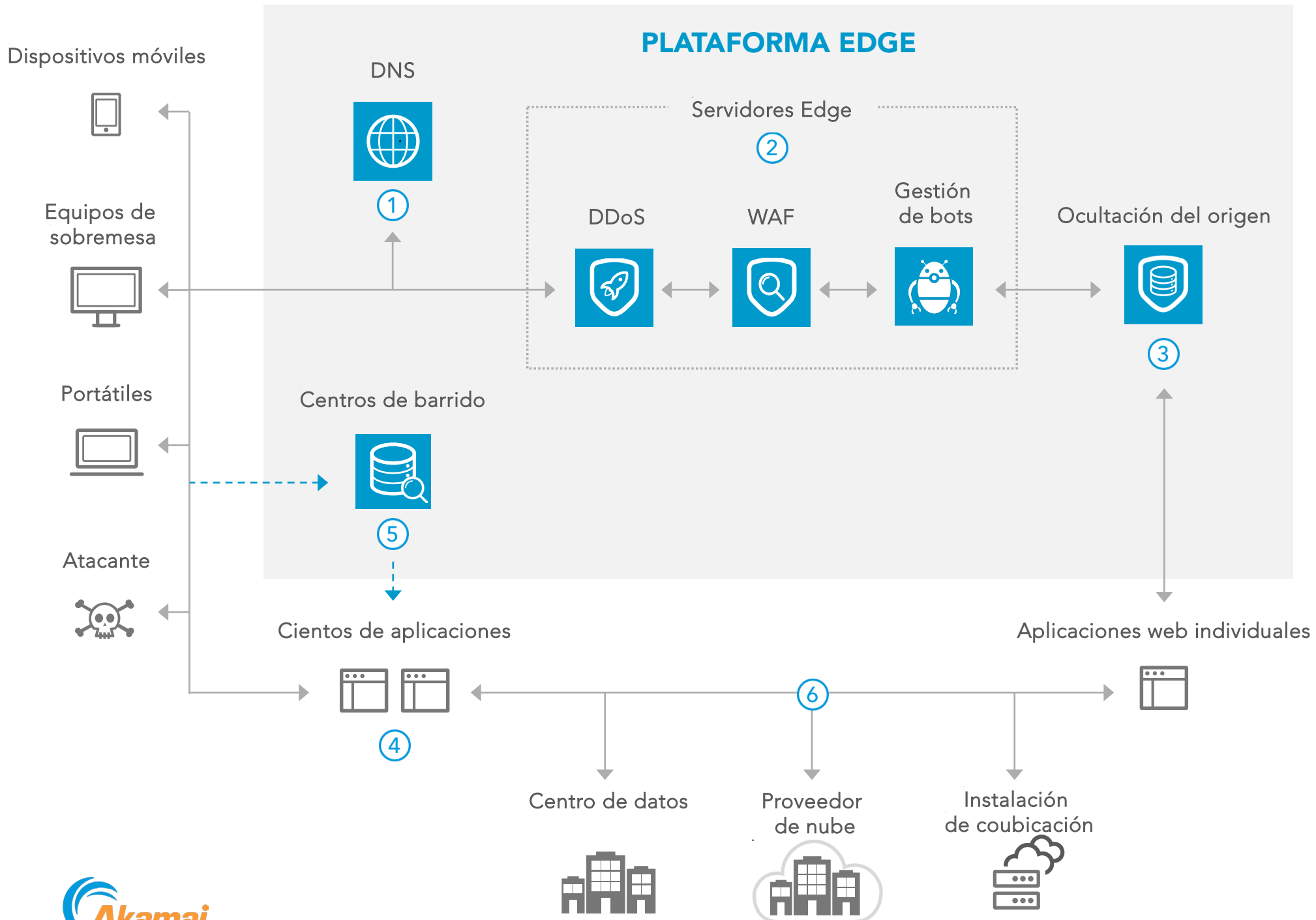


PROTECCIÓN CONTRA DDoS

Arquitectura de referencia



DESCRIPCIÓN GENERAL

Akamai mitiga el riesgo de sufrir ataques DDoS con una protección rápida y efectiva que está diseñada para contrarrestar los ataques DDoS de mayor tamaño y complejidad, independientemente de si las aplicaciones están implementadas en un centro de datos, en una infraestructura de nube pública o en una instalación de coubicación.

- 1 Los clientes realizan una búsqueda de DNS en el servicio de DNS de Akamai, que ha absorbido incluso los ataques DDoS de mayor impacto.
- 2 Los servidores Edge, ubicados en el borde de Internet, inspeccionan automáticamente el tráfico de CDN en busca de ataques DDoS, ataques dirigidos a aplicaciones web y ataques de bots, y bloquean las amenazas maliciosas.
- 3 Akamai enruta el tráfico de la CDN a través de servidores Edge designados, lo que permite a los clientes reducir el tráfico proveniente de otros orígenes y evitar que los atacantes eludan la protección basada en el Edge.
- 4 El tráfico que no es de la CDN se suele enrutar directamente al origen de acuerdo con los anuncios de ruta BGP del cliente.
- 5 Los clientes pueden enrutar el tráfico a través de los centros de barrido de Akamai (como servicio siempre activado o bajo demanda), en los que se bloquean los ataques DDoS mediante protocolos de mitigación proactiva o mediante la mitigación activa de SOC.
- 6 Los servicios de Akamai, tanto los basados en la CDN como los de barrido de DDoS, pueden proteger las aplicaciones implementadas en la infraestructura de los clientes, ya sea un centro de datos, una nube pública o una instalación de coubicación.

PRODUCTOS CLAVE

DNS ▶ Edge DNS

DDoS/WAF ▶ Kona Site Defender o Web Application Protector

Bot ▶ Bot Manager

Centros de barrido ▶ Prolexic Routed

