REQUERIMIENTOS NO FUNCIONALES

Calle 43 No. 57-14 Centro Administrativo Nacional, CAN, Bogotá, D.C.
PBX: (057) (1) 222 2800 - Fax 222 4953
www.mineducacion.gov.co - atencionalciudadano@mineducacion.gov.co

REQUERIMIENTOS NO FUNCIONALES

A continuación se describen las principales características no funcionales que debe contener el sistema de información.

Interfaces de usuario.

Dado que son múltiples herramientas que conformarán el sistema de información en referencia, se debe contemplar el diseño basado en Web que debe presentar el look and feel institucional del Ministerio de Educación, acorde al portal web del mismo y a los lineamientos del Manual para la implementación de la estrategia de Gobierno en Línea, en su versión vigente.

Los formularios y demás herramientas de apoyo deben ser intuitivos al usuario, presentar ayudas en línea, su despliegue frente al usuario debe ser rápida, permitir su navegación a través de los exploradores más comunes como Mozilla, e Internet Explorer, Chrome y las diferentes plataformas (Windows, Mac, Linux), autoajustable a cualquier tamaño y resolución de pantalla del usuario, utilizar imágenes optimizadas y componentes de diseño que permitan mostrar la información de manera dinámica, ágil y estética.

El navegador no debe requerir ninguna modificación o instalación de plugins, applets, o similares para que el software funcione, ni requerir soporte técnico al usuario para poder operar la aplicación.

Se debe considerar el diseño de interfaces para dispositivos móviles (celulares, tablets, iphone, ipod, etc.).

Interfaces de comunicación.

Las interfaces de comunicación deben contener los estándares Web y fundamentalmente se deben basar en protocolos HTTP, HTTPS para la comunicación con usuarios finales y para desarrollo de Web Services SOAP, WSDL, necesarios para las interfaces entre diferentes aplicaciones.

Indudablemente para los diferentes niveles de red será necesario la utilización de otros protocolos que complementan las diferentes interfaces de comunicación entre cada uno de los componentes que deberán ser definidos en un nivel mayor de diseño arquitectónico.

Requisitos de desempeño.

Los tiempos de respuesta relacionados con formularios de manejo de información adición, modificación, eliminación, consulta de registros, autenticación y emisión de avisos y confirmaciones por parte del usuario, en forma general, no debe ser superior a 2.5

segundos, los informes y consultas que presenten una complejidad mediana no deberá exceder el tiempo de 4 segundos.

Lo anterior se debe poder obtener en un ambiente tecnológico controlado individual y único para la medición del desempeño, que permita tener recursos de procesamiento, almacenamiento y comunicaciones disponibles solo para el sistema o solución desarrollada, por lo que en su momento es necesario definir los requerimientos de infraestructura para la ejecución de las mediciones correspondientes.

Sin embargo, y para que un sistema sea funcional, se espera que el 90% de las transacciones no excedan el tiempos de respuesta entre 3 y 4 segundos, sin embargo estos tiempos serán revisados en una etapa posterior de diseño detallado, una vez se identifique y defina la infraestructura y entorno tecnológico en el cual se implementará la solución.
Finalmente es necesario que su rendimiento sea acorde con los tiempos de respuesta y la cantidad de usuarios que deberá proyectarse, por lo que el diseño de sus componentes debe ser eficiente, siendo necesaria la aplicación de las mejores prácticas para diseño y construcción del sistema de información.

Seguridad.

Se requiere de la implementación de políticas de seguridad comúnmente aceptadas y las que sean definidas por el Ministerio de Educación, además se deben considerar los siguientes aspectos:

Identificación y Autentificación: La autenticación se debe hacer a nivel del aplicativo, se debe permitir la integración con servicios de directorios basados en el estándar LDAP, especialmente para las funcionalidades que permiten autenticación, autorización, administración y almacenamiento de datos de usuarios.

Los datos relacionados con la identificación de usuario y su contraseña de acceso deben tener una vigencia de acuerdo con las políticas de seguridad definidas por el Ministerio.

