Elaborar un análisis de amenazas previo a la auditoría e identificación de invariantes para **KipuBankV3**, con el fin de prepararlo para el despliegue en mainnet.

Descripción de la Tarea

El ciclo de vida de un proyecto Web3 debe estar impregnado de **DevSecOps**, y el *Ethereum Developer Pack* ha enseñado este enfoque desde la primera clase. Ahora, es momento de poner todo el conocimiento a prueba.

Este examen final cerrará tu recorrido para convertirte en un desarrollador de Solidity bien preparado y con mentalidad de seguridad. Para ello, ha llegado el momento de completar el espacio pendiente en el desarrollo de **KipuBankV3**, preparándolo para una auditoría y un entorno de producción.

Entregable

Debes presentar un **Informe de Análisis de Amenazas** que incluya:

1. Breve descripción general de cómo funciona KipuBankV3

→ Demuestra comprensión de la lógica y los componentes del protocolo.

2. Evaluar la madurez del protocolo

→ Identificar debilidades del protocolo y pasos faltantes para alcanzar la madurez.

- Cobertura de pruebas;
- Métodos de prueba;
- Documentación;
- Roles y poderes de los actores del protocolo;
- Invariantes.

3. Vectores de ataque y modelo de amenazas

→ Identificar al menos **3 superficies o escenarios de ataque**, incluyendo:

- Errores en la lógica de negocio del contrato inteligente;
- Uso indebido o abuso de supuestos del protocolo;
- Estrategias económicas/exploitativas;
- Problemas de permisos o de configuración de control de acceso.

4. Especificación de invariantes

→ Identificar al menos **3 invariantes del protocolo**.

⚠ Los invariantes son propiedades que **siempre deben cumplirse**, sin importar el escenario.

5. Impacto de las violaciones de invariantes

→ Los invariantes son partes críticas del sistema. Al identificarlos, también debes identificar su impacto en escenarios adversos.

6. Recomendaciones

→ Proporcionar recomendaciones claras sobre cómo validar los invariantes encontrados.

7. Conclusión y próximos pasos

→ Evaluar cualquier otra acción necesaria para alcanzar la madurez del protocolo y completar la preparación para una auditoría.

Consideraciones Finales

Este examen es más que una prueba: es una simulación de lo que los desarrolladores de Solidity deben hacer en la vida real para garantizar que sus protocolos sean **seguros, maduros y listos para producción**.

Al realizar un análisis de amenazas, identificar invariantes y pensar en escenarios adversarios, estás adoptando la mentalidad tanto de un investigador en seguridad como de un ingeniero de protocolos responsable.

Comprender cómo **probar, romper y fortalecer tu propio sistema** es una de las habilidades más valiosas en el desarrollo Web3. Los proyectos que se lanzan sin estos pasos se exponen —y exponen a sus usuarios— a fallos potencialmente catastróficos.

Al completar esta tarea, demuestras que no solo eres capaz de escribir contratos inteligentes, sino que también entiendes cómo:

- Evaluar riesgos,
- Estructurar lógica segura,
- Comunicar hallazgos de forma efectiva,
- Y contribuir activamente a ecosistemas descentralizados más seguros.

Seguir estos pasos es lo que separa un despliegue amateur de código de un desarrollo de protocolos a nivel profesional.
Deja que este sea tu primer aporte de muchos hacia un **Ethereum más seguro**.