Código Producto	
Nombre Producto	Módulo de Seguimiento y Monitoreo a Planes de Desarrollo Territoriales
Nombre Entregable	Documento de requerimientos para el desarrollo del sistema de información
Fecha Inicio	01/03/2020
Fecha Fin	05/06/2020
Codigo Entregable	

PROYECTO: MÓDULO DE SEGUIMIENTO Y MONITOREO A PLANES DE DESARROLLO TERRITORIALES

DOCUMENTO DE REQUERIMIENTOS

Descripción breve

En este documento se presentan los requerimientos funcionales y no funcionales de alto nivel para el módulo de seguimiento y monitoreo a los PDT

TABLA DE CONTENIDO

Tabla de contenido 1
Control del documento 2
1 Introducción 3
1.1 Descripción del Documento 3
1.2 Propósito del documento 3
2 Información del dominio del problema 3
2.1 Glosario de Términos 3
3 Requerimientos del sistema 4
3.1 Historias de usuario ..... **¡Error! Marcador no definido.**
3.2 Identificación de características funcionales 4
3.3 Requerimientos no funcionales 4
4 Principios de la arquitectura ..... **¡Error! Marcador no definido.**
5 Elementos de la arquitectura ..... **¡Error! Marcador no definido.**

CONTROL DEL DOCUMENTO

Versión	Descripción	Fecha	Autor(es)	Revisión
1.0	Versión inicial	06/04/2020	Ximena Buchelly, José Manuel Díaz Medina	
1.1	Ajustes de texto en el documento referenciando módulo de seguimiento y monitoreo a PDT	11/05/2020	Ximena Buchelly, José Manuel Díaz Medina	
1.2	Respuestas a comentarios DNP-OTSI	12/06/2020	José Manuel Díaz Medina	

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN DEL DOCUMENTO

1.2 ESTE DOCUMENTO PRESENTA LOS REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES DE ALTO NIVEL, ES DECIR SIN DETALLAR, PARA D*ISEÑAR Y DESARROLLAR EL MÓDULO DE SEGUIMIENTO Y MONITOREO A PLANES DE DESARROLLO TERRITORIALES EN EL MARCO DE LA CONCEPTUALIZACIÓN DEL MODELO DE GESTIÓN TERRITORIAL (MGT).*PROPÓSITO DEL DOCUMENTO

Brindar información más detallada a la presentada en los términos de referencia del proyecto, que permita a los proponentes conocer el alcance del proyecto para que realicen estimaciones en tiempo y costo más acertadas. Por lo tanto, es mandatorio conocer dichos términos para conocer el contexto del proyecto.

2 INFORMACIÓN DEL DOMINIO DEL PROBLEMA

2.1 GLOSARIO DE TÉRMINOS

- DDDR: Dirección de Descentralización y Desarrollo Regional del DNP.
- DNP: Departamento Nacional de Planeación.
- Entidad territorial (ET): Departamentos y municipios de Colombia.
- Gobierno Nacional: poder ejecutivo, representado por los ministerios y entidades de orden nacional.
- OTSI: Oficina de Tecnología y sistemas de Información del DNP.
- Plan de Desarrollo Territorial (PDT): es el instrumento de planificación que orienta las acciones de las administraciones departamentales, distritales y municipales durante un período de gobierno. En éste se determina la visión, los programas, proyectos y metas de desarrollo asociados a los recursos públicos que ejecutarán durante los próximos 4 años.
- MGT: Modelo de Gestión Territorial
- SIEE: Sistema de Información para la Evaluación de la Eficacia. Permite hacer seguimiento a los planes de desarrollo.
- TerriData: Herramienta Web desarrollada y administrada por la DDDR, para la visualización de indicadores de orden nacional y territorial.
- KPT: Kit de Planeación territorial para la formulación de los PDT.
- Plan Indicativo (PI): Instrumento de planeación estratégica que complementa y contribuye a especificar el alcance de las disposiciones contenidas en el Plan de Desarrollo Territorial (PDT), constituyéndose en el insumo principal para establecer el nivel de cumplimiento y avance en relación con la implementación del mismo.
- GESPROY-SGR: Sistema de Gestión y Monitoreo a la Ejecución de Proyectos
- SPI: Sistema de Seguimiento a Proyectos de Inversión
- MGA: Metodología General Ajustada
- SISFUT: Sistema de Información del Formato Único Territorial (FUT)
- PDT: Plan de Desarrollo Territorial

