GUÍA SENCILLA PARA
PREVENIR ATAQUES DDOS

Un ataque DDoS ocurre cuando muchas computadoras envían al mismo tiempo miles de solicitudes a un servicio en internet. Esto hace que la página o aplicación se vuelva lenta o deje de funcionar.

¿Qué es un ataque DDoS?

Es como si una multitud bloqueara la entrada de un edificio: los usuarios legítimos no pueden entrar porque la puerta está saturada. En internet, los atacantes usan miles de equipos infectados para generar ese bloqueo digital.

¿Cómo funciona?

- Los atacantes controlan computadoras o dispositivos comprometidos.
- Esos equipos envían tráfico masivo hacia un servidor.
- El servidor se sobrecarga y deja de atender a usuarios reales.

Riesgos asociados

- **Páginas web y servicios fuera de línea.**
- **Pérdida de confianza de clientes y usuarios.**
- **Costos económicos por interrupción.**
- **Posibilidad de que se aproveche para otros ataques.**

Pasos para prevenir y contrarrestar

- **Detectar** tráfico extraño con herramientas de monitoreo.
- **Analizar** si el tráfico es legítimo o malicioso.
- **Contener** el ataque usando filtros y bloqueos.
- **Erradicar** las conexiones maliciosas.
- **Monitorear** constantemente para evitar que vuelva a ocurrir.

Se recomienda

- Capacitar al personal en ciberseguridad.
- Mantener sistemas actualizados.
- Configurar reglas de seguridad en servidores y redes.
- Usar servicios especializados que bloqueen ataques masivos.
- Hacer simulacros de respuesta para estar preparados.

GOBIERNO DEL ECUADOR
Agencia de Regulación y Control de las Telecomunicaciones
ecucert