Especificación de requisito de seguridad de software

Proyecto:
Revisión

Ficha del documento

Fecha	Revisión	Autor	Verificado dep. calidad.

Documento validado por las partes en fecha:

Por el cliente	Por la empresa suministradora
Fdo. D./ Dña	Fdo. D./Dña

Contenido

1 Introducción

El presente documento describe la Especificación de Requisitos de Software (SRS) para el Sistema de prestación de libros, una aplicación web multiplataforma diseñada para gestionar y administrar el proceso de prestación de libros para los usuarios de la en la Universidad de las Fuerzas Armadas ESPE. El sistema tiene como objetivo facilitar el control del inventario en la prestación de libros, permitiendo a los usuarios registrarse y realizar el debido proceso de reserva o pedir prestado un libro de la biblioteca.

Para lograr un adecuado manejo de la información y enfrentar el desafío de la seguridad se va a desarrollar implementando las mejores prácticas del desarrollo del software seguro a nivel de requisitos como : el modelado de amenazas , caso de abuso, caso de usos, modelado de ataques , ingeniería de requisitos y para el diseño el patrón DDD a nivel de Backend , patrones de diseño, análisis de riesgo y patrones de diseño UI , la implementación de estas buenas prácticas ayudan a tener un sistema con un nivel alto de seguridad garantizando así la confianza por parte del usuario.

La implementación de esta combinación de buenas prácticas del desarrollo del software seguro es esencial para asegurar una gestión eficaz de la CID, Con esta solución, el sistema de prestación de libros de la biblioteca estará preparado para enfrentar los retos de un crecimiento de usuarios y garantizar una experiencia confiable y segura tanto para los usuarios como para los administradores involucrados en el sistema de la biblioteca de la ESPE.

1.1 Propósito

El propósito de este documento es proporcionar una descripción detallada de los requisitos funcionales y no funcionales del Sistema de gestión de libros de la Biblioteca de la Universidad de las Fuerzas Armadas ESPE. La Especificación de Requisitos de seguridad de Software (SRS) tiene como objetivo establecer una base clara y comprensible para el diseño, desarrollo, implementación y prueba del sistema. Además, busca servir como punto de referencia para el equipo de desarrollo, los administradores de la universidad y otras partes interesadas involucradas en el proyecto, asegurando que todos tengan una comprensión común de lo que se espera del sistema.
Las principales audiencias a las que va dirigido, incluye a todos aquellos que están involucrados en el desarrollo, implementación del sistema de gestión de libros en la Universidad de las Fuerzas Armadas ESPE, mencionando el equipo de desarrollo, administradores y personal de la Universidad, Docentes, estudiantes y Gestión de la Universidad.

1.2 Alcance

n la biblioteca central "Alejandro Segovia" de la Universidad de las Fuerzas Armadas ESPE, se requiere realizar la captura de un listado de varios libros nuevos junto al nombre de su autor que se van a agregar a su colección. Al mismo tiempo se requiere registrar los préstamos de los libros a los estudiantes.

La aplicación necesita operar en la nube, con un objetivo de nivel de servicio alto, pues varias aplicaciones clientes en distintas plataformas, tanto de dispositivos móviles como de escritorio, desean conectarse y consultar ese listado en Internet.

Además, se desea publicarlo en tiempo real en la página web de la ESPE. Esta consideración hace que la biblioteca se decante por una arquitectura de microservicios..

1.3 Personal involucrado

1.4

Nombre	Andrés Valarezo
Rol	Backend
Categoría profesional	Ingeniero
Responsabilidades	Desarrollador Backend
Información de contacto	
Aprobación	

Nombre	Henry Tiamba
Rol	Analista de seguridad
Categoría profesional	Ingeniero
Responsabilidades	desarrollo frontend
Información de contacto	
Aprobación	

Nombre	Jeremy Cadena
Rol	Frontend
Categoría profesional	Ingeniero
Responsabilidades	Desarrollo de frontend
Información de contacto	
Aprobación	

1.5 Definiciones, acrónimos y abreviaturas

Términos:

1. **Sistema de gestión de libros de la Biblioteca ESPE:** Aplicación web multiplataforma diseñada para gestionar y administrar el proceso de registro

y prestación de libros para usuarios en la Universidad de las Fuerzas Armadas ESPE.

