

ANEXO TÉCNICO PARA LA CONTRATACIÓN DEL PROYECTO "SISTEMA DE INFORMACIÓN DE APOYO A LOS PROCESOS DE ADMINISTRACION Y GESTIÓN DE BIENES PARA EL SENADO DE LA REPÚBLICA"

5. REQUERIMIENTOS FUNCIONALES MINIMOS

6.1. Interfaz de Usuario

Dado que son múltiples las divisiones o secciones que interactuarán en el sistema de información, se debe contemplar el diseño basado en Web que debe presentar el look and feel institucional, 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 todos los navegadores en las diferentes plataformas (Windows, Mac, Linux) en sus últimas versiones estables, 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.

Debe funcionar en Ambiente Web, sobre cualquier browser de internet (incluidos navegadores de dispositivos móviles) y 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.

Los formularios web serán construidos en estándares que ofrezcan una mayor compatibilidad con los navegadores de dispositivos móviles y permite realizar diseños adaptables a distintos dispositivos móviles (Dispositivos móviles y tabletas con sistema operativo Android, dispositivos móviles y tabletas con sistemas operativos IOS).

Con el objeto de que el sitio Web resulte de este proyecto sea accesible para el mayor número posible de usuarios, toda la solución deberá cumplir los estándares de accesibilidad W3C (World Wide Web Consortium), facilitando el acceso desde cualquier lugar, en cualquier momento y ser utilizado desde cualquier tipo de dispositivo, no importando el hardware, software, o una infraestructura de red que se utilice. A parte de las posibles restricciones técnicas, se debe dar cubrimiento la posibilidad de múltiples idiomas, las distintas localizaciones geográficas, y culturales o tradiciones, así como las posibles limitaciones físicas, psíquicas o sensoriales de los usuarios.

La solución diseñada está conformada por un único sistema que tendrá los diversos módulos requeridos para cada una de las áreas involucradas según su definición funcional, de roles y perfiles de usuarios. Se establecerá un solo diseño gráfico con los colores estilos distribuciones gráficas por medio de plantillas. Adicionalmente se deberá tener un encabezado y pie que será compartido por todos los formularios web.

El software (aplicaciones y servicios WEB) deberá estar implementado sobre el Protocolo IPv6 nativo con compatibilidad o soporte IPv4; argumentando los RFCs concretos del IETF88 y demás normas que determinan con sencillez y claridad esta compatibilidad.

6.2. Integración del sistema

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.

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.

El protocolo web será HTTPS por medio de certificado digital SSL que será definido por el Senado y adquirido por el proveedor para este sistema. Ninguna página utilizará HTTP debido a que va en contra de los requerimientos de seguridad.

Para las integraciones por medio de servicios web, la capa de servicios web que pueden ser consumidos y reutilizados por aplicaciones de plataforma cruzada para diferentes propósitos y desplegados a un bus de servicios empresarial; los sistemas con los cuales se integrará deberán poder construir clientes y exponer servicios por medio de la tecnología SOA los cuales pueden ser definidos y generados a través de definiciones WSDL.

Se requieren integraciones con:

- Servidor de correo electrónico del Senado(EXCHANGE)
- Directorio Activo (AD): para la gestión de usuarios (el Senado entregará la cadena de conexión de directorio activo y el proveedor realizará todas las gestiones y operaciones técnicas para la correcta integración, de acuerdo a las necesidades de la entidad)
- Software de recursos humanos (KACTUS) orientado a la asignación, seguimiento y control de bienes asignados a funcionarios o dependencias.

Debe cumplir con los estándares técnicos del Marco de interoperabilidad del Gobierno en línea que comprende un conjunto de principios y políticas que orientan los esfuerzos políticos, legales y organizacionales de las entidades, con el fin de facilitar el intercambio seguro y eficiente de información. Se debe contemplar múltiples dominios de interoperabilidad: Político-legal, Sociocultural, Semántico, Organizacional, Técnico.

Debe implementarse lenguaje común de intercambio de información definido por gobierno en línea(GEL).

Debe permitir integrarse e interoperar con otros sistemas de información basados en arquitectura orientada a servicios

6.3. 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, se acordarán por medio de un ANS con el proveedor para su cumplimiento.

