En esta etapa del proyecto se incorporan Requisitos No Funcionales (RNF) que complementan los funcionales, garantizando aspectos clave como calidad interna, evolución del sistema y robustez ante el uso real. A continuación, se detallan los RNF seleccionados junto con sus métricas de evaluación.

*Santiago Lorenzatti*

*Diseño de Sistemas de Información | Universidad Tecnológica Nacional FRSFCO*

*Gestor de tareas domésticas*

* **Adaptabilidad**

El sistema deberá ser capaz de adaptarse de forma efectiva y eficiente a distintos entornos de hardware y software, incluyendo navegadores modernos y dispositivos con diferentes resoluciones de pantalla, garantizando su correcto funcionamiento sin necesidad de modificaciones estructurales.

Métrica de evaluación:

Para verificar el cumplimiento de este requisito, se utilizarán las siguientes métricas:

* Compatibilidad multiplataforma: El sistema deberá ejecutarse sin errores en al menos 3 navegadores (Chrome, Firefox, Safari) y 2 sistemas operativos (Windows y macOS).
* Responsive design: La interfaz deberá adaptarse correctamente a resoluciones móviles (mínimo 360px de ancho) y de escritorio (mínimo 1024px de ancho), sin pérdida de funcionalidad.

Herramientas necesarias para la implementación y verificación:

Para garantizar la adaptabilidad, se emplearán las siguientes herramientas:

* React y CSS Flex/Grid: Para construir una interfaz flexible y responsive, adaptable a distintos tamaños de pantalla sin necesidad de múltiples versiones del diseño.
* Media queries en CSS: Para aplicar estilos condicionales según el tipo de dispositivo o resolución.
* DevTools del navegador: Utilizados para simular diferentes tamaños de pantalla y verificar comportamiento en múltiples dispositivos virtuales.
* Lighthouse (integrado en Chrome): Para generar reportes automáticos sobre rendimiento, accesibilidad y adaptabilidad del sitio.
* Testing cross-browser: Las pruebas se complementarán con herramientas como BrowserStack o pruebas manuales para garantizar funcionamiento en distintos navegadores y sistemas.
* **Autenticidad del sistema**

El sistema debe garantizar la autenticidad de los usuarios mediante un mecanismo de autenticación seguro.

Implementación:

Para ello, las contraseñas serán almacenadas utilizando funciones de hash seguras (como bcrypt) y nunca en texto plano. Además, una vez autenticado, el sistema emitirá un JSON Web Token (JWT) firmado, que servirá para validar la identidad del usuario en las acciones posteriores dentro del sistema. Este token incluirá información codificada y será verificado en cada solicitud protegida para asegurar que el usuario es quien dice ser.

Métricas de medición:

Para evaluar el cumplimiento del requisito de autenticidad, se definen métricas orientadas a verificar la correcta implementación de los mecanismos de seguridad. Entre ellas se incluye: la proporción de contraseñas almacenadas en formato hash (esperado: 100%), la emisión exitosa de tokens JWT tras un inicio de sesión válido, la validación obligatoria del token en los endpoints protegidos y el tiempo de expiración configurado para cada token. Estas métricas se pueden controlar mediante pruebas automatizadas, inspección del almacenamiento de usuarios y simulaciones de acceso mediante herramientas como Postman o tests de integración.

Herramientas necesarias para la implementación y verificación:

Para garantizar la autenticidad en el sistema, se requiere el uso de herramientas específicas tanto para su implementación como para su verificación. En primer lugar, se utilizará bcrypt (u otra librería de hash segura) para el almacenamiento cifrado de contraseñas. La autenticación de usuarios se gestionará mediante JWT (JSON Web Tokens), permitiendo emitir y validar tokens firmados digitalmente. Para verificar el correcto funcionamiento, se recurrirá a herramientas como Postman para simular solicitudes autenticadas, así como pruebas automatizadas con Jest u otras bibliotecas de testing. Además, será útil contar con herramientas de inspección como DevTools del navegador o extensiones JWT debugger para visualizar y validar los tokens emitidos en tiempo real.