2. **DDD:** un enfoque para el desarrollo de software que pone énfasis en entender el dominio de negocio y basar el diseño del software en ese entendimiento.

3. **Caso de abusos:** Se refiere a situaciones en las que un sistema informático es utilizado de manera indebida o para propósitos maliciosos, como ataques informáticos.

4. **Modelado de amenazas**: Es un proceso en el cual se identifican y analizan las posibles amenazas a la seguridad de un sistema informático, con el objetivo de diseñar controles de seguridad efectivos.

5. **Caso de usos:** También conocido como "Use Case" en inglés, se refiere a una descripción detallada de cómo interactúan los usuarios con un sistema de software para lograr ciertos objetivos.

6. **Modelado de ataques**: Es similar al modelado de amenazas, pero se enfoca específicamente en identificar y analizar los posibles ataques que podrían ser llevados a cabo por actores maliciosos contra un sistema informático.

7. **Encriptación**: Es el proceso de convertir información legible en un formato ilegible mediante el uso de algoritmos matemáticos, con el fin de proteger la confidencialidad de los datos.

8. **Mínimo privilegio:** Es un principio de seguridad que establece que los usuarios y procesos deben tener únicamente los privilegios necesarios para llevar a cabo sus funciones, y no más, con el fin de reducir la superficie de ataque de un sistema.

9. **Autenticación:** Es el proceso de verificar la identidad de un usuario o entidad, generalmente a través de credenciales como contraseñas, huellas dactilares, o certificados digitales.

Abreviaturas y Acrónimos:

1. **SRS**: Especificación de Requisitos de Software.

2. **ESPE**: Universidad de las Fuerzas Armadas "ESPE". (Universidad de las Fuerzas Armadas, Ecuador)

3. **DDD:** Domain-Driven Design

1.6 Referencias

1.7 Resumen

El presente documento detalla la Especificación de Requisitos de Software (SRS) para el Sistema de Prestación de Libros de la Biblioteca Central "Alejandro Segovia" de la Universidad de las Fuerzas Armadas ESPE. Este sistema tiene como objetivo principal gestionar y administrar el proceso de prestación de libros para los usuarios de la universidad.

El sistema permitirá a los usuarios registrarse y realizar el proceso de reserva o préstamo de libros de la biblioteca. Para garantizar un adecuado manejo de la información y enfrentar los desafíos de seguridad, se implementarán las mejores prácticas de desarrollo de software seguro, incluyendo el modelado de amenazas, casos de uso y abuso, análisis de riesgos, y patrones de diseño a nivel de Backend y UI.

El propósito de este documento es proporcionar una descripción detallada de los requisitos funcionales y no funcionales del sistema, sirviendo como referencia para el diseño, desarrollo, implementación y prueba del mismo. Está dirigido a todos los involucrados en el proyecto, incluyendo el equipo de desarrollo, administradores de la universidad, docentes, estudiantes y personal de gestión.

El alcance del sistema incluye la captura de listado de libros nuevos junto con sus autores, así como el registro de préstamos de libros a estudiantes. Además, el sistema operará en la nube con un alto nivel de servicio, permitiendo a múltiples aplicaciones clientes en diferentes plataformas acceder y consultar el listado de libros en tiempo real. Se busca también publicar esta información en la página web de la ESPE, lo que motiva la elección de una arquitectura de microservicios para la implementación del sistema.

En resumen, el Sistema de Prestación de Libros de la Biblioteca de la ESPE estará preparado para enfrentar los retos de un crecimiento de usuarios y garantizar una experiencia confiable y segura tanto para los usuarios como para los administradores involucrados en el sistema de la biblioteca

2 Descripción general

2.1 Perspectiva del producto

La perspectiva del producto del Sistema de Prestación de Libros de la Biblioteca Central "Alejandro Segovia" de la Universidad de las Fuerzas Armadas ESPE se centra en proporcionar una solución integral para la gestión y administración eficiente del proceso de préstamo de libros. El sistema estará diseñado para garantizar la seguridad de la información y ofrecer una experiencia confiable tanto para los usuarios como para los administradores involucrados.