Es necesario que su rendimiento este 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.

Se debe garantizar la confidencialidad e integridad de la información y acceso para los diferentes componentes de hardware y software del sistema

- Niveles de red
- Conexión del sistema con otros sistemas de información
- Bases de datos
- Sistemas operativos

6.4. 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.

6.4.1. 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 5 años en el mercado e implementada en el sector público, 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

6.4.2. Tolerancia a Fallos.

El sistema deberá mantener el nivel especificado de rendimiento en casos de fallos del software.

Manejo de errores: Permitir el manejo estándar de mensajes de error, mensajes de ayuda y mensajes de confirmación en la ejecución de procesos. Los mensajes de error deben presentarse al usuario en idioma español

6.4.3. Capacidad de Recuperación.

Se debe considerar 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.

Ante fallas como caídas del sistema, la base de datos debe estar protegida y su recuperación debe propender por la mínima pérdida de datos

6.4.4. 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 ajustadas 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.

Los procesos son diseñados de manera estándar y el SENADO indicará cuales características deben ser parametrizables debido a los cambios futuros que puedan sufrir estas variables

6.5. 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

6.6. Disponibilidad.

El sistema debe soportar una operación en alta disponibilidad, no debe presentar ningún punto de fallo, es decir, debe mantener una disponibilidad no menor del 99% mensual y 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.¹, proveedor se encargará de todas las operaciones técnicas necesarias para garantizar la alta disponibilidad de acuerdo a un modelo presentado.

6.7. 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. Para la implementación de la solución en lo relacionado con la capa de presentación, que está basada en servicios web bajo protocolos HTTPS, la capa de aplicación en Visual Basic, PHP o JAVA con servicios publicados por Tomcat y Zend, y en la capa de datos con motores SQL Server y MYSQL.

6.8. Seguridad

- | |
|--|
| a. Se requiere de la implementación de políticas de seguridad comúnmente aceptadas, definidas por el SENADO. |
| b. Las políticas de seguridad deben estar regidas bajo la norma ISO/IEC 27001 |
| c. El sistema deberá contar con los mecanismos procedimentales para generar copias en los diferentes puntos de control que se establezcan en los diferentes procesos. |
| d. El sistema deberá permitir sacar copias de seguridad diaria, mensual o por periodo o las establecidas por la entidad. |
| e. Garantizar la seguridad de la información (confidencialidad, estabilidad, integridad, no repudio e inviolabilidad) mediante la implementación de adecuados controles de seguridad, definidos en la fase de Consultoría. |
| f. Debe proveer cifrado para los passwords, incluso al ser transmitidos por la red o almacenados en el servidor |

¹ El diseño del sistema de información y sus características deben estar desarrolladas para soportar alta disponibilidad, tolerancia a fallos y continuidad del servicio, independiente de la plataforma sobre la cual sea desarrollada, la cual también debe estar afinada y sincronizada para que cumpla con las características descritas inicialmente. Es claro que los temas relacionados con alta disponibilidad, tolerancia a fallos y continuidad del servicio no son un aspecto exclusivo de la plataforma tecnológica (Manejador de Bases de Datos, Servidores, Comunicaciones y otros relacionados) sino que en ellos tiene mucho que ver el diseño, desarrollo e implementación del sistema de información.

- | |
|--|
| g. Debe proveer inicio de sesión único y se debe autenticar con una cuenta de dominio en el Directorio Activo, para los usuarios internos (funcionarios, contratistas, etc...) |
| h. Debe implementar encriptación de datos y administración de llaves encriptadas. |
| i. Debe crear marcas de agua obligatorias para documentos impresos |
| j. Debe proveer un mecanismo para separar los usuarios de ambientes de prueba, preproducción y producción. |

6.8.1.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

6.8.2.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. Las validaciones que diseñaremos son:

Web

- Validar acceso externo.
- Validar la vigencia de la autenticación.
- Validar el perfil involucrado.
 - Validar la existencia de solo una sesión concurrente.

Aplicación

- Validar la invocación por solo los servidores web habilitados.
- Registrar los intentos de conexiónIPs Usuarios Aplicaciones.

