**Requerimientos No Funcionales**:

Son aquellos que describen atributos o características del sistema que no están directamente relacionados con la funcionalidad de este, sino que se centran en aspectos como el rendimiento, la seguridad, la usabilidad, la disponibilidad, entre otros.

Ejemplo de algunos requerimientos no funcionales:

1. **Rendimiento:** Define los criterios de desempeño del sistema, como el tiempo de respuesta, la capacidad de procesamiento, la escalabilidad y la eficiencia en el uso de recursos.
2. **Seguridad**: Establece los mecanismos de protección de la información y los datos almacenados en el sistema, incluyendo la autenticación, la autorización, el cifrado y la integridad de los datos.
3. **Usabilidad:** Se refiere a la facilidad de uso del sistema y la experiencia del usuario, incluyendo aspectos como la intuitivita de la interfaz, la accesibilidad, la documentación y el soporte.
4. **Disponibilidad:** Define el tiempo durante el cual el sistema debe estar disponible para su uso, así como los mecanismos de redundancia y recuperación en caso de fallos o interrupciones.
5. **Mantenibilidad**: Se refiere a la capacidad del sistema de ser modificado, actualizado y reparado de manera eficiente, incluyendo el modularidad, la documentación del código y la facilidad de prueba.

# Requerimientos No Funcionales

|  |  |  |  |
| --- | --- | --- | --- |
| **Identificador:** RNF 1 | | **Nombre:**  Rendimiento | |
| **Tipo:**  Necesario | **Requerimiento que lo utiliza o especializa:** | | **¿Crítico?**  Si |
| **Prioridad de desarrollo:**  Alto | **Documentos de visualización asociados:**   * En menos de 5 segundos la página ya tiene que haber guardado. * Después de 6 segundos se, mostrara un mensaje de error por conexión   . | | |
| **Entrada:**  El número de usuarios concurrentes son de 50, volumen de datos a procesar son de 4, límites de tiempo de respuesta 3 segundos. | **Salida:**  Informes de rendimiento del sistema, gráficos y tablas que muestren el uso de recursos del sistema y la capacidad de procesamiento y almacenamiento, mensajes de error en caso de situaciones anormales | | |
| **Descripción:**   * el sistema debe ser capaz de cargar la página en un tiempo máximo de 5 segundos y mostrar la sección de datos adicionales de manera eficiente, incluso si hay múltiples usuarios accediendo a la página al mismo tiempo. * Este requerimiento no funcional se refiere a la capacidad del sistema para responder de   Manera rápida y eficiente a las solicitudes de los usuarios y manejar grandes volúmenes de datos sin afectar la velocidad y el tiempo de respuesta. | | | |
| **Manejo de situaciones anormales**   * Si el tiempo de respuesta del sistema supera el límite establecido, se debe mostrar un mensaje de error al usuario y se debe realizar un seguimiento para identificar la causa y resolver el problema. * Si el volumen de usuarios concurrentes afecta el rendimiento del sistema, se debe considerar el uso de herramientas de balanceo de carga. * Si el volumen de datos supera la capacidad de almacenamiento, se debe considerar la implementación de estrategias de almacenamiento en la nube | | | |
| **Criterios de aceptación**   * El sistema debe responder a las solicitudes de los usuarios en menos de 3 segundos. * El tiempo de carga de la página no debe superar los 5 segundos. * La capacidad de procesamiento de datos debe ser capaz de manejar un volumen de usuarios concurrentes sin afectar el rendimiento del sistema. * La capacidad de almacenamiento de datos debe ser escalable para manejar un creciente volumen de información. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identificador:** RNF 2 | | **Nombre:**  seguridad | |
| **Tipo:**  Necesario | **Requerimiento que lo utiliza o especializa:** | | **¿Crítico?**  Si |
| **Prioridad de desarrollo:**  Alto | **Documentos de visualización asociados:**   * Usuario contraseña * Formulario de registro * Formulario para validar usuario y contraseña * Mensajes de error o confirmación | | |
| **Entrada:**  Inicio de sección  Registro de usuarios  Validación de contraseña | **Salida:**  Ingreso del usuario a la plataforma  Confirmación de usuario | | |
