Informe de Test Exploratorio – Sprint 1

# Objetivo general

El propósito de este test exploratorio es evaluar el comportamiento inicial del sistema luego de implementadas las funcionalidades básicas relacionadas al registro, autenticación, acceso a endpoints protegidos y creación de cuentas y tarjetas. Se busca identificar errores tempranos en la lógica que no están contemplados en los test automatizados.

# Organización del test exploratorio

| Elemento | Detalle |
| --- | --- |
| Sesiones de prueba | Cada sesión se enfocará en un área específica de la funcionalidad agregada en este sprint. Se documentarán los hallazgos y tendrán duración de 30 min. |
| Sesión 1 | Prueba de registro de usuario. |
| Sesión 2 | Prueba de login y persistencia del token. |
| Sesión 3 | Prueba de logout y validación de tokens en lista negra. |

# Tours ejecutados

| Tour | Descripción |
| --- | --- |
| Tour del Novato | - Registrar un nuevo usuario con datos válidos.  - Intentar registrarse con datos incorrectos o faltantes.  - Verificar si el sistema proporciona mensajes de error claros. |
| Tour de Autenticación | - Iniciar sesión con credenciales correctas y validar el token recibido.  - Intentar iniciar sesión con credenciales incorrectas.  - Intentar acceder a recursos protegidos sin autenticación. |
| Tour de Seguridad | - Cerrar sesión y verificar que el token queda invalidado.  - Intentar usar un token de la lista negra para acceder a recursos protegidos.  - Revisar si un usuario deslogueado puede seguir realizando operaciones restringidas. |

# 

# Escenarios explorados

| Escenario | Resultado |
| --- | --- |
| Registro de usuario con datos válidos | ✔ Usuario registrado correctamente sin exponer la contraseña |
| Login con credenciales correctas | ✔ Se devuelve token válido y acceso a recursos autorizados |
| Logout e invalidez de token | ✔ Token invalidado exitosamente, no permite nuevos accesos |
| Acceso sin token o con token inválido | ✔ Se devuelve 403 Forbidden de forma controlada |
| Registro duplicado o con errores | ⚠️ Se valida error 400/409 con mensajes adecuados |
| Uso de tokens en lista negra | ✔ Acceso denegado (403) como se espera |

# Workflows revisados

1. Flujo de registro y autenticación inicial- Acceder al formulario de registro  
- Enviar datos completos y válidos  
- Confirmar creación de usuario sin contraseña visible  
- Iniciar sesión con las credenciales recién creadas  
- Recibir y guardar token JWT válido

2. Acceso a recursos protegidos- Acceder a un endpoint sin token → recibir 403  
- Acceder a un endpoint con token válido → acceso exitoso  
- Intentar usar token manipulado → denegación de acceso

3. Logout y control del token invalidado- Realizar logout correctamente  
- Confirmar que el token fue agregado a la lista negra  
- Intentar reutilizar el token → se rechaza

4. Creación y validación de cuenta- Ingresar al endpoint de creación de cuenta con token válido  
- Confirmar persistencia en base de datos  
- Verificar que no se pueda duplicar la cuenta del mismo usuario

# 

# Notas y hallazgos

* ✔ Registro, login y logout funcionan según lo esperado.
* ✔ Tokens inválidos o ausentes son correctamente rechazados.
* ✔ Se utiliza lista negra de tokens para logout.
* ✔ Validación de campos en login y registro manejados correctamente.
* ❌ No se detectaron vulnerabilidades por rutas públicas.

# Conclusión

Las funcionalidades entregadas en el Sprint 1 muestran un comportamiento estable y alineado a los requerimientos iniciales del sistema: registro de usuarios, autenticación con JWT, protección de endpoints y control de sesión mediante blacklist.  
Se recomienda:  
- Continuar reforzando la seguridad con pruebas de penetración más exhaustivas en sprints posteriores.