Bases de Datos

- Validar que se realicen llamado únicamente por los servidores de aplicación.
- Validar que no se realicen consultas directas por otras aplicaciones

6.8.3.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 SENADO.

Las limitaciones se definirán en los roles los cuales definen cuales funcionalidades pueden ejecutar los usuarios que tenga ese rol. Las funcionalidades que no tenga asignadas no podrán ser invocadas o ejecutadas

6.8.4. Identificación y Autenticación.

La autenticación se debe hacer a nivel del aplicativo, se debe permitir la integración con servicios de directorios basados en el estándar LDAP para usuarios internos y para usuarios externos de acuerdo a lo establecido por la entidad, especialmente para las funcionalidades que permiten autenticación, autorización, administración y almacenamiento de datos de usuarios y todos los que intervienen en el sistema.

La conexión y autenticación con el directorio activo (LDAP) debe ser dinámica en la cual no se debe realizar copia de la misma, si no, consultar el árbol de conexión entregado por la entidad.

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

6.8.5. Políticas y contraseñas.

Las mejores prácticas incluyen el manejo de políticas para las contraseñas, las cuales serán definidas por el SENADO.

6.8.6. 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
- Rol almacén
- Rol suministros
- Rol contable
- Rol de Consulta

NOTA: el sistema debe permitir parametrizar roles nuevos y existentes.

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.

- i. Creación
- ii. Modificación
- iii. Inactivación
- Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas, opciones o módulos

Los roles serán reflejados en el modelo como actores y tendrán relacionados los casos de uso (funcionalidades) que podrán ejecutar. Se debe llevar un log de las novedades realizadas a los usuarios registrados en el sistema a nivel de datos personales y roles asignado. Esto teniendo en cuenta que los usuarios pueden cambiar de roles a lo largo del tiempo y debe poder establecer que rol tenía un usuario en el momento de una transacción.

6.8.7. Auditoría.

Se debe implementar el registro de acciones realizadas por los usuarios a las principales transacciones (usuario, fecha y hora, entre otros) 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 generarán trazabilidad. Se deben incluir el diseño de reportes y alertas de indicadores de seguridad.

Las creaciones modificaciones y eliminaciones deberán ser almacenadas con la horas, usuario y estación que se realizó.

Se debe extraer por medio de un reporte que podrán filtrar por cualquier combinación de los anteriores parámetros

6.9. 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 los demás elementos que el SENADO considere 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.

6.10. Mantenibilidad.

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

Escalabilidad: El sistema debe estar construido sobre la base de un desarrollo incremental el tiempo, de manera tal que nuevas funcionalidades y requerimientos relacionados puedan ser incorporados afectando el código existente de la menor manera posible:

- Horizontal (aumentando el número de servidores)
- Vertical (aumentando la memoria RAM de los servidores y CPU).

6.11. Proceso de Adaptación.

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 con su respectiva documentación. Deberá ser construida para IIS (Internet Information Server) ²

6.12. Documentación.

Se debe especificar la definición y el manejo de la documentación y funcional del sistema de información, establecer procedimientos claros de actualización y aprobación. El software, por lo menos, debe tener:

- Cronograma
- Documento con recomendaciones para espacio en servidores para el almacenamiento y su seguridad.
- Material E-LEARNING, sobre los módulos contratados.
- Documento Manual técnico
- Documento Manual de usuario final
- Documento Ayuda en línea de la aplicación
- Permisos y Patentes, certificación de derechos de propiedad intelectual.
- Documento Manual de administración
- Documento Manual de instalaciones e integración
- Documento de fallos y errores
- Documento Instructivos técnicos y funcionales.

Toda la documentación debe estar en idioma español.

Dentro del proyecto se debe incluir en la documentación relacionada con los planes de prueba del sistema, que abarquen como mínimo las pruebas funcionales, pruebas técnicas, pruebas de stress y pruebas test de penetración al sistema. Las pruebas realizadas por el proponente seleccionado deberán estar certificadas de modo que las funcionalidades que se entreguen para pruebas, deberán tener una calidad suficiente.