3 REQUERIMIENTOS DEL SISTEMA

La identificación de los requerimientos del sistema se realizó teniendo en cuenta los siguientes insumos:

- Durante la vigencia 2017 y 2018 se realizó una consultoría que se encargó de evaluar el sistema de seguimiento a planes de desarrollo territoriales, esta consultoría se encargó de elaborar un diagnóstico donde se revisaron documentos, materiales y herramientas relacionados con el sistema de seguimiento a Planes de Desarrollo.
- Se llevaron a cabo entrevistas a funcionarios y/o contratistas de las alcaldías de seis municipios.
- Se consultó la opinión de los asesores del Proyecto de Fortalecimiento a las Entidades Territoriales (PFET) del DNP, quienes conocen de cerca la gestión de los municipios con los que trabajan.
- Se realizó una jornada de trabajo con 21 gobernaciones, para identificar los comentarios y recomendaciones relacionados con el seguimiento a planes de desarrollo territoriales, el sistema de información utilizado para el seguimiento y el rol de las gobernaciones en el proceso de seguimiento.

Para expresar las necesidades de los diferentes actores usamos historias de usuario, que permiten de una manera simple describir una tarea concisa que aporta valor.

3.1 IDENTIFICACIÓN DE CARACTERÍSTICAS FUNCIONALES

El sistema debe contar con las siguientes características funcionales:

3.1.1 Equipos de trabajo de las ET

- Inscripción

3.1.2 Construcción del Plan Indicativo

- Módulo para registro, modificación y desactivación de metas
- Creación y programación del plan indicativo
- Modificaciones del Plan Indicativo
- Exportar Plan Indicativo en diferentes formatos
- Cargue de soporte para la modificación de planes indicativos

3.1.3 Reportes e interoperabilidad

- Reportes parciales de avance físico de metas de resultado y de producto para las entidades territoriales, reportes definitivos para municipios,s gobernaciones, entes de control y DNP.
- Generación de diferentes tipos de visualizaciones de la información.
- Mecanismos de interoperabilidad con otros sistemas de información, como el KPT, la MGA, el SPI, el GESPROY-SGR y el SISFUT y TerriData.
- Resumen de Plan indicativo con información de avance de productos y resultados.
- Generación de alertas
- Mecanismo de interacción con ciudadanía.

3.1.4 Parametrización

- Gestión del contenido de las diferentes secciones

3.1.5 Seguridad

- Iniciar sesión
- Terminar sesión
- Gestión de usuarios
- Consultar usuarios
- Agregar usuario
- Modificar usuario
- Deshabilitar usuario
- Gestión de roles (entidades territoriales, departamentos, DNP, otras entidades)
- Módulo de auditoria y trazabilidad

3.1.6 Contenidos adicionales, instructivos y videos

- Consultar contenidos adicionales, instructivos y videos
- Agregar contenidos adicionales, instructivos y videos
- Modificar contenidos adicionales, instructivos y videos

3.2 ELIMINAR CONTENIDOS ADICIONALES, INSTRUCTIVOS Y VIDEOSREQUERIMIENTOS COMPLEMENTARIOS

Con base en reuniones con diferentes actores involucrados, los lineamientos de la OTSI y funcionalidades necesarias en sistemas de información (S.I) de este tipo se identificaron los siguientes requerimientos, teniendo en cuenta que se hace referencia como S.I al módulo de seguimiento y monitoreo a PDT.

3.2.1 Requerimientos de tecnología

- Línea base para el desarrollo de software es la plataforma Microsoft .NET Core, el sistema operativo para servidores es Windows, el lenguaje para desarrollo es C#, el motor de base de datos relacional es Microsoft SQL Server, el servidor web es IIS.
- Para temas de sistemas de información geográfica se usa la plataforma y servicios de ARCGIS.
- Ambientes diferenciados durante la ejecución del proyecto. Se deben disponer al menos tres
    - Ambiente de desarrollo
    - Ambiente de pruebas funcionales
    - Ambiente de pruebas de aceptación

  Los primeros dos ambientes, desarrollo y pruebas funcionales deben ser provistos por el Consultor, el DNP proveerá el ambiente de pruebas para las pruebas de aceptación.