| **Descripción:**   * Todos los datos sensibles deben estar cifrado tanto en transito como en tanto en tránsito como en reposo para evitar el acceso no autorizado * Definir longitud mínima, uso de caracteres especiales, combinación de letras y números, y caducidad periódica de contraseñas. * Establecer restricciones sobre quiénes pueden acceder a ciertas funciones o datos dentro del sistema, asegurando que solo las personas autorizadas tengan acceso. * Requerir que el sistema registre todas las actividades relevantes, como inicios de sesión, cambios en los datos y acciones realizadas por los usuarios, para poder rastrear eventos en caso de incidentes de seguridad * Especificar la frecuencia y el proceso de respaldo de datos, así como los procedimientos de recuperación en caso de fallos o ataques. * Especificar la necesidad de contar con soluciones antivirus y antimalware actualizadas para proteger el sistema contra amenazas informáticas. * Establecer la necesidad de tener sistemas y procedimientos para detectar y responder a intentos de acceso no autorizado o actividades sospechosas. * Definir cómo se manejarán las actualizaciones de software y parches de seguridad para mantener el sistema protegido contra vulnerabilidades conocidas. | | | |
| **Manejo de situaciones anormales**   * Se debe especificar la necesidad de que el sistema cuente con mecanismos de detección temprana de eventos anormales o sospechosos * Notificaciones y alertas: establecerse cómo se notificará a los administradores o responsables de seguridad en caso de detección de situaciones anormales * Respuesta automática: definir respuestas automáticas a situaciones anormales, como bloquear un usuario después de múltiples intentos fallidos de inicio de sesión o aislar una parte del sistema en caso de detectar actividad maliciosa. * el sistema registre y almacene información sobre las situaciones anormales detectadas, las acciones tomadas en respuesta y los resultados obtenidos. Esto es esencial para un análisis posterior y para mejorar las estrategias de seguridad. * Recuperación y restauración: planes de recuperación y restauración en caso de que una situación anormal cause daños o interrupciones * Actualización: requerimientos deben contemplar la necesidad de mantener actualizados los mecanismos de detección y respuesta | | | |
| **Criterios de aceptación**   * Cifrado de datos en tránsito y en reposo   + Todos los datos confidenciales se cifran utilizando algoritmos de cifrado fuertes.   + Se utiliza HTTPS para todas las comunicaciones web.   + Los datos almacenados en reposo están cifrados y protegidos de accesos no autorizados. * Políticas de contraseñas seguras   + Los usuarios son requeridos a crear contraseñas que cumplan con los criterios especificados (longitud, caracteres, etc.).   + El sistema impide el uso de contraseñas débiles y comunes.   + Se realiza un bloqueo temporal después de un número determinado de intentos fallidos de inicio de sesión. * Control de acceso y autenticación   + El sistema permite diferentes niveles de acceso según el rol y privilegios del usuario.   + La autenticación de dos factores (2FA) está habilitada para cuentas de alto nivel de privilegios.   + Los usuarios inactivos son desconectados automáticamente después de un período de tiempo establecido. * Registro de auditoría y eventos   + Todas las actividades de inicio de sesión, cambios en datos y acciones administrativas se registran en un archivo de auditoría.   + Los registros de auditoría son inalterables y solo accesibles por personal autorizado.   + Los registros de auditoría son almacenados durante al menos X meses para análisis posterior. * Respuesta a incidentes de seguridad   + Existe un plan documentado para responder a incidentes de seguridad, con roles y responsabilidades claramente definidos.   + Se realizan simulacros regulares de respuesta a incidentes para garantizar la efectividad del plan.   + Los incidentes se manejan de acuerdo con las políticas y regulaciones de seguridad vigentes. * Actualizaciones y parches de seguridad   + El sistema se actualiza regularmente con los últimos parches de seguridad y actualizaciones de software.   + Se realiza una evaluación de vulnerabilidades de forma periódica y se abordan de manera oportuna.   + Existe un proceso para mitigar vulnerabilidades críticas en un plazo definido. * Cumplimiento normativo y estándares de seguridad   + El sistema cumple con las regulaciones y estándares de seguridad específicos, como ISO 27001 o GDPR.   + Se realiza una auditoría de seguridad externa para verificar el cumplimiento con los estándares aplicables.   + Se mantienen registros de cumplimiento y se realizan ajustes según las recomendaciones de las auditorías. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identificador:** RNF 3 | | **Nombre:**  Usabilidad | |
| **Tipo:**  Necesario | **Requerimiento que lo utiliza o especializa:** | | **¿Crítico?**  Si |
| **Prioridad de desarrollo:**  Medio | **Documentos de visualización asociados:**     * Informes que muestran la facilidad de acceso y documentación al sistema ligero. | | |
| **Entrada:**  Facilidad del uso del sistema con los formularios, accesibilidad ligera. | **Salida:**  El sistema debe agilizar el proceso de completar formularios por la manera fácil y simplificada de los espacios a rellenar. | | |