² El software ofertado debe operar sobre la infraestructura tecnológica existente en el senado de la República

7. IMPLEMENTACIÓN

El proponente deberá incluir los siguientes servicios necesarios para la implementación y puesta en operación de la solución ofrecida

7.1. Licenciamiento.

La licencia debe ser perpetua, el SENADO deberá ser propietario de los derechos de uso de la licencia. Los derechos de autor serán propiedad de quien legalmente los tenga así registradas.

El software y sus herramientas deben ser un producto licenciado, por lo cual no debe ser basado en software libre ni el GNU.

Deberá ser entregado al SENADO el licenciamiento de uso a perpetuidad y la licencia de uso para usuarios ilimitados a perpetuidad y de todos los componentes que integrarán la solución.

La licencia de uso solo será instalada en los servidores, junto con los ambientes de producción requeridos y solo será utilizada por el SENADO en todas sus dependencias, pero no por ninguna otra de entidad.

Los derechos de actualización de las licencias y módulos implementados deben garantizar el buen funcionamiento de la aplicación instalada, el proveedor debe comprometerse a realizar los cambios que cumpla con las nuevas leyes y decretos reglamentarios, resoluciones, circulares, anexos, y demás documentos emitidos por las entidades de control y las cuales hayan sido formalmente emitidas y sean de carácter obligatorio por el Gobierno Nacional o las entidades de control y/o por mejoras realizadas en el software, tanto como en cada uno de los servicios generados por la empresa contratista (Service Packs, Motores de Bases de Datos, Nuevas versiones en arquitectura de Software) y cualquier sugerencia que contribuya con el buen desempeño, por una duración de dos (2) años a partir de la finalización de la implementación del mismo y no se podrá generar ningún costo adicional por las mismas.

7.2. Instalación

El proponente seleccionado deberá entregar el software instalado y configurado en la infraestructura tecnológica, teniendo en cuenta lo presentado en el numeral 7.8 infraestructura para producción y preproducción.

7.3. Migración.

Se considera que la migración de datos es una de las actividades críticas de éxito en el proceso de implementación, presenta riesgos en su ejecución, por lo anterior se han diseñado mecanismos tendientes a garantizar que los productos y actividades que el Senado debe entregar y ejecutar cumplan con los tiempos establecidos.

El proponente seleccionado deberá:

Implementar un plan de migración de datos que ejecutará con el fin de hacer la carga de datos a la base de datos del sistema ofrecido.

El proceso de Migración deberá contemplar como mínimo las siguientes etapas o fases:

- ✓ Extracción de la información de la base de datos de Dinámica Gerencial. Esta Base de datos contiene información de los activos y bienes desde el año 2004 a la fecha.
- ✓ Organización de la información conforme a la estructura de datos de la Base de Datos del Sistema ofrecido.
- ✓ Cargue de la información migrada en la Base de Datos del Sistema ofrecido,
- ✓ Verificación funcional de la información migrada en la Base de Datos del Sistema ofrecido, lo cual debe permitir emitir los reportes correspondientes y necesarios para la validación de la información migrada, durante el plazo de ejecución del contrato.

El oferente debe entregar un informe final sobre pruebas y operación de los datos migrados y en cumplimiento a lo requerido por la entidad.

Todas las actividades descritas en el punto 7.3 Migración, deberán ser realizadas por el proveedor.

7.4. Parametrización

Durante esta fase el proponente y el Senado, definirán precisa y completamente, los parámetros que el sistema de información necesita para funcionar con niveles satisfactorios de desempeño. Esto implica un acompañamiento en la revisión y ajuste a la parametrización y formulación inicial con los aspectos particulares del Senado.

Revisar el marco legal pertinente a cada módulo del sistema de información y entregar al Senado una cartilla de formulación general del sistema.

El proponente seleccionado parametrizará el sistema con base en la cartilla levantada, el personal que parametrize debe poseer formación y experiencia en parametrización del sistema.

El proponente seleccionado hará la personalización del sistema con los logotipos y títulos del Senado (Look and Feel) así como la configuración de seguridad, asignando los perfiles, nombres de usuarios y claves

7.5. Capacitación.

Esta deberá incluir planes de Capacitación funcionales y técnicos, los cuales se ejecutarán dentro de la ejecución contractual, se deberán entregar los respectivos certificados de asistencia, material de estudio y refrigerios.