- Ambiente diferenciado para la transición y puesta en producción del S.I.

  Este ambiente será provisto por el DNP. La aceptación final del producto software se hará inicialmente sobre el ambiente de pruebas de aceptación y finalizará cuando el S.I. se encuentre implementado y desplegado sin objeciones en el ambiente de producciónLa documentación técnica requerida es la siguiente:

    - Especificación de requerimientos funcionales y atributos de calidad del software.

- Código fuente del componente software, con todos sus módulos, librerías y demás dependencias de elementos constitutivos.
- Documento de arquitectura del sistema
- Informes de pruebas funcionales y no funcionales del sistema de información
- Manual técnico y de gestión del Sistema de Información
- Manual de Usuario y de operación del Sistema de Información

- La documentación técnica mencionada en el ítem anterior debe ser ubicada y entregada por el proveedor en el repositorio (DevOps Server) dispuesto por el DNP para el proyecto de acuerdo con la estructura definida por el DNP. El consultor debe mantener actualizado el código fuente de los diferentes proyectos en la herramienta destinada para tal fin, DevOps Server, y entregar a la Oficina de Tecnologías y Sistemas de Información la documentación relacionada con el proyecto, Pruebas unitarias, Documento de Arquitectura, Manuales Operativos, Manuales Técnicos, Catálogo de Servicios, Plan de Contingencia y Matriz de Riesgos relacionados con las aplicaciones y sistemas a cargo.
- Se requerirá previa autorización por parte del DNP, para la utilización de tecnologías, componentes o librerías de software no contempladas o adicionales a la línea base del DNP, así mismo el proveedor deberá entregar el correspondiente licenciamiento a nombre del DNP ya sea a perpetuidad o por un mínimo tres años según corresponda, con el respectivo soporte técnico y actualización del software, para cada ambiente, así: desarrollo, pruebas y producción por un lapso de tiempo mínimo de tres años.
- Metodología de referencia del DNP: El contratista debe adaptar su metodología de desarrollo a la metodología de referencia del DNP, se sugiere privilegiar el uso de metodologías ágiles de desarrollo.

3.2.2 Requerimientos de accesibilidad y usabilidad

- El sistema debe permitir realizar operaciones de lectura, escritura y eliminación sobre múltiples registros, cuando haya lugar, por ejemplo: eliminar todas las metas de producto de un plan de desarrollo.
- El sistema debe informar al usuario el resultado de las operaciones realizadas en el mismo.
- El sistema debe alertar y confirmar las operaciones que eliminen registros.
- El sistema debe contar con caracterizas adaptativas (responsive) para la visualización en dispositivos móviles.
- Acatar el decreto 620 del 2 de mayo de 2020, sobre servicios ciudadanos digitales.
- Los elementos, acciones y navegación de las interfaces de usuario deben ser consistentes y uniformes para todo el sistema
- El diseño de las interfaces de usuario debe orientarse a una comprensión fácil e intuitiva por parte del usuario, para reducir la demanda de asistencia o soporte técnico.
- El Sistema de información debe cumplir con los estándares Sitio Web descritos en la página 41 y diligenciar la matriz correspondiente, de acuerdo al manual de Gobierno en línea 3.1 http://programa.gobiernoenlinea.gov.co/apc-aa-files/e5203d1f18ecfc98d25cb0816b455615/manual3.1.pdf.
- El S.I debe permitir la parametrización de la visualización de acuerdo con la Guía de sistema gráfico del Gobierno de Colombia.
- El diseño de las interfaces de usuario debe estar orientado a reducir el tiempo de operación e incrementar la productividad
- El S.I debe cumplir con la guías de usabilidad y accesibilidad de la política de Gobierno Digital, véase (http://estrategia.gobiernoenlinea.gov.co/623/articles-8237_guia_usabilidad.pdf).