| **Descripción:**   * Si un usuario accede a los formularios de inscripción, el sistema debe ser capaz de mostrar de manera fácil, concreta y creativa los formularios, indicando exactamente dónde debe rellenar información, cargar y descargar sus documentos. | | | |
| **Manejo de situaciones anormales**     * En caso de fallo de internet. | | | |
| **Criterios de aceptación**     * La capacidad de documentación debe ser fácil y entendible. * La accesibilidad del sistema debe ser lo suficientemente buena para el usuario. * La interfaz del sistema debe ser intuitiva y fácil de entender. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identificador:** RNF 4 | | **Nombre:**  **Disponibilidad** | |
| **Tipo:**  Necesario | **Requerimiento que lo utiliza o especializa:** | | **¿Crítico?**  Si |
| **Prioridad de desarrollo:**  Alto | **Documentos de visualización asociados:**  ⦁ Informe de Disponibilidad del Sistema  ⦁ Gráficos de Disponibilidad  ⦁ Tablas de Disponibilidad por Componente  ⦁ Informe de Seguimiento de Errores y Problemas de Disponibilidad  ⦁ Comparación de Disponibilidad en Diferentes Períodos | | |
| **Entrada:**  Número de usuarios concurrentes, volumen de datos a procesar, límites de tiempo de respuesta.: | **Salida:**  Informes de rendimiento del sistema, gráficos y tablas que muestren el uso de recursos del sistema y la capacidad de procesamiento y almacenamiento, mensajes de error en caso de situaciones anormales. | | |
| **Descripción:**  El sistema debe garantizar una alta disponibilidad para asegurar una experiencia óptima de usuario, incluso en condiciones de carga y situaciones anormales. Este requerimiento no funcional se enfoca en la capacidad del sistema para responder de manera eficiente a las solicitudes de los usuarios y manejar volúmenes sustanciales de datos sin comprometer la velocidad y el tiempo de respuesta. | | | |
| **Manejo de situaciones anormales**   * Si el sistema experimenta una degradación en la velocidad o la disponibilidad, se debe realizar un seguimiento para identificar las causas subyacentes y tomar acciones correctivas para restaurar el rendimiento óptimo. * Se deben implementar mecanismos de monitoreo continuo para detectar patrones de uso inusuales o picos de tráfico, lo que permite anticipar y mitigar posibles problemas de disponibilidad. * Si se detecta una anomalía, se debe notificar al equipo de operaciones para que tome medidas inmediatas y se resuelva la situación. * Se debe realizar una auditoría periódica del rendimiento y la disponibilidad del sistema para garantizar que se mantenga dentro de los límites definidos y para identificar oportunidades de mejora. | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Identificador:** RNF 5 | | **Nombre:**  Mantenibilidad: | |
| **Tipo:**  Necesario | **Requerimiento que lo utiliza o especializa:** | | **¿Crítico?**  Si |
| **Prioridad de desarrollo:**  Alto | **Documentos de visualización asociados:**  ● Documentación detallada.  ● Comentarios en el código fuente.  ● Modularidad.  ● Gestionar versiones. | | |
| **Entrada:**  El sistema debe tener una forma de medir qué tan complicado es el código para que los desarrolladores puedan saber si es fácil de mantener. | **Salida:**  El sistema debe guardar una lista de todos los cambios que se hacen en el código, para que los desarrolladores puedan ver cómo ha evolucionado con el tiempo. | | |
| **Descripción:**  ● Si un usuario accede el sistema debe ser construido de manera que cargar la página de que no tome más de 5 segundos, incluso cuando muchas personas estén usando la página al mismo tiempo.  ● Los pedazos del sistema deben estar ordenados de forma fácil de entender, para que las personas  que trabajen en el sistema después puedan ajustarlo, hacerlo mejor o arreglarlo sin problemas. | | | |
| **Manejo de situaciones anormales**  ● El sistema debe ser capaz de cargar la página en un máximo de 5 segundos, incluso si muchas personas están usando el catálogo al mismo tiempo.  ● crear instrucciones claras que expliquen cómo el sistema hace su trabajo, para que las personas que cuiden del sistema después sepan cómo manejar situaciones inusuales. | | | |
| **Criterios de aceptación**  ● El sistema será considerado exitoso si puede cargar la página en un tiempo máximo de  5 segundos, incluso si muchas personas están usando la página al mismo tiempo.  ● Si varias personas intentan acceder a la página al mismo tiempo, el sistema no debe volverse lento ni colapsar, sino que debe seguir funcionando sin problemas.  ● La documentación sobre cómo el sistema maneja situaciones inusuales debe ser clara y fácil de entender para las personas encargadas del mantenimiento futuro. | | | |