Las capacitaciones deben ser realizadas por uno o varios instructores certificados por el fabricante de la herramienta(s) adquiridas, la capacitación debe ser en la ciudad de Bogotá D.C; el contratista debe proveer el sitio y medios tecnológicos para la capacitación.

Si durante la prestación del servicio, se presenta una situación que amerite el cambio de las personas del equipo de trabajo, sustentada por alguna de las partes, el contratista se obliga a cambiar el personal, cumpliendo con los perfiles mínimos en el equipo mínimo de trabajo exigido

por el Senado.

El horario de instrucción será acordado y aprobado con el Senado, las instalaciones de instrucción deben ser cercanas a las instalaciones de la entidad.

Se deben garantizar capacitación como mínimo cinco personas por cada una de las dependencias involucradas incluyendo sus unidades o secciones.

Esta deberá incluir dos (2) planes de Capacitación, los cuales se ejecutarán dentro de la ejecución contractual, debe contar con soporte de asistencia y entregar certificado personalizado de la capacitación:

Capacitación a Usuarios de Almacén

- Mínimo veinte (20) horas enfocadas en el uso del control de activos, traslados, serialización.
- Enfocadas a conocer la operación, funcionalidad, administración operativa del Sistema, Atención y solución de alertas, alarmas y errores en la operación.
- Esta capacitación deberá darse a los funcionarios que la División de Bienes y servicios Designe.

Capacitación a Usuarios de Suministros

- Mínimo veinte (20) horas enfocadas en
- Enfocadas a conocer la operación, funcionalidad, administración operativa del Sistema, Atención y solución de alertas, alarmas y errores en la operación.
- Esta capacitación deberá darse a los funcionarios que la División de Bienes y servicios Designe.

Capacitación a Usuarios de Contabilidad

- Mínimo veinte (20) horas enfocadas en
- Enfocadas a conocer la operación, funcionalidad, administración operativa del Sistema, Atención y solución de alertas, alarmas y errores en la operación.
- Esta capacitación deberá darse a los funcionarios que la División financiera y presupuesto Designe.

Capacitación Personal Técnico

- Mínimo veinte (20) horas enfocadas a conocer todos los aspectos de administración del Sistema desde el rol TI, en cuanto a instalación, desinstalación, reinstalación, copias de respaldo, configuración de usuario final si aplica, revisión de Logs de seguridad, atención y solución de alertas, alarmas y errores en la operación que deba resolver el área de TI.
- Esta capacitación deberá darse a los funcionarios que la entidad designe.
- En esta deberá definir el perfil de los usuarios de la división de planeación y sistemas que deberá tomar la capacitación.
- Se debe aplicar una evaluación al culminar la capacitación.
- El proponente será el encargado de la logística y coordinación de las capacitaciones, tanto en espacios físicos como cronograma de ejecución.

7.6. Paralelo, Pruebas y/o Ajustes.

Mediante esta actividad se ejecutará 1 paralelo del Software de administración y gestión de bienes, para determinar el punto de inicio en producción del sistema, se ejecutarán pruebas relacionadas con la parametrización y formulación y se realizarán los ajustes que sean necesarios.

Para desarrollar los paralelos, el proponente seleccionado ejecutará y apoyará directamente los trabajos en las instalaciones del Senado.

Se ejecutarán pruebas relacionadas con la parametrización y formulación y se realizarán los ajustes que sean necesarios.

El proponente seleccionado diseñará y ejecutará directamente los trabajos en las instalaciones del Senado.

El Proponente dispondrá de un plan de pruebas que deberá ser aprobado por la División de Planeación y sistemas; este deberá ser ejecutado para el respectivo recibo a satisfacción del sistema de información.

El proponente deberá realizar todas las pruebas necesarias para comprobar el correcto montaje, conexión y condiciones para el adecuado funcionamiento del Software de administración y gestión de bienes, sus herramientas, el sistema operativo y motor de base de datos; estas pruebas serán coordinadas por la supervisión por parte del Senado.

