Documento de Pruebas de Calidad para el Proyecto de E-Commerce de FENDERMED

1. Introducción

El presente documento detalla las pruebas de calidad requeridas para asegurar el funcionamiento adecuado de la plataforma de E-Commerce de FENDERMED. Estas pruebas están orientadas a verificar la estabilidad, seguridad, usabilidad y rendimiento de la plataforma, garantizando así que cumpla con los requisitos y expectativas del cliente.

2. Tipos de Pruebas de Calidad

2.1 Pruebas Funcionales

- **Pruebas Unitarias**: Verificar que cada componente individual de la plataforma funcione según lo previsto. Se realizarán pruebas para validar módulos como la gestión de usuarios, carrito de compras y notificaciones.
- **Pruebas de Integración**: Evaluar la interacción entre los distintos módulos de la plataforma, asegurando que el sistema como un todo funcione de manera coordinada y sin errores. Se probará la integración entre la gestión de usuarios, el módulo de pagos y la base de datos.
- **Pruebas de Sistema**: Validar que la plataforma en su totalidad cumple con los requisitos establecidos en el TDR. Esto incluye pruebas sobre todos los módulos desarrollados, como la gestión de productos, pagos y reportes.
- **Pruebas de Regresión**: Asegurar que los cambios o actualizaciones no afecten el funcionamiento previo de la plataforma. Se ejecutarán pruebas automatizadas para confirmar que las funcionalidades ya desarrolladas no presenten fallas después de cada modificación.

2.2 Pruebas de Usabilidad

- **Pruebas de Interfaz de Usuario (UI)**: Evaluar la facilidad de uso y la intuitividad de la plataforma desde la perspectiva del usuario final. Se trabajará con un grupo de usuarios para recoger su experiencia y retroalimentación sobre la interfaz.
- **Pruebas de Accesibilidad**: Comprobar que la plataforma pueda ser utilizada por personas con discapacidades, cumpliendo con las pautas WCAG (Web Content Accessibility Guidelines).

2.3 Pruebas de Rendimiento

- **Pruebas de Carga**: Evaluar cómo se comporta la plataforma bajo una carga considerable de usuarios concurrentes. Se utilizarán herramientas como **Apache JMeter** para simular diferentes escenarios de carga y verificar la estabilidad de la plataforma.
- **Pruebas de Estrés**: Probar los límites de la plataforma sometiéndola a un tráfico extremo para identificar los puntos de fallo y la capacidad máxima del sistema.
- **Pruebas de Escalabilidad**: Asegurar que la plataforma pueda escalar adecuadamente si la cantidad de usuarios aumenta. Estas pruebas verificarán que

los recursos de hosting puedan ajustarse automáticamente para soportar la demanda.

2.4 Pruebas de Seguridad

- **Pruebas de Vulnerabilidad**: Utilizar herramientas como **Nessus** para identificar posibles vulnerabilidades que puedan ser explotadas por atacantes, tales como inyecciones SQL, vulnerabilidades XSS, y problemas de configuración.
- **Pruebas de Autenticación y Autorización**: Asegurar que solo los usuarios autorizados puedan acceder a la plataforma y que los roles y permisos estén correctamente configurados.
- **Pruebas de Ataque DDoS**: Evaluar la capacidad del servidor para manejar ataques de denegación de servicio distribuido, probando que las medidas de seguridad implementadas, como el firewall, funcionen adecuadamente.

