**Mitigaciones clave contra DdoS**

1. **Prevención en la capa de red / entrega**

* **Protección a nivel de infraestructura y red**: usar firewalls, routers y balanceadores de carga configurados para limitar tráfico no legítimo y prevenir saturación.
* **Servicios de mitigación DDoS en la nube**: integrar proveedores de mitigación como Cloudflare, AWS Shield, Akamai, que absorben y filtran tráfico malicioso antes de llegar a la app.
* **Rate limiting / throttling**: limitar el número de solicitudes por IP, región o usuario en endpoints críticos (login, API).
* **Filtrado de tráfico sospechoso**: bloquear IPs, ASN (Número de Sistema Autónomo) para bloquear rangos de IP's o rangos conocidos de origen malicioso usando feeds reputacionales.
* **Redundancia y escalabilidad**: arquitectura distribuida con múltiples instancias, balanceo de carga y failover automático para soportar picos de tráfico.

1. **Educación y conciencia del equipo**

* **Formación del personal de operaciones**: capacitar en detección temprana de ataques DDoS y patrones de tráfico anómalo.
* **Simulaciones de tráfico malicioso**: realizar pruebas controladas de estrés y ataque para evaluar la resiliencia de la infraestructura.
* **Políticas internas claras**: definir quién puede activar mitigaciones manuales y protocolos de escalamiento en caso de ataque.

1. **Detección y enriquecimiento (Data / AI)**

* **Monitoreo de tráfico en tiempo real**: analizar métricas como número de requests, tasa de errores 5xx, latencia y saturación de recursos.
* **Análisis de patrones de tráfico**: Machine Learning para detectar anomalías en volumen, origen geográfico, comportamiento de usuario o API.
* **Correlación con Threat Intel**: listas de IPs maliciosas, rango de IP's sospechosos, ataques históricos reportados en feeds públicos y privados.
* **Reglas Sigma / SIEM**: alertas automáticas cuando el tráfico supera umbrales definidos, se detectan picos inusuales o patrones de flooding.
* **Detección de botnets y tráfico automatizado**: análisis de user-agent, headers, comportamiento de sesión y secuencias de requests.

1. **Respuesta y mitigación automatizada**

* **Bloqueo automático de IPs / rangos** cuando se detecta tráfico malicioso repetitivo.
* **Rate limiting dinámico** y **throttling** por usuario, región o endpoint crítico.
* **Redirección de tráfico a scrubbing centers** (servicios de mitigación de DDoS en la nube).
* **Escalado automático de infraestructura**: añadir instancias o balancear carga para absorber picos de tráfico legítimo y malicioso.
* **Notificación y coordinación**: alertar a administradores y equipo de operaciones, generar tickets automáticos y documentar el incidente.

1. **Herramientas, procesos y gobernanza**

* **Integración con dashboards**: visualizar métricas de tráfico, alertas de saturación y patrones sospechosos en tiempo real.
* **Playbooks documentados**: pasos automáticos y manuales para mitigación de ataques DDoS, incluyendo escalamiento a proveedores de mitigación.
* **Retención de evidencia**: logs de tráfico, picos de requests y métricas de red para análisis forense y mejora continua.
* **Simulaciones periódicas**: pruebas controladas de resiliencia frente a ataques para reentrenar modelos y ajustar umbrales de detección.
* **Automatización de alertas y respuestas**: integración con herramientas de orquestación para ejecutar bloqueos, throttling y escalado sin intervención manual inmediata.