- El S.I debe cumplir con el Nivel A de Accesibilidad de la Política de Seguridad Digital y la norma NTC 5854, véase https://ntc5854.accesibilidadweb.co:
    - (3.1.1) 1.1 Textos alternativos
    - (3.1.1.1) 1.1.1 - Contenido no textual
    - (3.1.2) 1.2 Medios basados en el tiempo
    - (3.1.2.1) 1.2.1 - Sólo audio y solo vídeo (grabaciones)
    - (3.1.2.2) 1.2.2 - Subtítulos (pregrabados)
    - (3.1.2.3) 1.2.3 – Audio-descripción o Medio Alternativo (Pregrabado)
    - (3.1.3) 1.3 Adaptable
    - (3.1.3.1) 1.3.1 - Información y relaciones
    - (3.1.3.2) 1.3.2 - Secuencia con significado
    - (3.1.3.3) 1.3.3 - Características sensoriales
    - (3.1.4) 1.4 Distinguible
    - (3.1.4.1) 1.4.1 - Uso del color
    - (3.1.4.2) 1.4.2 - Control del audio
    - (3.2.1) 2.1 Accesible mediante el teclado
    - (3.2.1.1) 2.1.1 - Teclado
    - (3.2.1.2) 2.1.2 - Sin bloqueos de teclado
    - (3.2.2) 2.2 Tiempo suficiente
    - (3.2.2.1) 2.2.1 - Tiempo ajustable
    - (3.2.2.2) 2.2.2 - Pausar, detener, ocultar
    - (3.2.3) 2.3 Provocar ataques
    - (3.2.3.1) 2.3.1 - Umbral de tres destellos o menos
    - (3.2.4) 2.4 Navegable
    - (3.2.4.1) 2.4.1 - Evitar bloques
    - (3.2.4.2) 2.4.2 - Páginas tituladas
    - (3.2.4.3) 2.4.3 - Orden del foco
    - (3.2.4.4) 2.4.4 - Propósito de los enlaces (en contexto)
    - (3.3.1) 3.1 Legible
    - (3.3.1.1) 3.1.1 - Idioma de la página
    - (3.3.2) 3.2 Predecible
    - (3.3.2.1) 3.2.1 - Al recibir el foco
    - (3.3.2.2) 3.2.2 - Al introducir datos
    - (3.3.3) 3.3 Introducción de datos asistida
    - (3.3.3.1) 3.3.1 - Identificación de errores
    - (3.3.3.2) 3.3.2 - Etiquetas o instrucciones
    - (3.4.1) 4.1 Compatible
    - (3.4.1.1) 4.1.1 - Procesamiento
    - (3.4.1.2) 4.1.2 - Nombre, función, valor
- Habilitar en el sistema de información aquellas características funcionales y no funcionales, necesarias para la apertura de sus datos, de acuerdo con la normativa del Estado colombiano.

3.2.3 Requerimientos de desempeño

- El sistema debe soportar al menos dos mil usuarios conectados simultáneamente, durante al menos sesenta minutos.
- El sistema debe estar optimizado para que la transferencia de datos desde el servidor hacia el cliente sea mínima, dado que hay entidades territoriales con un ancho de banda limitado, no deberá sobrepasar los 4MB, excepto cuando se trate de archivos multimedia que deben ir por streaming o documentos (PDF, Excel o Word).
- El sistema debe ser ligero, no más de 2 MB por sección, esto debido a la deficiente conectividad a internet en las entidades territoriales.
- El sistema no debe degradar su rendimiento ante momentos pico de utilización.

3.2.4 Requerimientos de seguridad

3.2.4.1 Autenticación

- El S.I debe tener un módulo de administración de usuarios para la creación, modificación, eliminación o inactivación de usuarios.
- La autenticación del sistema debe realizarse contra el servicio federado dispuesto por el DNP. En el S.I la cuenta de los usuarios internos de la entidad debe estar integrada con el directorio activo.