Roles: El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso de acuerdo con los usuarios identificados, los cuales se pueden agrupar en:

- Rol administrador (Ministerio de Educación)
- Rol aprobador (Ministerio de Educación)
- Rol Institución (Instituciones de Formación)
- Rol OEC (Organismos de evaluadores)

- Rol OTP (Organismos de tercera parte)
- Rol ONAC (ONAC)
- Rol gestión (Ministerio de Educación)

Debe contener la definición y administración de niveles de acceso a las funcionalidades del sistema, de tal forma que se asocien roles a las funcionalidades y para cada funcionalidad se definan privilegios clasificados en:

Lectura: el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
Escritura: este tipo de acceso permite agregar datos, modificar o borrar información.
Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas, opciones o módulos.
Borrado: permite al usuario eliminar registros del sistema.
Creación: permite al usuario crear nuevos registros o campos.

Limitaciones a los servicios: Implementar las restricciones relacionadas con políticas de seguridad definidas para el sistema de información y sus componentes externos de integración, de acuerdo con los lineamientos del Ministerio de Educación.

Integridad: El modelo de seguridad debe estar presente en cada una de las capas del sistema, garantizando el acceso autorizado a la información. No deben existir “puertas traseras” que permitan el manejo de información fuera del flujo lógico del sistema. Se requiere la encriptación de los principales datos almacenados en la base de datos.

De igual forma se debe proveer un mecanismo de aseguramiento de integridad de toda la información registrada en la base de datos. Esta integridad, debe ser estructural, referencial y de restricción funcional.

Control de Acceso Externo: Se debe considerar que parte de la infraestructura presenta un esquema basado en redes seguras en donde se dispone de Firewalls mediante los cuales el manejo de puertos y protocolos son administrados desde este punto, y no desde los sistemas de información.

Se debe considerar aspectos de seguridad relacionados a su utilización a través de redes públicas, garantizando la confidencialidad e integridad de la información y acceso a ella.

Se debe incluir el diseño de pruebas de penetración que permitan identificar debilidades en el acceso al sistema en lo relacionado con el entorno, entrada, datos y lógica. No se debe permitir dos o más sesiones simultáneas con el mismo usuario.
Auditoría: Se debe implementar el registro de acciones realizadas por los usuarios a las principales transacciones (usuario, fecha, hora) y registros del sistema en lo relacionado con la creación, modificación y eliminación. De igual forma se debe disponer de la administración de estos log o base de trazabilidad posibilitando la parametrización de las transacciones o tipos de registros que generaran trazas. Se deben incluir el diseño de reportes y alertas de indicadores de seguridad.

Administración: Se debe disponer de una opción dentro del sistema que permita el manejo y definición de información relacionada con usuarios, roles, accesos, logs, puertos, conexiones, opciones, módulos, definiciones de auditoría y demás elementos que permitan realizar la administración del componente de seguridad del sistema. Se deben incluir reportes y consultas necesarias para el control y seguimiento de esta información.

Fiabilidad

A continuación se describen los principales factores que se deben considerar para garantizar la fiabilidad del sistema de información a desarrollar y por ende reducir al máximo la presencia de fallos futuros en el sistema que afecten directamente el servicio prestado por el mismo.

Madurez: se enfoca inicialmente a la utilización de componentes base o herramientas utilizadas para el diseño, construcción, pruebas e implementación reconocidas que tengan más de 3 años en el mercado, que tengan soporte por parte del fabricante, que exista un fabricante reconocido y con trayectoria y que exista el desarrollo continuo de cada herramienta que permita el mejoramiento y acceso a nuevas versiones de acuerdo con la evolución de las plataformas.

Tolerancia a fallos: el sistema deberá mantener el nivel especificado de rendimiento en casos de fallos del software.

Capacidad de recuperación: se debe considerar como parte del diseño la capacidad para restablecer el nivel de rendimiento y de recuperación de datos afectados directamente en el caso de un fallo. Se deben incluir el diseño de eventos de recuperación como parte de las pruebas diseñadas y que formaran parte de la aceptación del producto.

