Ejercicio 3 - Curso de Cyberseguridad

Propietario: Franco Prieto
Revisor: José Antonio Muñoz
Colaboradores:
Generado en fecha: Fri Jan 16 2026

Resumen Ejecutivo

Descripción de alto nivel del sistema (high level system)

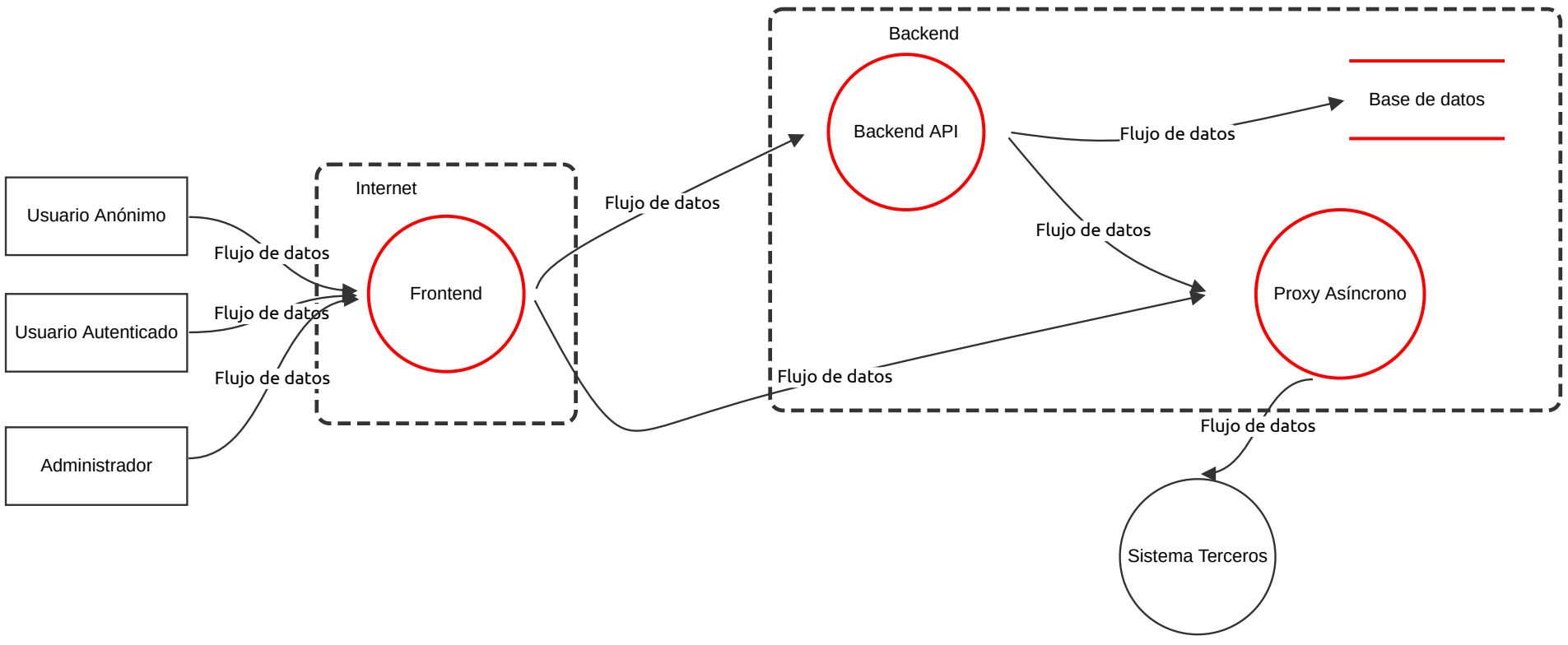
Ejercicio 3 - Modelado de Amenazas

Aplicación de Banco con la siguiente arquitectura:
- Frontend,
- Backend,
- Base de datos,
- Proxy asíncrono hacia otro sistema de terceros

Resumen

Total amenazas	11
Total amenazas mitigadas	0
No Mitigadas	11
Abierto / Crítica Prioridad	0
Abierto / Alta Prioridad	11
Abierto / Prioridad Media	0
Abierto / Baja Prioridad	0

App Banco - CIA



App Banco - CIA

Frontend (Proceso)

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
20	Exposición de credenciales y datos sensibles (CIA: Confidentiality)	Confidentiality - Confidencialidad	Alta	Abierto		Las credenciales de usuario (usuario/contraseña, tokens JWT, cookies de sesión) o datos financieros pueden ser interceptados o expuestos durante la transmisión o por un manejo inseguro en el frontend o backend. Esto puede ocurrir por: - Comunicación sin cifrado - Almacenamiento inseguro de tokens - XSS o robo de sesión	- Uso obligatorio de TLS 1.2+ en todas las comunicaciones - Cookies seguras - Cifrado de secretos y tokens en backend - Evitar almacenamiento de credenciales en el frontend

