# Informe sobre incidentes de ciberseguridad:

# Análisis de tráfico de red

|  |
| --- |
| Parte 1: Proporciona un resumen del problema encontrado en el registro de tráfico DNS e ICMP. |
| El registro indica que una IP cliente está realizando una consulta DNS al servidor a través del puerto 53, recibiendo de respuesta “udp port 53 unrecheable”, lo que indica que el puerto es inaccesible. Aquello puede indicar que el servidor DNS está caído. Esto podría deberse a un problema de configuración, mantenimiento o bloqueo por sobrecarga. |
|

|  |
| --- |
| Parte 2: Explica tu análisis de los datos y proporciona una solución para implementar |
| El incidente se produjo a las 13:24. Uno de los trabajadores identificó los problemas del servidor tras observar avisos de malfuncionamiento de la web. A través de un análisis más profundo utilizando herramientas de monitoreo de red, se determinó que el puerto 53 (utilizado para solicitudes DNS) se encontraba inaccesible. Investigando más a fondo, se identificó que el problema se debía a un ataque de denegación de servicio (DoS), en el que un conjunto específico de IPs estaba enviando un volumen inusualmente elevado de solicitudes DNS.  El ataque fue posible debido a que el servidor carecía de configuraciones avanzadas en el firewall para detectar y bloquear automáticamente IPs con un comportamiento sospechoso. Para mitigar el ataque, se implementaron reglas en el firewall para limitar la tasa de solicitudes DNS por IP, y se bloqueó manualmente el rango de IPs involucradas en el ataque. Esto permitió restablecer el funcionamiento del servidor y prevenir futuros ataques similares. |