7.7. Garantía

La garantía del Software de administración y gestión de bienes, software instalado, sus herramientas, sistema operativo, motor de base de datos, base de datos y servidores contra defectos de fabricación por un tiempo no inferior de tres (3) años, los cuales serán contabilizados a partir de la fecha de recibo a satisfacción de la solución.

El contratista deberá anexar certificación del fabricante donde conste que garantizará el Software de administración y gestión de bienes, software instalado, sus herramientas, el sistema operativo y el motor de base de datos contra defectos de fabricación.

7.8. Soporte y acompañamiento

El soporte y acompañamiento del sistema será de dos años a partir de la puesta en marcha del software de administración y gestión de bienes en ambiente de producción recibida a satisfacción por parte de la entidad.

El soporte y acompañamiento debe cubrir todos y cada uno de sus componentes y al sistema de información en su totalidad, la cual debe cubrir cualquier tipo de falla sin ningún costo adicional para el Senado de la República. Estas fallas deberán ser atendidas en menos de dos (2) horas hábiles y solucionadas en menos de cuatro (4) horas hábiles, contadas ambas a partir del reporte el incidente.

El soporte y acompañamiento es por dos (2) años sin costo adicional para la Entidad e incluye:

1. Actualizaciones de últimas versiones de la solución.
2. parametrización y configuración del sistema de Información por cambios en la normatividad o procesos al interior de la Entidad.

En caso de presentarse inconsistencias, problemas o solicitudes sobre el software instalado, el proveedor deberá atender estas solicitudes en un tiempo de respuesta de máximo dos (2) horas.

El servicio de soporte se prestará como mínimo los días hábiles de la semana, entre las 7:00 A.M. y las 6:00 P.M.

El proveedor deberá ofrecer el soporte técnico en sitio necesario para la instalación, estabilización del sistema de información.

Se deberá garantizar las actualizaciones, incluyendo nuevas versiones del software implantado con las modificaciones y/o cambios de la normativa a que haya lugar durante el tiempo de ejecución del contrato y los (2) años de garantía y de soporte técnico y acompañamiento.

Acuerdos Niveles de Servicio

- El contratista debe contar con un servicio que permita la atención y recepción de los requerimientos solicitados por el Senado de la Republica, Para ello debe indicar los canales de comunicación en Bogotá D.C.
- Ante un requerimiento de soporte por parte del Senado de la Republica, el contratista se obliga a atender y diagnosticar este requerimiento en un tiempo de respuesta no máximo de dos (2) horas, solucionarlo y dejarlo operativo normal dentro de las 4 horas siguientes a la solicitud.
- El contratista deberá prestar el servicio de soporte telefónico o a través de la Web o por correo electrónico en la administración, configuración, resolución de problemas de manera ilimitada durante el tiempo de garantía de todo el sistema.
- Todo soporte técnico que requiera apagado del equipo donde se encuentre instalado la solución implementada deberá ser coordinado previamente con el Senado de la Republica.
- Los costos en que incurra el contratista para atender cualquier solicitud de soporte, mantenimiento preventivo o correctivo necesarios para garantizar el correcto funcionamiento de la solución implementada, durante la ejecución, periodo de soporte y garantía, correrán por cuenta del contratista y no tendrán costo adicional para el Senado de la Republica.

Soporte preventivo: el contratista deberá realizar mínimo dos (soporte preventivo) en el año durante el periodo de ejecución del contrato, garantía y soporte técnico (sin costo adicional), donde incluya:

- Afinamiento de la solución.
- Afinamiento de las bases de datos
- Corrección de errores.
- Análisis logs de eventos.
- Análisis y auditoria del sistema de información.
- Informe final y recomendaciones de cada visita.
- Actualización de parches de seguridad del producto.

Las fechas de mantenimientos preventivos deberán ser acordadas previamente con el Senado de la Republica, garantizando el normal funcionamiento y continuidad de la prestación de los

servicios.

El contratista entregara un plan de trabajo donde se especifique fechas de realización de mantenimientos, actividades a realizar, los recursos requeridos por el mismo, así como los requeridos por parte de la entidad, previa aprobación de Senado para su ejecución.

El contratista deberá suministrar un informe escrito de cada visita, evidenciando recomendaciones para obtener el mejor desempeño de la solución implementada, el cual debe ser aprobado por el Senado de la Republica.