2.2 Funcionalidad del producto

En cuanto a la seguridad, el Sistema de Prestación de Libros de la Biblioteca Central "Alejandro Segovia" debe implementar varias medidas para garantizar la protección de la información y la privacidad de los usuarios, así como para

prevenir posibles ataques o vulnerabilidades. Algunas consideraciones importantes en este aspecto son:

Autenticación y Autorización: El sistema debe implementar un mecanismo robusto de autenticación para verificar la identidad de los usuarios al registrarse y al acceder a sus cuentas. Además, se deben establecer controles de autorización para garantizar que cada usuario tenga acceso solo a las funciones y datos pertinentes a su rol.

Encriptación de Datos: Se debe utilizar encriptación para proteger la información confidencial almacenada en la base de datos del sistema, como los datos personales de los usuarios y los detalles de los préstamos de libros. Esto ayuda a prevenir el acceso no autorizado a la información en caso de una brecha de seguridad.

Prevención de Ataques: El sistema debe estar protegido contra diversos tipos de ataques, como ataques de inyección SQL, cross-site scripting (XSS), y ataques de denegación de servicio (DDoS). Se deben implementar filtros y validaciones de entrada para evitar la ejecución de comandos maliciosos y se deben establecer medidas de control de tráfico para mitigar los efectos de los ataques DDoS.

Implementar estas medidas de seguridad contribuirá a proteger la integridad, confidencialidad y disponibilidad de los datos del Sistema de Prestación de Libros de la Biblioteca Central "Alejandro Segovia", asegurando así una experiencia segura para los usuarios y administradores del sistema.

2.3 Características de los usuarios

Tipo de usuario	Usuarios Docentes, estudiantes para realizar la gestión de libros de la biblioteca de la Universidad de las Fuerzas Armadas ESPE.
Formación	Población universitaria
Habilidades	Gestionar libros
Actividades	Manejo de tecnologías

2.4 Restricciones

- Exclusividad para la ESPE:

El sistema solo estará disponible para la Universidad de las Fuerzas Armadas "ESPE", específicamente para el departamento de Recursos Humanos.
No se permitirá el acceso a usuarios externos a la ESPE.

- Acceso Restringido:

Se implementará un sistema de autenticación y autorización para controlar el acceso a las diferentes funcionalidades del sistema.
Los usuarios solo podrán acceder a las funciones y datos relevantes a su rol dentro del proceso de selección de personal.

Se establecerán diferentes niveles de permisos para los usuarios, como administradores, personal de selección y postulantes.

- Cumplimiento Normativo:

El sistema se desarrollará en estricto cumplimiento de las normativas y regulaciones legales relacionadas con la contratación docente y la protección de datos personales en Ecuador.
Se implementarán medidas para garantizar la confidencialidad, integridad y disponibilidad de la información.
Se aplicarán las mejores prácticas para la protección de datos personales, como la Ley Orgánica de Protección de Datos Personales y el Código Civil ecuatoriano.

- Usabilidad:

Se diseñará una interfaz intuitiva y fácil de usar para los postulantes, con un lenguaje claro y conciso.
Se implementarán ayudas contextuales y tutoriales para facilitar la navegación y el uso del sistema.
Se realizarán pruebas de usabilidad con usuarios reales para asegurar la eficacia y eficiencia del sistema.

2.5 Suposiciones y dependencias

Suposición: El sistema será compatible con los navegadores web más comunes (Chrome, Firefox, Safari, Edge) y accesible desde diferentes dispositivos (computadoras de escritorio, laptops, tabletas y teléfonos móviles).

Dependencia: La experiencia del usuario puede variar según el navegador y dispositivo utilizado. Es posible que algunas funcionalidades no estén disponibles en todos los navegadores o dispositivos.

Impacto: Si los requerimientos de compatibilidad cambian o surgen nuevas tecnologías, podría ser necesario adaptar el sistema para garantizar una experiencia óptima para los usuarios.

2.6 Evolución previsible del sistema

- Ampliación del catálogo de libros: Se ampliará el catálogo de libros disponibles en el sistema, incluyendo libros electrónicos, audiolibros y otros formatos digitales.