3.2.4.2 Autorización

- El S.I debe realizar las autorizaciones por configuración de roles de acceso, la creación y modificación de los accesos comunes de múltiples usuarios. Solo personas autorizadas por la DDDR pueden tener acceso al sistema con roles con mayores privilegios que los usados por las entidades territoriales.
- El sistema debe permitir el acceso a la información limitado únicamente a los datos pertinentes según el contexto del usuario externo o interno autenticado y a la funcionalidad definida en la autorización del rol al que pertenezca el usuario.
- Los perfiles de los usuarios deben ser configurados por medio de roles.
- Los usuarios administradores podrán ver toda la información que carguen los usuarios normales del sistema, pero no podrán modificarla.
- Los usuarios de la aplicación no deben contar con acceso a la base de datos, para ello debe existir un usuario de servicio en la base de datos para brindar esta comunicación. El usuario de bases de datos debe ser una cuenta de servicio.
- Los permisos de acceso deben realizarse exclusivamente por los servicios que presta cada servidor, a través del firewall de la Entidad, ya sea para publicaciones como para acceso interno.
- El acceso a las bases de datos de las aplicaciones debe ser restringido solamente a los usuarios que la administran y la del servicio que se comunica con la aplicación

3.2.4.3 Administración

- La administración de la base de datos es responsabilidad del DNP a menos que la entidad exija lo contrario.

3.2.4.4 *Registros de auditoría*

- El S.I. debe contar con logs de auditoria sobre los cambios realizados en los diferentes registros del sistema y proveer los mecanismos para consultarlos. El consultor debe revisar la Guía G.SIS.02 Guía Técnica de Sistemas de Información -Trazabilidad de MinTIC versión 1.0 para su implementación en el Sistema de información, véase https://www.mintic.gov.co/arquitecturati/630/w3-article-9263.html.

3.2.4.5 Manejo *de sesiones*

En el S.I el tiempo de inactividad de una sesión activa no debe ser superior a 15 minutos.

3.2.4.6 Interfaces

- El consultor entregará un documento técnico donde se detalla el funcionamiento de los servicios web y sus respectivos métodos HTTPS. El S.I debe tener identificadas las interfaces y recursos que comparte con otros sistemas de información
- El Sistema de información sólo debe permitir archivos con extensiones .pdf, .doc, .docx, .xls, .xlsx, así mismo debe indicarle esto al usuario.
- El consultor debe diligenciar la Hoja de Servicio donde se identifica toda la información técnica, puertos origen, destino, excepciones antivirus etc, al finalizar el proyecto.
- El consultor debe indicar al DNP los puertos con los que interactúan los servicios, servidores que hacen parte del sistema de Información.
- El consultor debe indicar al DNP las excepciones de antivirus en los servidores del sistema de información.

3.2.4.7 Normatividad

- Todo el contenido audiovisual desarrollado por el Consultor debe cumplir con la normativa vigente en Derechos de autor.
- Cumplir con los lineamientos de administración de bienes disponible en https://www.dnp.gov.co/DNP/sistema-gestion-decalidad/Paginas/apoyo.aspx, revisar los numerales del Lineamiento sobre ingresos y registros de bienes a los inventarios, “Para Ingresos y Registros de Bienes Adquiridos”, “Ingresos y Registros de Bienes Transferidos por los Proyectos”
- El proyecto debe registrar el software en la Dirección Nacional de Derechos de Autor y remitir el certificado de inscripción, como requisito previo para la suscripción del acta de recibo de transferencia al DNP.
- El consultor debe preservar la normativa de derechos de autor del DNP. El Contratista se compromete a no implementar hardware y/o software en la Entidad que no se encuentre debidamente autorizado por la Oficina de Tecnologías y Sistemas de Información.
- El Sistema de Información debe tener un enlace al Sistema de PQRD del DNP, con el fin de cumplir con el proceso de Atención a Peticiones del DNP, donde todas las solitudes que los ciudadanos y grupos de interés radiquen en el sistema Orfeo serán respondidas por el administrador funcional del Aplicativo/sistema/Portal. Se tendrán en cuenta los protocolos de atención al ciudadano que contiene los canales de atención definidos por el DNP, los cuales pueden ser consultados en https://www.dnp.gov.co/atencion-al-ciudadano/Paginas/carta-de-trato-digno.aspx.
- El Sistema de Información debe enlazar la página de Políticas y Privacidad al link del portal del DNP.
- Si el Sistema de Información recolecta información personal de los ciudadanos y grupos de interés debe acogerse a la política de protección de datos DNP descrita en el Manual y Políticas de seguridad, al Lineamiento para la Política de Tratamiento de la Información de Datos Personales en el DNP y el Lineamiento para la Identificación y Valoración de Activos de Información en el Sistema de Seguridad de la Información disponibles en https://www.dnp.gov.co/DNP/sistema-gestion-decalidad/Paginas/apoyo.aspx.
- El Sistema de Información no debe publicar documentos que contengan información personal privada o sensible.
- El consultor debe conocer, aplicar el “Manual y políticas de seguridad de la información” SE-M01 publicado en la Intranet del DNP y participar en las actividades relacionadas con el Sistema de Gestión de Seguridad de la Información del DNP.

