🛠️ Ejercicio Práctico

📌 **Título:** Análisis de Seguridad y Mitigación en un Módulo de Administración

---

🎯 Objetivo:

Analizar un módulo de una aplicación web con múltiples vulnerabilidades, **identificar los riesgos existentes** y **proponer medidas de mitigación concretas**, justificando la elección de cada una.

🧱 Escenario:

La empresa **TechData** ha desarrollado un panel de administración para gestionar usuarios, reportes y contenido. Durante una auditoría inicial, se detectan los siguientes problemas:

1. El formulario de búsqueda de usuarios permite escribir directamente en una caja de texto sin validación y los resultados se imprimen sin codificación en el HTML.

2. Un endpoint expone los datos de todos los usuarios (`/admin/users/export`) sin requerir autenticación ni validación de rol.

3. El sistema usa una librería JavaScript obsoleta que aparece listada con vulnerabilidades críticas en Snyk y aún no ha sido actualizada.

4. Se detectaron intentos de ejecución automatizada de scripts desde dominios externos que apuntan al botón "Eliminar usuario".

📋 Actividades:

1. Identifica el tipo de vulnerabilidad en cada uno de los cuatro casos.

2. Propón al menos una técnica de mitigación adecuada por cada caso.

3. Justifica brevemente por qué esa técnica es apropiada y cómo reduce el riesgo.

4. Indica cuál de los cuatro problemas priorizarías corregir primero y por qué.

📌 Formato sugerido de respuesta:

Caso	Vulnerabilidad Identificada	Técnica de Mitigación	Justificación
1			
2			
3			
4			

✍️ Recomendaciones:

- Puedes basarte en técnicas como: validación de entradas, escape de salida, control de acceso por roles (RBAC), CSP, tokens CSRF, actualización de dependencias, uso de WAF, etc.
- Considera incluir código o referencias a herramientas como parte de tu respuesta (opcional).
- Fundamenta bien tu prioridad de mitigación según riesgo, impacto y facilidad de explotación.

📦 Entregables esperados:

- Tabla completa con los 4 casos.
- Justificación clara y técnica.
- Argumento sobre la prioridad de intervención.
- (Opcional) Fragmentos de código ilustrativos.
