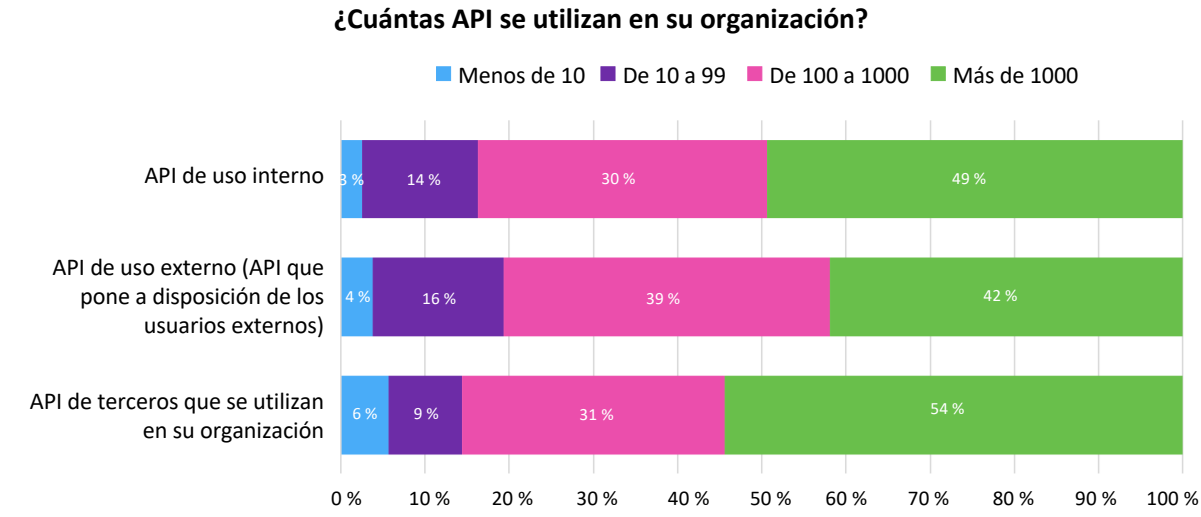
Figura 1: Número de API en uso



Nota: n=160
Fuente: Omdia

El uso de API está aumentando. Al mismo tiempo, muchos de nuestros encuestados indicaron incidentes de seguridad de API con problemas específicos, como la exfiltración de registros internos y el scraping de datos a gran escala.

Este escenario significa que las empresas deberían aumentar sus esfuerzos en materia de seguridad de API ahora mismo, ya que el aumento de las API solo va a continuar, agravando así los problemas de seguridad a menos que se tomen estas medidas. Con el aumento del número de API, la superficie de ataque seguirá expandiéndose, lo que dará lugar a incluso más ataques potenciales.

Información breve sobre la seguridad de API

El flujo común de seguridad de API se centra en cuatro casos de uso principales que funcionan en un bucle infinito, a diferencia del ciclo de creación, despliegue, ejecución y supervisión que se utiliza en DevOps:

- **Detección de las API que se utilizan en los entornos:** esto se puede hacer de muchas formas diferentes, incluida la ingesta de definiciones de OpenAPI (Swagger), el análisis de repositorios de código y el análisis activo de entornos. La mayoría de las API se detectan mediante el análisis del tráfico. La carga de archivos de especificaciones de API es una táctica que se utiliza menos y solo es posible cuando la organización ya sabe qué API tiene. Además, ningún enfoque es suficiente: la combinación de análisis continuo del tráfico y de repositorios probablemente proporcione una visión completa del uso de API en las organizaciones.

  Las organizaciones deben tener en cuenta las consideraciones de seguridad de API en toda su infraestructura tecnológica, no solo en los entornos específicos de API. En muchos casos, la gestión del uso de API heredadas requiere un enfoque diferente.