2.5 Pruebas del Servidor, Hosting y Dominio

- **Pruebas de Configuración del Servidor**: Verificar que el servidor esté correctamente configurado para asegurar la disponibilidad y estabilidad de la plataforma. Se realizarán pruebas para validar la correcta instalación de software, configuración del sistema operativo y seguridad del servidor.
- **Pruebas de Rendimiento del Hosting**: Evaluar el rendimiento del hosting bajo diferentes condiciones de carga para garantizar que los recursos contratados sean suficientes para el tráfico esperado. Se utilizarán herramientas como **Apache JMeter** para simular escenarios de carga y evaluar la capacidad de respuesta.
- **Pruebas de DNS y Dominio**: Comprobar que el dominio esté correctamente configurado, que los registros DNS apunten al servidor adecuado y que el sitio sea accesible desde diferentes ubicaciones. Se realizarán pruebas utilizando herramientas como **Dig** o **nslookup** para verificar los registros DNS.
- **Pruebas de Certificado SSL**: Verificar la correcta instalación y configuración del certificado SSL para garantizar que todas las comunicaciones entre el usuario y el servidor estén encriptadas y seguras. Se utilizarán herramientas como **SSL Labs** para evaluar la calidad del cifrado y la seguridad del certificado.
- **Pruebas de Vulnerabilidad**: Utilizar herramientas como **Nessus** para identificar posibles vulnerabilidades que puedan ser explotadas por atacantes, tales como inyecciones SQL, vulnerabilidades XSS, y problemas de configuración.
- **Pruebas de Autenticación y Autorización**: Asegurar que solo los usuarios autorizados puedan acceder a la plataforma y que los roles y permisos estén correctamente configurados.
- **Pruebas de Ataque DDoS**: Evaluar la capacidad del servidor para manejar ataques de denegación de servicio distribuido, probando que las medidas de seguridad implementadas, como el firewall, funcionen adecuadamente.

3. Herramientas de Pruebas

- **Selenium**: Para la automatización de pruebas funcionales y de regresión, permitiendo validar la interfaz de usuario y el comportamiento esperado del sistema.
- **Apache JMeter**: Para las pruebas de carga y rendimiento, simulando múltiples usuarios accediendo a la plataforma de manera simultánea.

- **Nessus**: Para la identificación de vulnerabilidades y pruebas de seguridad.
- **Postman**: Para probar y verificar las APIs desarrolladas, asegurando que las integraciones y la comunicación entre módulos sean efectivas.

4. Cronograma de Pruebas

Las pruebas se llevarán a cabo de acuerdo con el siguiente cronograma, en coherencia con el diagrama de Gantt del proyecto:

- **Semana 13 - 14**: Pruebas de Integración y Sistema, Pruebas de Seguridad. Esta fase coincide con las pruebas en laboratorio.
- **Semana 15**: Pruebas de Usabilidad y Pruebas de Rendimiento. Estas pruebas se realizarán durante la fase de prueba final en producción y entrega del tutorial.
- **Semana 16**: Pruebas de Regresión y Evaluación Final del Proyecto. Esta etapa se llevará a cabo durante el cierre del proyecto y la evaluación final.
- **Semana 13 - 14**: Pruebas de Integración y Sistema, Pruebas de Seguridad.
- **Semana 15**: Pruebas de Usabilidad y Pruebas de Rendimiento.
- **Semana 16**: Pruebas de Regresión y Evaluación Final del Proyecto.

5. Criterios de Aceptación

Para que la plataforma sea aceptada, debe cumplir con los siguientes criterios:

- **Funcionamiento sin errores críticos**: Todos los módulos deben funcionar sin errores que afecten la operatividad principal.
- **Rendimiento aceptable**: La plataforma debe ser capaz de manejar al menos 500 usuarios concurrentes sin problemas de rendimiento.
- **Seguridad garantizada**: Todas las vulnerabilidades críticas deben ser resueltas antes del despliegue en producción.
- **Usabilidad validada**: La interfaz debe ser intuitiva y fácil de usar para todos los usuarios, con una retroalimentación positiva durante las pruebas de usabilidad.

6. Conclusión

El proceso de pruebas es fundamental para asegurar la calidad de la plataforma de E-Commerce de FENDERMED. Con las pruebas detalladas en este documento, se busca garantizar la estabilidad, seguridad y rendimiento de la plataforma, asegurando así una experiencia satisfactoria tanto para los administradores como para los usuarios finales.