Playbook de Respuesta ante Ataque DDoS

TechNova Solutions S.L.

1. Introducción

Este documento describe el protocolo oficial de TechNova Solutions S.L. ante un ataque de Denegación de Servicio Distribuida (DDoS). El propósito es garantizar una respuesta rápida, coordinada y efectiva para minimizar el impacto en la disponibilidad de servicios, mitigar el tráfico malicioso y restaurar la operativa normal.

- Ámbito de aplicación: Infraestructura de red, servicios en la nube, aplicaciones web y APIs.

- Frecuencia de revisión: Semestral o tras un incidente significativo.

2. Escenario

Se detecta un aumento inusual de tráfico hacia los servicios críticos, provocando latencias elevadas o indisponibilidad.

Ejemplo:

El martes 22 de abril de 2025, a las 14:30h, el sistema de monitorización alerta de un pico de 10 Gbps dirigido al balanceador de carga de la aplicación web. Los usuarios experimentan tiempos de respuesta >5 segundos e intermitencias.

3. Objetivos

☑Detectar y mitigar el tráfico malicioso de forma inmediata.

☑Mantener la disponibilidad de servicios esenciales.

☑Coordinar con proveedores de red y seguridad externa.

☑Preservar evidencias para análisis de tráfico.

☑Notificar a las autoridades y partes interesadas si procede.

☑Revisar y reforzar controles post-incidente.

4. Roles y Responsabilidades

Rol	Responsabilidad
Empleado	Reportar anomalías de servicio al equipo de Operaciones.
Equipo de Operaciones	Verificar alertas de monitoreo y recopilar métricas de tráfico.
CISO / DPO	Coordinar la respuesta, evaluar el impacto y decidir notificaciones.
Redes	Implementar filtros de tráfico (ACLs, listas negras) y ajustar balanceadores.
Proveedor de CDN / ISP	Colaborar en la absorción y filtrado de tráfico malicioso.
Seguridad (SOC / SIEM)	Analizar patrones de ataque y activar reglas de mitigación en WAF/IPS.
Infraestructura Cloud	Ajustar escalado y políticas de seguridad en la nube.
Comunicación	Gestionar la comunicación interna y externa, incluyendo status pages.
Legal	Asesorar sobre implicaciones legales y coordinación con autoridades.

5. Procedimiento de Respuesta

Fase 1: Detección y Alerta

☑Monitorizar umbrales de tráfico y latencia.

☑Generar ticket automático en la herramienta de ITSM.

☑Notificar al equipo de respuesta.

Fase 2: Contención y Mitigación

☑Activar filtros en CDN/Firewall (Blackholing, Geo-IP).

☑Implementar rate limiting y ACLs en routers/core.

☑Escalar recursos en la nube para absorción de picos.

Fase 3: Análisis y Erradicación

☑Capturar y almacenar logs de tráfico y pcap para forense.

☑Identificar patrones (botnets, reflection/amplification).

☑Ajustar reglas en WAF/IDS para bloquear firmas.

Fase 4: Recuperación y Verificación

☑Verificar restauración de niveles de servicio (SLA).

☑Cerrar filtros temporales cuando sea seguro.

☑Documentar métricas de antes/durante/después del ataque.

