de visibilidad y protección de API, descargue el [Estudio sobre el impacto de la seguridad de API de 2024](#).

¿Todo listo para hablar sobre sus retos y descubrir cómo puede ayudarle Akamai?

[Solicite una demostración personalizada de la solución Akamai API Security](#)



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 prevenir las, 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](https://akamai.com) y [akamai.com/blog](https://akamai.com/blog), o siga a Akamai Technologies en [X](#), antes conocido como Twitter, y [LinkedIn](#). Publicado en noviembre de 2024.