Casos de Abuso

Caso de Abuso 1: Spoofing Biomético / Deepfake

- **Descripción:** Un atacante intenta burlar el mecanismo de autenticación biométrica utilizando una fotografía de alta resolución, un molde de huella dactilar o software de emulación de cámara para inyectar una imagen falsa (Deepfake) y hacerse pasar por un usuario legítimo.
- **Categoría STRIDE: S**poofing (Suplantación).
- **Probabilidad: Media**. Requiere acceso físico al dispositivo o compromiso del canal de video/sensor, además de recursos técnicos específicos.
- **Impacto: Alto**. Si tiene éxito, el atacante accede a la cuenta sin necesitar la contraseña (si la biometría es el único factor) o supera el segundo factor.
- **Mitigación:** Implementación de TOTP obligatorio como factor complementario (algo que tienes + algo que eres) y uso de APIs nativas del dispositivo que verifican "liveness" (prueba de vida) a nivel de hardware.

Caso de Abuso 2: Ataque de Replay de Token

- **Descripción:** Un atacante intercepta la comunicación HTTP entre el Frontend (Next.js) y el Backend (FastAPI). Captura un paquete válido que contiene un código TOTP o un Token JWT recién emitido y lo reenvía al servidor segundos después para intentar duplicar la sesión o ejecutar una acción autorizada.
- **Categoría STRIDE: T**ampering (Manipulación) / **I**nformation Disclosure.
- **Probabilidad: Media**. Requiere estar en la misma red (MitM) si no se usa HTTPS correctamente.
- **Impacto: Alto**. Podría permitir el acceso no autorizado o la duplicación de transacciones.
- **Mitigación:** Uso estricto de **HTTPS (TLS 1.3)** para cifrar el canal. En el backend, el servicio TOTP implementa una ventana de tiempo estricta (30 segundos) y evita la reutilización del mismo código (One-Time use enforcement).

Caso de Abuso 3: Escalada de Privilegios vía Manipulación de JWT

- **Descripción:** Un usuario registrado con el rol de CLIENT intercepta su propio Token JWT, decodifica el payload, modifica el campo "role": "CLIENT" a "role": "ADMIN", vuelve a firmar el token (intentando explotar debilidades como el algoritmo 'None' o fuerza bruta a la clave secreta) y lo envía para acceder al Dashboard de Administrador.
- **Categoría STRIDE: E**levation of Privilege (Elevación de Privilegios).

- **Probabilidad: Baja**. Depende de la robustez de la SECRET_KEY y la configuración de la librería JWT.
- **Impacto: Crítico**. Compromiso total del sistema, acceso a datos de todos los usuarios y capacidad de modificación.
- **Mitigación:** Validación de firma criptográfica robusta en el Backend (Auth Service) usando algoritmos seguros (HS256/RS256) y una clave secreta compleja y rotativa. Validación de roles en cada endpoint protegido (dependencies.py en FastAPI).

Caso de Abuso 4: Credential Stuffing / Fuerza Bruta

- **Descripción:** Un atacante utiliza una base de datos de correos y contraseñas filtrados de otros sitios web para intentar iniciar sesión masivamente en el sistema, automatizando miles de intentos por minuto.
- **Categoría STRIDE: D**enial of Service (DoS) / **S**poofing.
- **Probabilidad: Alta**. Es el ataque más común en sistemas públicos.
- **Impacto: Medio/Alto**. Bloqueo de cuentas de usuarios legítimos y posible compromiso de cuentas con contraseñas débiles.
- **Mitigación:** Implementación de **Rate Limiting** (límite de peticiones) en el API Gateway o en el router de Login de FastAPI, y bloqueo temporal de la cuenta tras N intentos fallidos.