- Implementación de un sistema de recomendaciones: Se implementará un sistema de recomendaciones que sugiera a los usuarios libros de su interés en base a sus préstamos y búsquedas anteriores.

- Integración con redes sociales: Se integrará el sistema con redes sociales para que los usuarios puedan compartir sus experiencias de lectura y recomendaciones de libros.

- Desarrollo de un módulo de estadísticas: Se desarrollará un módulo que permita obtener estadísticas sobre el uso del sistema, los préstamos realizados y las preferencias de los usuarios.

3 Requisitos específicos

3.1 Requisitos comunes de los interfaces

3.1.1 Interfaces de usuario

Interfaz de administrador para gestionar libros : Esta interfaz permite a los administradores de la biblioteca gestionar el inventario de libros y realizar tareas relacionadas con su administración

Interfaz de Inicio de Sesión para usuarios: Esta interfaz permite a los usuarios acceder al sistema ingresando sus credenciales de inicio de sesión.

Interfaz de gestión de libros: Esta interfaz está diseñada para que los usuarios administren su propia colección de libros dentro del sistema.

Interfaz de usuarios: Esta interfaz brinda a los usuarios una vista general de su perfil y les permite acceder a las funcionalidades disponibles para ellos en el sistema.

Interfaz de Solicitud de Libro: Esta interfaz permite a los usuarios solicitar la reserva o préstamo de un libro específico de la biblioteca.

3.1.2 Interfaces de hardware

Computadoras de escritorio y portátiles: Los usuarios interactuarán con el sistema utilizando computadoras de escritorio o portátiles.

Dispositivos móviles: Es probable que se desarrolle una versión responsive o aplicación móvil para permitir el acceso al sistema desde dispositivos móviles como smartphones o tabletas.

3.1.3 Interfaces de software

Interfaz de Usuario (UI): Es la interfaz gráfica que permite a los usuarios interactuar con el sistema, presentando la información y recibiendo las acciones del usuario.

Base de Datos: Existe una interfaz de comunicación entre el sistema y las bases de datos para almacenar y recuperar datos relevantes del proceso de gestión de libros de la biblioteca

3.1.4 Interfaces de comunicación

Protocolo HTTP/HTTPS: Se utilizará para permitir la comunicación entre el sistema y los navegadores web de los usuarios, permitiendo el acceso a la plataforma a través de internet.

Protocolo SMTP: Será empleado para enviar notificaciones al correo sobre sus contraseñas para el inicio de sesión .

3.2 Requisitos funcionales

3.2.1 Requisito funcional 1

Id. Requerimiento	**REQ001**
Nombre	Autenticación y autorización
Actor	Estudiante y Administrador
Descripción	Los usuarios deben ser autenticados y autorizados antes de acceder a la aplicación.
Entradas	Credenciales de usuario (nombre de usuario y contraseña)
Salidas	Interfaz del sistema: Pantalla de inicio de sesión
Proceso	1. Acceder a la interfaz de inicio de sesión
	2. Ingresar nombre de usuario y contraseña
	3. Validar las credenciales ingresadas
	4. Autorizar el acceso según los privilegios asociados al usuario
Precondiciones	La aplicación debe estar disponible en línea
Post condiciones	El usuario autenticado tendrá acceso a las funcionalidades correspondientes a sus privilegios
Efectos Colaterales	Si las credenciales son incorrectas, el acceso será denegado y se mostrará un mensaje de error.
Prioridad	Alta

3.2.2 Requisito funcional 2

Id. Requerimiento	**REQ002**
Nombre	Encriptación de datos
Actor	Estudiante, Administrador y Aplicación

Descripción	La información transmitida entre la aplicación y los clientes debe ser encriptada.
Entradas	Datos transmitidos entre la aplicación y los clientes
Salidas	Datos encriptados
Proceso	1. Configurar la aplicación para utilizar protocolos de comunicación seguros (por ejemplo, HTTPS)
	2. Configurar la aplicación para utilizar algoritmos de encriptación fuertes
	3. Encriptar los datos antes de transmitirlos a los clientes
Precondiciones	La aplicación y los clientes deben estar configurados para admitir encriptación de datos
Post condiciones	Los datos transmitidos entre la aplicación y los clientes estarán protegidos de accesos no autorizados
Efectos Colaterales	La encriptación puede causar un aumento en el uso de recursos del sistema y un ligero aumento en el tiempo de procesamiento.
Prioridad	Alta

