Ejercicio Práctico NFR

**SEGURIDAD**

* **Confidencialidad de Datos Bancarios**
  + **Descripción**: Garantizar la encriptación de los datos bancarios en tránsito y en reposo para proteger la confidencialidad del usuario final. Implementar estándares PCI DSS en todas las operaciones de pago.
  + **Stakeholders**: Equipo de Seguridad de TI, Administradores de Backoffice, Usuarios Finales, Entidades de Pago.
  + **Métrica**: Medición del cumplimiento de PCI DSS; pruebas de penetración y auditorías de seguridad bianuales para asegurar la confidencialidad.
* **Autenticación y Control de Acceso**
  + **Descripción**: Implementar un sistema de autenticación robusto (autenticación multifactor) y gestión de accesos basada en roles para garantizar que solo el personal autorizado acceda a datos sensibles y funciones críticas.
  + **Stakeholders**: Administradores del Sistema, Equipo de Desarrollo, Usuarios Internos.
  + **Métrica**: Auditoría semestral de accesos y revisión de privilegios de usuarios, reportando los intentos de acceso fallidos y accesos no autorizados.

**RENDIMIENTO**

* **Latencia en Procesamiento de Transacciones**
  + **Descripción**: Las transacciones de pago deben completarse en menos de 2 segundos para evitar demoras en el tránsito de vehículos.
  + **Stakeholders**: Operadores del Peaje, Usuarios Finales.
  + **Métrica**: Tiempo promedio de respuesta por transacción monitoreado en tiempo real (segundos), además debe ser < 2 segundos en un 95% de las transacciones.
* **Escalabilidad para soportar tráfico variable**
  + **Descripción**: Diseñar el sistema para gestionar picos de tráfico de hasta el 150% de la carga promedio, es decir el sistema debe soportar picos de tráfico de hasta 1 millón de transacciones por día, especialmente en horarios de alto flujo sin pérdida de rendimiento.
  + **Stakeholders**: Administradores de Infraestructura, Operadores del Sistema, Usuarios Finales.
  + **Métrica**: Midiendo el rendimiento monitoreado mediante métricas de uso de CPU y memoria o mediante el porcentaje de transacciones exitosas bajo carga máxima simulada.

#### **DISPONIBILIDAD**

* **Disponibilidad del sistema del 99.9%**
  + **Descripción**: Minimizar el tiempo de inactividad mediante redundancia y alta disponibilidad.
  + **Stakeholders**: Administradores de TI o Usuarios Finales.
  + **Métrica**: Tiempo de inactividad registrado, porcentaje de disponibilidad mensual.
* **Recuperación ante desastres en menos de 5 minutos**
  + **Descripción**: Implementar un sistema de recuperación rápida (menos de 5 minutos) para minimizar el impacto de fallos.
  + **Stakeholders**: Administradores de TI, Operadores del Sistema.
  + **Métrica**: Tiempo de recuperación monitoreado en casos de pruebas de recuperación simuladas; cada falla crítica debe ser resuelta dentro del SLA acordado.

**INTEGRACIÓN**

* **Interoperabilidad con Sistemas Bancarios Externos**
  + **Descripción**: El sistema debe integrar API bancarias para procesar pagos en tiempo real y permitir validación instantánea de transacciones.
  + **Stakeholders**: Bancos asociados, Proveedores de servicios de pago, Administradores del Sistema.
  + **Métrica**: Latencia de integración < 1 segundo por transacción; tasa de éxito del 99.5% en las transacciones de pago.
* **Sincronización de Datos en Tiempo Real**
  + **Descripción**: Sincronizar los datos entre el backend y los dispositivos de peaje cada 30 segundos para mantener información precisa de estado y transacciones.
  + **Stakeholders**: Operadores del Peaje, Administradores de Infraestructura.
  + **Métrica**: Tasa de sincronización de datos monitoreada cada minuto; objetivo de sincronización fallida < 1% en cada intervalo de 30 segundos.

**ACCESIBILIDAD**

* **Compatibilidad Multidispositivo y Multiplataforma**
  + **Descripción**: El sistema debe ser accesible desde dispositivos móviles, tablets y desktops con funcionalidades completas.
  + **Stakeholders**: Usuarios Finales, Administradores del Sistema, Personal de Soporte.
  + **Métrica**: Pruebas de accesibilidad realizadas en distintos dispositivos y plataformas, con una tasa de éxito de acceso del 98%.
* **Funcionalidad Multilenguaje**
  + **Descripción**: El sistema debe ser accesible en al menos tres idiomas (inglés, español y uno específico del país de operación).
  + **Stakeholders**: Usuarios Finales, Operadores de Peaje.
  + **Métrica**: Inspección de calidad y pruebas de localización; al menos el 95% de las interfaces traducidas adecuadamente en cada idioma.

#### **GESTIÓN DE DATOS**

* **Integridad de datos en todas las transacciones**
  + **Descripción**: Garantizar que los datos no se pierdan ni alteren durante las transacciones.
  + **Stakeholders**: Usuarios, administradores del sistema.
  + **Métrica**: Porcentaje de transacciones sin pérdida de datos, revisiones de integridad mensuales.
* **Almacenamiento Seguro y Control de Datos Históricos**
  + **Descripción**: Garantizar el almacenamiento seguro de datos históricos de transacciones y su acceso controlado, respetando políticas de privacidad y conformidad con RGPD.
  + **Stakeholders**: Administradores de TI, Usuarios Internos, Autoridades de Regulación.
  + **Métrica**: Auditoría de conformidad de datos con RGPD; revisión semestral de permisos de acceso y seguridad en datos almacenados.