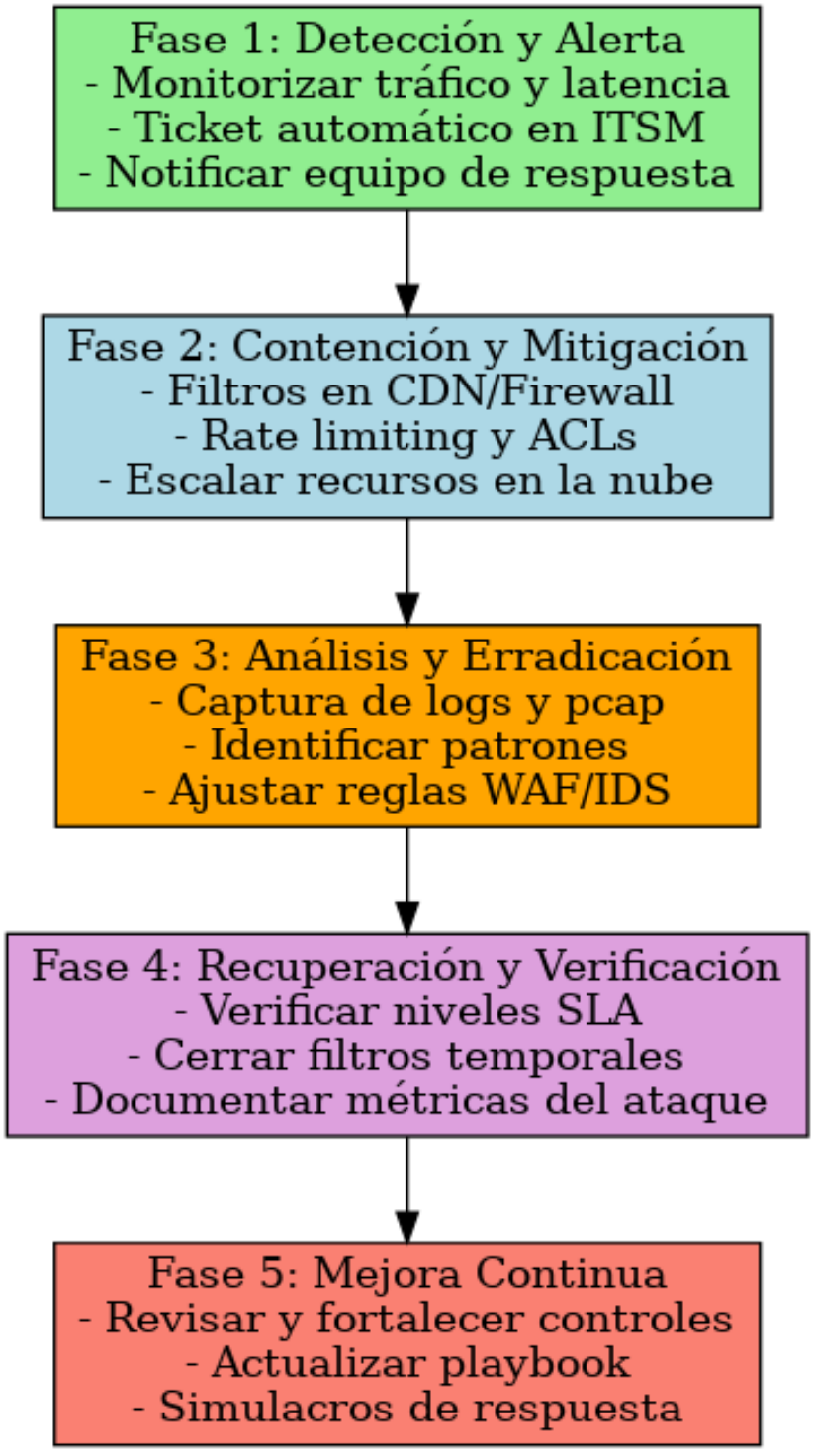
Fase 5: Mejora Continua

☑Revisar punto de entrada y fortalecer controles.

☑Actualizar playbook con lecciones aprendidas.

☑Realizar simulacros de respuesta DDoS periódicos.

6. Diagrama de Flujo del Procedimiento



7. Herramientas Recomendadas

Fase	Herramienta	Función
Detección y Alerta	Zabbix (https://www.zabbix.com), Grafana (https://grafana.com)	Alertas de tráfico y métricas de rendimiento
Contención y Mitigación	Cloudflare (https://www.cloudflare.com), Akamai (https://www.akamai.com)	Filtrado a nivel de borde, WAF y blackholing
Análisis y Erradicación	Wireshark (https://www.wireshark.org), TCPdump (https://www.tcpdump.org)	Captura y análisis de paquetes
Contención y Análisis	Fortinet (https://www.fortinet.com), Palo Alto Networks (https://www.paloaltonetworks.com)	IPS/IDS y filtrado avanzado
Contención y Mitigación	AWS Auto Scaling (https://aws.amazon.com/autoscaling), Azure Scale Sets (https://azure.microsoft.com)	Absorción de picos mediante autoescalado
Detección y Análisis	Splunk (https://www.splunk.com), Elastic Security (https://www.elastic.co/security)	Correlación de eventos y detección de anomalías
Gestión Integral	ServiceNow (https://www.servicenow.com), Jira Service Management (https://www.atlassian.com/software/jira/service-management)	Rastreo y documentación de acciones

8. Notificación a Autoridades

Ejemplo de información a incluir en la notificación:

Debe realizarse cuando el ataque comprometa infraestructuras críticas, afecte datos de usuarios o sea de gran escala.

Organismos:

- INCIBE-CERT: https://www.incibe-cert.es

- CERT-EU: https://cert.europa.eu

Datos requeridos:

Campo	Descripción
Fecha y hora de inicio	22 de abril de 2025, 14:30h
Fecha y hora de mitigación	22 de abril de 2025, 15:10h
Servicios afectados	Aplicación web principal, API pública
Alcance del ataque	10 Gbps sostenidos durante 40 minutos
Tipo de ataque	DDoS por amplificación UDP (DNS y NTP)
Medidas adoptadas	Blackholing en CDN, escalado en nube, filtrado Geo-IP, ajuste de WAF
Responsable del análisis	SOC TechNova / CISO
Evidencia adjunta	Logs de tráfico, capturas PCAP, alertas de Zabbix y Splunk
Autoridad notificada	INCIBE-CERT ((https://www.incibe-cert.es)

9. Prevención y Formación

☑Simulacros trimestrales de ataques DDoS.

☑Formación de equipos en configuración de filtros y escalado.

☑Implementación de arquitectura de mitigación distribuida.

☑Políticas de redundancia y multi-ISP.

☑Actualización continua de firmas de IPS/IDS.

10. Bibliografía

INCIBE. (2024). Guía de protección ante ataques DDoS. https://www.incibe.es

Cloudflare. (s.f.). Understanding and Mitigating DDoS attacks. https://www.cloudflare.com

OWASP. (2023). OWASP DDoS Prevention Cheat Sheet. https://owasp.org

Arbor Networks. (2022). Worldwide Infrastructure Security Report. https://www.arbornetworks.com