Soporte Correctivo: el contratista deberá realizar todos los mantenimientos correctivos que sean necesarios para mantener en funcionamiento la solución.

El proponente suministrara los canales de comunicación para los canales de soporte, en ningún momento el Senado proporcionara enlaces, canales directos o VPN'S para el cumplimiento de esta tarea.

7.9. Infraestructura para Preproducción y Producción.

El contratista debe proporcionar la arquitectura para los ambientes definidos por el Senado de la Republica, en el cual establezca la cantidad de servidores y elementos de comunicación que requieran para el óptimo funcionamiento de la solución ofrecida teniendo en cuenta la siguiente infraestructura técnica disponible.

Licencias: el proveedor debe proporcionar a nombre del Senado de la Republica las licencias necesarias para el óptimo funcionamiento de la solución.

Infraestructura servidores: el Senado de la República dispondrá de la siguiente infraestructura para el desarrollo de la solución, todo requerimiento adicional en software o infraestructura debe ser asumido por el proveedor y no compromete a la entidad a su adquisición.

- Servidor prueba Base de datos
Licencia Windows Server 2012
Motor base de datos Windows SQL Server Standard
Processor 6 nucleos
Ram 10 GB
Disco: 100 GB
- Servidor prueba Aplicaciones
Licencia Windows Server 2012
Processor 6 nucleos
Ram 10 GB
Disco: 80 GB
- Servidor producción Base de datos
Licencia Windows Server 2012
Motor base de datos Windows SQL Server Standard
Processor 6 nucleos
Ram 10 GB
Disco: 100 GB

- Servidor producción Aplicaciones
Licencia Windows Server 2012
Processor 6 nucleos
Ram 10 GB
Disco: 80 GB

NOTA: Para todos los ámbitos se deben manejar ambientes de producción y preproducción, además debe soportar una alta disponibilidad de la herramienta en fase de producción, que deberá ser realizada por el proveedor. En el momento de salida a producción, los servidores de prueba se utilizarán para la implementación de la alta disponibilidad.

7.10. Implementación y Entrega

A partir de la firma del acta de inicio, el contratista contara con plazo máximo de treinta días calendario para la entrega e instalación de las licencias, base de datos, servidores y de la solución ofrecida

Firmado el acta de inicio, el contratista contara con un máximo de ocho (8) meses para el desarrollo, configuración, parametrización, implementación, migración, pruebas y puesta en funcionamiento del Software de administración y gestión de bienes, esto de acuerdo con el cronograma que se establezca al firmar el acta de inicio para la realización de estas labores

En ningún caso el plazo máximo de ejecución del contrato superara los 6 meses contados a partir de la fecha de suscripción del acta de inicio.

8. EQUIPO DE TRABAJO MÍNIMO REQUERIDO

Para una adecuada ejecución del proceso de adquisición, implementación y soporte del sistema de información de apoyo a los procesos de administración y gestión de los bienes para el Senado de la República se requiere que el equipo de acompañamiento, cumpla como mínimo con los siguientes perfiles:

Ver Archivo en Excel

9. FLUJOGRAMA PROCESO DE PROPIEDAD PLANTA Y EQUIPO



10. FLUJOGRAMA MEDICION POSTERIOR DE LA PROPIEDAD PLANTA Y EQUIPO

Por su Costo	
Menos: Depreciación Acumulada	
Menos: Deterioro Acmulado	

11. FLUJOGRAMA VALOR A DEPRECIAR DE LA PROPIEDAD PLANTA Y EQUIPO

Costo del Activo	
Menos: Valor Residual	
Valor a Depreciar	

12. FLUJOGRAMA VALOR DEL SERVICIO RECUPERABLE DE LA PROPIEDAD PLANTA Y EQUIPO

VALOR DEL SERVICIO RECUPERABLE	
VALOR DE MERCADO	
Menos: Costos de Disposición	
Trámites Legales	
Comisión sobre venta	
Gastos para colocar el Bien en condiciones de venta	
Costos o Gastos de transporte del activo	

13. FLUJOGRAMA INDICIOS DE DETERIORO DE LA PROPIEDAD PLANTA Y EQUIPO

