# 📄 SEGUNDA PARTE DEL EJERCICIO

Después de la primera parte, deberías haber tomado acción. En este punto, ya era recomendable registrar el incidente en LUCIA como incidente en análisis, aunque todavía no estuviera confirmada la intrusión. Se configura el firewall perimetral para bloquear todo tráfico saliente desde el servidor SRV-EDU-02 hacia esa IP concreta o cualquier IP que no esté en una lista blanca. Decides investigar logins.

Tras el análisis inicial:

- El IDS confirmó múltiples paquetes ICMP de 1400 bytes
- Periodicidad constante cada 5 segundos
- Comunicación iniciada pocos minutos después del arranque de sesión

Habéis investigado la IP 185.203.119.17:

- Pertenece a un proveedor de hosting europeo
- No está asociada directamente a un organismo oficial
- Aparece en algunas bases OSINT vinculada a infraestructura de VPS

Para evitar posibles exfiltraciones de datos, decidís aplicar una medida de contención:

> Se configura el firewall perimetral para bloquear todo tráfico saliente desde el servidor SRV-EDU-02 hacia el exterior.

De momento, el tráfico ICMP cesa.

Recuerda, no apages el servidor (elimina evidencias en la RAM) ni cortes todo el tráfico saliente de la red, desde todos los dispositivos. No tienes pruebas de que haya movimiento laterales en la red.

---

## 🔐 Revisión de autenticaciones

Decides revisar los logs de autenticación del servidor.

Observas lo siguiente:

- Usuario: **jlopez**
- Hora de autenticación: 09:01
- Tipo de acceso: remoto
- IP origen: 185.203.119.17

---

# ❓ Preguntas para el alumnado

1. ¿Te parece normal que un usuario corporativo se autentique desde una IP perteneciente a un proveedor de hosting?
2. ¿Utilizó VPN corporativa?
3. ¿Qué hipótesis gana más peso ahora?
4. ¿Crees que el servidor está comprometido o la cuenta está comprometida?
5. ¿La medida aplicada (bloquear salida en firewall) es suficiente?
6. ¿Podría haberse perdido evidencia con esta acción?
7. En este punto, ¿deberías haber abierto ya un ticket en LUCIA?

---