Backend API (Proceso)

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
21	Exposición de credenciales y datos sensibles (CIA: Confidentiality)	Confidentiality - Confidencialidad	Alta	Abierto		Las credenciales de usuario (usuario/contraseña, tokens JWT, cookies de sesión) o datos financieros pueden ser interceptados o expuestos durante la transmisión o por un manejo inseguro en el frontend o backend. Esto puede ocurrir por: - Comunicación sin cifrado - Almacenamiento inseguro de tokens - XSS o robo de sesión	- Uso obligatorio de TLS 1.2+ en todas las comunicaciones - Cookies seguras - Cifrado de secretos y tokens en backend - Evitar almacenamiento de credenciales en el frontend
22	Manipulación de transacciones financieras (CIA: Integrity)	Integrity - Integridad	Alta	Abierto		Modificación de datos críticos de transacciones como montos, destinatarios o estados de una transacción en caso de que los datos no son validados o protegidos adecuadamente. Esto puede darse por: - Falta de validación de integridad - Alteración de mensajes asíncronos - Ataques de replay sobre eventos de cobro	- Validaciones estrictas en backend (no confiar en el frontend) - Uso de firmas digitales - Controles de idempotencia en eventos de cobro - Logs transaccionales inmutables
23	Denegación de servicio sobre servicios críticos (CIA: Availability)	Availability - Disponibilidad	Alta	Abierto		El sistema puede quedar indisponible por: - Flood de requests (DoS) - Abuso de endpoints de autenticación o cobro - Saturación de colas asíncronas	- Limitación de solicitudes por tiempo por IP / usuario - Protección WAF / API Gateway - Timeouts y circuit breakers - Monitoreo y escalado automático

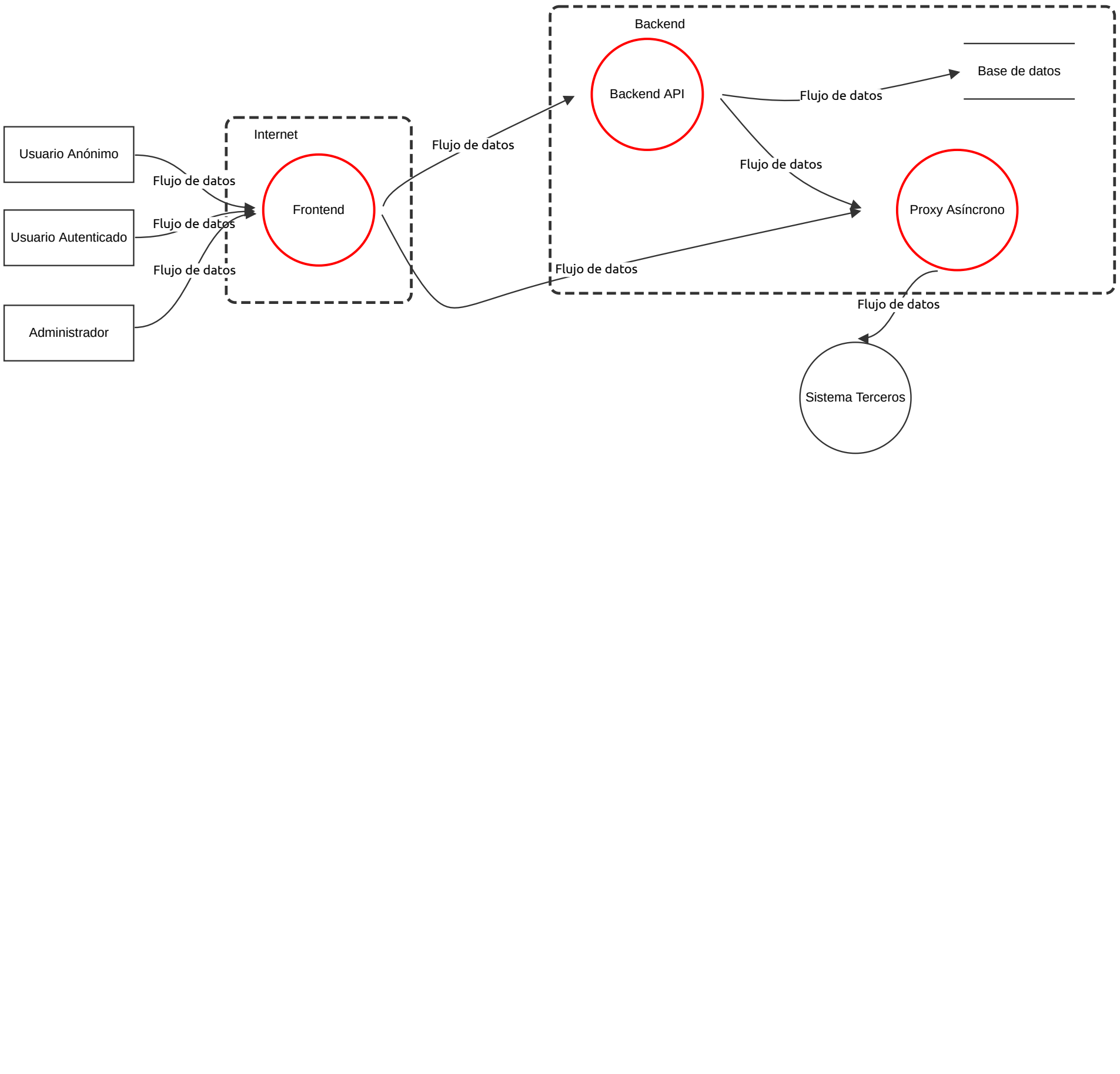
Base de datos (Dispositivo de almacenamiento)

