Ataque de denegación de servicio (DDoS)

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Responsables de infraestructura, redes y servicios en línea.

Qué hacer cuando un sitio o servicio deja de responder porque lo saturan con tráfico. El objetivo es restablecer el servicio con ayuda del proveedor y verificar que el ataque no esté ocultando otra intrusión.

Señales de que está ocurriendo

- Sitio o aplicación lentos o inaccesibles para todos los usuarios.
- Aumento repentino de tráfico desde muchas direcciones o desde un solo país.
- Ancho de banda, CPU o conexiones del servidor al límite.
- Mensaje de extorsión que amenaza con un ataque o lo reivindica.

Qué tan grave es

Crítica	Servicio esencial al público caído por más de una hora, o ataque con extorsión.
Alta	Servicio degradado para la mayoría de usuarios.
Media	Ataque absorbido por la protección, con impacto menor.

Primera hora

- [ ] **1.** Confirma que es un ataque y no una falla interna ni un pico legítimo de visitas.
- [ ] **2.** Llama a tu proveedor de internet o de hosting y abre un caso de emergencia.
- [ ] **3.** Activa el modo de protección de tu CDN o WAF si cuentas con uno.
- [ ] **4.** Captura una muestra del tráfico y guarda los registros antes de que roten.
- [ ] **5.** Publica un aviso de estado por un canal alterno (redes sociales, página de estado).
- [ ] **6.** No respondas ni pagues si recibes un mensaje de extorsión.

Preparación (antes del incidente)

- Coloca los servicios públicos detrás de una CDN con protección anti-DDoS.
- Ten a mano el contacto de emergencia de tu proveedor y el procedimiento de mitigación.
- Conoce tu tráfico normal para poder reconocer lo anormal.
- Oculta la dirección IP de origen de tus servidores.

Detección y análisis

- Identifica el tipo: volumétrico, de protocolo o de capa de aplicación.
- Determina el objetivo exacto: dirección IP, puerto, URL o servicio DNS.
- Busca patrones: países de origen, agente de usuario, rutas solicitadas.
- Revisa si al mismo tiempo hay intentos de intrusión en otros sistemas.

Contención

- Pide al proveedor filtrado en su red o desvío a un centro de limpieza.
- Aplica límites de peticiones y bloqueos por país si tu público es local.
- Activa desafíos para navegadores en las rutas atacadas.
- Desactiva temporalmente las funciones más costosas (búsquedas, reportes).

Erradicación

- Cambia la dirección IP de origen si quedó expuesta y restringe el acceso sólo a la CDN.
- Cierra puertos y servicios que no deban estar publicados.
- Corrige los servicios propios que puedan usarse para amplificar ataques.

Recuperación

- Retira las restricciones por etapas mientras vigilas el tráfico.
- Mantén la protección reforzada al menos 72 horas: los ataques suelen repetirse.
- Comunica el restablecimiento por los mismos canales del aviso inicial.

Lecciones aprendidas

- Documenta duración, volumen máximo e impacto en el servicio.
- Evalúa si la capacidad de mitigación contratada fue suficiente.
- Prueba el procedimiento con el proveedor al menos una vez al año.

Evidencia que debes conservar

- Captura de tráfico (PCAP) o registros de flujo durante el ataque.
- Registros del servidor web, firewall y CDN.
- Gráficas de ancho de banda y de disponibilidad.
- Mensajes de extorsión, con cabeceras si llegaron por correo.

Qué no hacer

- Pagar una extorsión: no garantiza nada y te marca como objetivo.
- Reiniciar servidores una y otra vez sin haber filtrado el tráfico.
- Bloquear direcciones a mano una por una en un ataque distribuido.
- Suponer que sólo es un DDoS: puede ser una distracción.

A quién avisar

- Proveedor de internet, hosting o CDN.
- Usuarios y clientes, con un aviso de estado claro.
- Gerencia, con el impacto y el tiempo estimado.
- Ministerio Público, si hubo extorsión.
- cert.gt, para correlacionar con ataques a otras organizaciones.

Cuándo dar por cerrado el incidente

- El servicio opera con normalidad por 72 horas sin restricciones extraordinarias.
- La dirección de origen ya no es alcanzable directamente desde internet.
- Se descartó una intrusión paralela.
- El contrato o plan de mitigación fue revisado.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Guía general de buenas prácticas; no sustituye asesoría legal ni técnica especializada para tu caso. No es un documento de una entidad gubernamental. Puedes copiarla y adaptarla citando la fuente (CC BY 4.0).