# 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 tráfico capturado muestra que el cliente **192.51.100.15** intentó resolver el dominio yummyrecipesforme.com enviando solicitudes DNS al servidor **203.0.113.2** mediante el protocolo **UDP** en el puerto **53**.  El servidor respondió con mensajes **ICMP “udp port 53 unreachable”**, lo que indica que no había servicio escuchando en ese puerto o que estaba bloqueado por firewall.  Este comportamiento se repitió en varios intentos (13:24, 13:26 y 13:28) sin éxito, impidiendo que el navegador pudiera resolver el dominio y acceder al sitio web.. |
|

|  |
| --- |
| Parte 2: Explica tu análisis de los datos y proporciona una solución para implementar |
| **Análisis del incidente:**   * El problema se notificó cuando varios clientes no podían acceder a www.yummyrecipesforme.com y recibían el error “puerto de destino inalcanzable”. * Las capturas de tcpdump muestran intentos de resolución DNS en **UDP/53** desde el cliente al servidor **203.0.113.2**, con respuestas ICMP indicando puerto inaccesible. * Esto confirma una **falla en el servicio DNS**, lo que explica la imposibilidad de acceder al sitio.   **Presunta causa raíz:**   * El servicio DNS del servidor **203.0.113.2** no estaba operativo en **UDP/53**, * o el puerto estaba bloqueado por un firewall o lista de control de acceso.   **Estado actual del problema:** El sitio www.yummyrecipesforme.com continúa inaccesible, ya que no se logra resolución de nombres a través del DNS configurado.  **Propuesta de solución:**   1. Verificar que el servicio DNS en **203.0.113.2** esté en ejecución. 2. Comprobar reglas de firewall/red para permitir tráfico **UDP/53**. 3. Validar consultas DNS tanto por **UDP** como por **TCP** para confirmar operatividad. 4. Configurar servidores DNS redundantes (ej. 8.8.8.8, 1.1.1.1) para tolerancia a fallas. 5. Implementar monitoreo y alertas sobre disponibilidad del puerto **53**. |