📄 PRIMERA PARTE DEL EJERCICIO

Eres el responsable de seguridad TIC de la **Consellería de Educación de la Xunta de Galicia**, organismo público que gestiona infraestructuras críticas relacionadas con centros educativos, personal docente y plataformas académicas utilizadas por miles de usuarios diariamente.

La Consellería dispone de:

- Un CPD principal en Santiago de Compostela
- Servicios internos (Active Directory, servidores de archivos, bases de datos académicas)
- Acceso remoto mediante VPN corporativa con autenticación multifactor
- Monitorización mediante IDS/IPS y SIEM

Tus responsabilidades incluyen:

- Supervisión de alertas del SOC
- Coordinación de la respuesta ante incidentes
- Clasificación y documentación en la herramienta LUCIA
- Comunicación con el CCN-CERT en caso de incidente relevante
- Preservación de evidencias digitales
- Coordinación con sistemas y dirección

Situación inicial

El lunes llegas puntual a tu puesto de trabajo y a las 09:06 recibes una alerta del IDS.

El sistema informa de que el servidor interno **SRV-EDU-02 (10.0.15.23)** ha enviado tráfico ICMP anómalo hacia la IP externa:

185.203.119.17

Detección

El IDS genera alerta por:

- ICMP con tamaño anómalo (1400 bytes)
- Repetición periódica cada 5 segundos.

📂 Clasificación inicial del incidente

Se realiza una clasificación preliminar.

Como estudiante, responde:

¿Cómo clasificarías inicialmente este incidente?

Posibles categorías:

- Acceso remoto legítimo + comportamiento anómalo
- Compromiso de cuenta
- Compromiso de servidor
- Canal de mando y control (C2) mediante ICMP
- Exfiltración encubierta (ICMP tunneling)

📊 Nivel de criticidad provisional

- Sistema afectado: servidor corporativo
- Comunicación externa sospechosa
- Potencial brecha de seguridad
- Posible impacto en datos personales

→ Nivel provisional: medio/alto (pendiente de análisis).

🌍 Acción immediata

¿Qué acciones tomas?

¿Mandas un tiquet a LUCIA?

🌍 Investigación inicial

1. Averigua a qué país pertenece la IP 185.203.119.17.
2. ¿Pertenece a un proveedor de hosting?
3. ¿Está asociada a alguna actividad maliciosa conocida?
4. ¿Es habitual que un servidor corporativo envíe tráfico ICMP de ese tamaño?
5. Abrirías un ticket mediante LUCIA?
6. ¿Qué fuentes OSINT utilizarías para esta investigación?