3.2.3 Requisito funcional 3

Id. Requerimiento	**REQ003**
Nombre	Control de acceso basado en roles
Actor	Administrador, Estudiante y Aplicación
Descripción	Se debe implementar un control de acceso basado en roles para proteger la información de la aplicación.
Entradas	Roles de usuario, identificación de usuario
Salidas	Acceso autorizado o denegado a funcionalidades de la biblioteca
Proceso	1. Definir roles de usuario y sus privilegios asociados
	2. Asignar roles a los usuarios según sus responsabilidades y funciones
	3. Configurar la aplicación para verificar los roles de usuario durante el acceso a funcionalidades y datos
Precondiciones	La aplicación debe tener una estructura de roles definida y usuarios registrados con roles asignados
Post condiciones	Los usuarios solo tendrán acceso a las funcionalidades y datos autorizados según sus roles
Efectos Colaterales	Los cambios en los roles de usuario pueden requerir actualizaciones en la configuración de acceso de la aplicación.
Prioridad	Alta

3.2.4 Requisito funcional 4

ID de Requerimiento	REQ004
Nombre	Bloque de Usuario por Intentos Fallidos al Ingreso al Sistema
Actor	Sistema
Descripción	Después de cierto número de intentos fallidos al ingresar al sistema, bloquear el acceso del usuario por un período determinado.
Entradas	Nombre de usuario, contraseña
Salidas	Mensaje de error, bloqueo de cuenta
Proceso	1. El usuario intenta acceder al sistema ingresando su nombre de usuario y contraseña.
Precondiciones	El usuario debe ingresar mediante la URL a la interfaz de inicio de sesión
Post Condiciones	La aplicación de la acceso a las funcionalidades de la biblioteca

3.3 Requisitos no funcionales

3.3.1 Requisitos de rendimiento

- El sistema debe ser capaz de manejar múltiples usuarios concurrentes sin experimentar una degradación significativa del rendimiento.
- El tiempo de respuesta para las acciones del usuario, como cargar documentos o enviar formularios, debe ser rápido y eficiente.
- Se deben establecer criterios de rendimiento, como tiempo de carga de páginas, tiempos de respuesta de la base de datos y tiempo de procesamiento de solicitudes, y estos deben cumplirse para brindar una experiencia fluida a los usuarios.

3.3.2 Seguridad

- La información confidencial y personal de los estudiantes, deben estar protegidos mediante medidas de seguridad apropiadas, como cifrado y autenticación.
- El acceso al sistema debe estar protegido por un sistema de inicio de sesión seguro, con niveles de acceso y permisos adecuados para los diferentes usuarios.
- Se deben implementar mecanismos para prevenir ataques de seguridad, como inyección de SQL, ataques de denegación de servicio, entre otros.
- Se deben realizar pruebas de seguridad periódicas y auditorías para identificar posibles vulnerabilidades y corregirlas.

3.3.3 Fiabilidad

- El sistema debe ser confiable y consistente en su funcionamiento, evitando errores y fallos inesperados.

3.3.4 Disponibilidad

- El sistema debe estar disponible para los usuarios en un horario determinado y, en la medida de lo posible, funcionar sin interrupciones durante el período crítico de postulación y evaluación.
- Se deben implementar medidas de alta disponibilidad y redundancia para asegurar que el sistema siga funcionando incluso en caso de fallos en hardware o software.

3.3.5 Mantenibilidad

- El código del sistema debe ser mantenible y estar bien documentado para facilitar futuras actualizaciones y correcciones.
- Se deben seguir prácticas de desarrollo de software seguro que permitan una fácil extensión del sistema si es necesario agregar nuevas funcionalidades en el futuro.
- Se deben evitar dependencias obsoletas y mantener actualizadas las bibliotecas y herramientas utilizadas en el desarrollo.

3.3.6 Portabilidad

- El sistema debe ser compatible con diferentes plataformas y navegadores web, para que los usuarios puedan acceder a él desde una variedad de dispositivos.

3.4 Otros requisitos

4 Apéndices