Adherencia a normas: debe presentar directa coherencia con la aplicación de la normatividad establecida, teniendo en cuenta la flexibilidad que debe tener el sistema para el cambio de variables importantes que puedan ser ajustas en el tiempo y que no impliquen cambios estructurales o de ajuste al código de la aplicación desarrollada. Por lo que el sistema debe tener un alto nivel de parametrización para garantizarlo.

Minimizar Fallos: para minimizar la existencia futura de fallos del sistema que impidan garantizar una correcta fiabilidad del sistema, se deben identificar claramente la planeación y ejecución de estrategias que permitan la prevención de fallos, reutilización de componentes fiables, metodologías de diseño rigurosas, lenguajes de desarrollo adecuado, detección de fallos, inspección del diseño y programas, revisiones de calidad y pruebas de calidad.

Las ventajas de definir desde el inicio del proyecto de desarrollo las estrategias de aseguramiento de calidad del software permiten obtener una reducción significativa de los valores de costo, tiempo y esfuerzo requerido para desarrollar un producto, al igual que el incremento de la calidad del software producido, el aumento de la productividad de los grupos de desarrollo y la reducción del riesgo global del proyecto.

Flexibilidad

La configuración de los parámetros de instalación no debe requerir modificaciones al código fuente de la instalación.

Debe ser totalmente independiente de la topología de red utilizada, es decir, el sistema debe poder funcionar en múltiples esquemas de comunicación, tanto para equipos conectados remotamente, como para equipos conectados por una red LAN, WAN o Internet y todas las combinaciones anteriormente descritas.

Disponibilidad

El sistema debe soportar una operación en alta disponibilidad, de acuerdo con la arquitectura planteada en el numeral 6 de este documento, no debe presentar ningún punto de fallo, es decir, debe estar provisto de mecanismos o componentes que aseguren la continuidad del servicio y que se integren a servicios de capa media espejo, procesamiento distribuido y almacenamiento en múltiples servidores. Por lo que al momento de realizar el diseño detallado se debe validar la arquitectura física en la que funcionará el sistema. Se espera una disponibilidad mínima del 99.6 %.

Mantenibilidad

Se hace referencia a la facilidad con la que el nuevo sistema o componente de software puede ser modificado para corregir fallos, mejorar su funcionamiento u otros atributos o

adaptarse a cambios en el entorno. Los factores que se debe tener en cuenta para garantizar un adecuado proceso de mantenibilidad son:

Proceso de desarrollo: La mantenibilidad debe formar parte integral del proceso de desarrollo del software. Las técnicas utilizadas deben ser lo menos intrusivas posible con el software existente. Por lo que es necesario que se identifique claramente la aplicación de metodologías de ingeniería del software y el seguimiento de estándares, que incorporen intrínsecamente modelos estructurados de diseño y código. Se debe considerar la facilidad para la realización de las pruebas técnicas y de aceptación.

Cesión de derechos: Se requiere la Cesión de Derechos de uso sobre el software implantado y todos sus componentes.

Documentación: Se debe especificar la definición y el manejo de la documentación técnica (manuales técnicos y de instalación) y funcional (manuales de administración, configuración y de usuario final) del sistema de información, establecer procedimientos claros de actualización y aprobación. En múltiples ocasiones, ni la documentación ni las especificaciones de diseño están disponibles, y por tanto, los costos del mantenimiento se incrementan debido al tiempo requerido para que un ingeniero entienda el diseño del software antes de poder ponerse a modificarlo.
El software desarrollado, por lo menos, debe tener:

- manual técnico
- manual de usuario final
- manual de administración
- manual de instalaciones e integración

Portabilidad

El sistema diseñado y sus componentes deben ser portables en plataformas GNU/Linux y Windows, con máquinas que presentan arquitecturas de 64 bits, las plataformas conexas no deberán utilizar componentes propietarios o que carezcan de sostenibilidad y evolución tecnológica. Sin embargo se deben considerar las características actuales de infraestructura del Ministerio para la implementación de la solución en lo relacionado con la capa de presentación que es basada en servicios web bajo protocolos HTTP, la capa de aplicación en PHP y JAVA con servicios publicados por Tomcat y Zend, y en la capa de datos con motores Oracle y postgres. En general debe estar acorde con la arquitectura planteada en el numeral 6.4 de este documento.