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
24	Acceso no autorizado a datos persistentes (CIA: Confidentiality)	Confidentiality - Confidencialidad	Alta	Abierto		Acceso a información sensible (cuentas, balances, historiales de transacciones) si existen: - Credenciales débiles - Falta de segmentación de red - Ausencia de controles de acceso a nivel de aplicación o base de datos	- Control de acceso basado en roles - Principio de mínimo privilegio en usuarios de BD - Cifrado de datos en reposo (TDE / column-level encryption) - Separación de entornos (producción, test, etc)

Proxy Asíncrono (Proceso)

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
25	Manipulación de transacciones financieras (CIA: Integrity)	Integrity - Integridad	Alta	Abierto		Modificación de datos críticos de transacciones como montos, destinatarios o estados de una transacción en caso de que los datos no son validados o protegidos adecuadamente. Esto puede darse por: - Falta de validación de integridad - Alteración de mensajes asíncronos - Ataques de replay sobre eventos de cobro	- Validaciones estrictas en backend (no confiar en el frontend) - Uso de firmas digitales - Controles de idempotencia en eventos de cobro - Logs transaccionales inmutables
26	Denegación de servicio sobre servicios críticos (CIA: Availability)	Availability - Disponibilidad	Alta	Abierto		El sistema puede quedar indisponible por: - Flood de requests (DoS) - Abuso de endpoints de autenticación o cobro - Saturación de colas asíncronas	- Limitación de solicitudes por tiempo por IP / usuario - Protección WAF / API Gateway - Timeouts y circuit breakers - Monitoreo y escalado automático

App Banco - STRIDE



App Banco - STRIDE

Frontend (Proceso)

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
15	Suplantación de identidad (STRIDE: S)	Spoofing	Alta	Abierto		Un atacante puede hacerse pasar por un usuario legítimo (usuario autenticado o administrador) utilizando: - Credenciales robadas - Tokens de sesión comprometidos - Ataques de phishing o fuerza bruta	- Autenticación fuerte - Gestión segura de sesiones (expiración, rotación de tokens) - Protección contra fuerza bruta (bloqueos progresivos) - Uso de HTTPS obligatorio

Backend API (Proceso)

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
17	Repudio de acciones (STRIDE: R)	Repudiation	Alta	Abierto		Un usuario o administrador puede negar haber realizado una operación (por ejemplo, un cobro o un cambio administrativo) si no existen evidencias confiables que lo prueben.	- Logs de auditoría inmutables - Identificadores únicos de transacción - Registro de usuario, timestamp y origen - Firma de operaciones sensibles Retención segura de logs
19	Escalada de privilegios (TRIDE: E)	Elevation of privilege	Alta	Abierto		Un usuario autenticado puede ejecutar funciones reservadas a un administrador debido a: - Fallas en controles de autorización - Endpoints mal protegidos - Confianza excesiva en datos del frontend Esto permite acciones críticas no autorizadas.	- Control de acceso basado en roles - Principio de mínimo privilegio - Autorización centralizada en backend - Separación de funciones (segregation of duties) Pruebas de seguridad sobre endpoints

Proxy Asíncrono (Proceso)

Número	Título	Tipo	Prioridad	Estado	Puntuación	Descripción	Mitigaciones
18	Repudio de acciones (STRIDE: R)	Repudiation	Alta	Abierto		Un usuario o administrador puede negar haber realizado una operación (por ejemplo, un cobro o un cambio administrativo) si no existen evidencias confiables que lo prueben.	- Logs de auditoría inmutables - Identificadores únicos de transacción - Registro de usuario, timestamp y origen - Firma de operaciones sensibles Retención segura de logs