- El consultor debe informar de manera anticipada a la Oficina de Tecnologías y Sistemas de Información los cambios y despliegues que se requieren en los Sistemas de Información relacionados con el objeto del contrato y a cargo de la dependencia, con el fin revisar y emitir el aval para el proceso de gestión de cambios
- El consultor debe asistir cuando sea necesario o requerido, a las reuniones del Comité de Arquitectura de TIC, establecido y liderado por la Oficina de Tecnologías y Sistemas de Información con el objetivo de realizar el análisis, evaluación y seguimiento a las iniciativas y proyectos de TIC desarrollados en la Entidad.
- El consultor debe conocer y cumplir con los estándares y buenas prácticas establecidas por fabricantes e industria en materia de TIC, asociadas con el objeto y actividades contractuales a desarrollar.
- El consultor debe conocer y cumplir con las políticas, lineamientos, estándares y normatividad establecidas por el DNP, MINTIC y el Gobierno Nacional, en materia de implementación y uso de tecnologías.

3.2.4.8 Prevención de ataques A1-Inyección (OWASP)

- Los errores generados por sentencias erróneas ingresadas deliberadamente en el S.I. no deben presentar información relacionada con la versión de la base de datos.
- Las casillas de autenticación e ingreso de datos en el S.I deben contar con validación de datos que filtran caracteres especiales de sentencias SQL.
- En las consultas públicas el S.I debe tener la opción de validación de captcha, con el fin de evitar la denegación de servicios.
- El S.I debe controlar los caracteres especiales en campos para evitar ataques de inyección de código.
- El S.I debe controlar los tipos de datos permitidos por cada campo

3.2.4.9 Prevención de ataques A2-Pérdida de autenticación y Gestión de Sesiones (OWASP)

- Incluir en el encabezado (header) “Cookies: secure: httponly”
- Los identificadores de sesiones deben variar entre cada sesión de un usuario.
- Los identificadores de sesiones no deben ser fácilmente predecibles, contando con suficiente aleatoriedad.
- El S.I debe contar con mecanismos que impidan la autenticación de sesiones a través de un único identificador de sesión (cookie).
- Los identificadores de sesiones no se deben presentar en la URL
- Para la autenticación el S.I debe usar el protocolo seguro (HTTPS) con un certificado digital firmado por una entidad certificadora de confianza con el dominio definido por la Entidad.
- El S.I debe utilizar protocolos seguros (SFTP, HTTPS) para la transferencia de datos entre el cliente (browser) y el servidor de aplicaciones.
- El S.I debe usar solo verbos o métodos http GET/POST o indicar al DNP los métodos adicionales requeridos para evitar bloqueos
- Las contraseñas no deben ser almacenadas en texto plano, se deben proteger por medio de técnicas criptográficas, incluyendo el código las Cadena de conexión. El algoritmo de cifrado debe ser SHA256 o superior.
- Toda contraseña debe ser compleja y no incluir DNPaño+
- El S.I debe realizar la correcta eliminación de los indicadores de sesiones

3.2.4.10 Prevención de ataques A3-Secuencia de comandos en sitios Cruzados (OWASP)

- Todas las casillas de ingresos de datos deben contener validaciones que eviten la inyección de código (XSS, SQLi, HTMLi)

3.2.4.11 Prevención de ataques A4-Referencia Directa Insegura a Objetos (OWASP)

- El S.I debe restringir el acceso a recursos de otros usuarios modificando parámetros HTTP (p.e. cookie de sesión)
- Un usuario no debe acceder a información de otro usuario a menos que el rol lo permita
- Las tareas críticas deben ser ejecuten con cuentas de servicio y deben contar con restricciones y/o validaciones que eviten scripts o robots

3.2.4.12 Prevención de ataques A5 – Configuraciones de Seguridad Incorrecta (OWASP)

- El software base usado en el S.I debe encontrarse actualizado (Sistema Operativo, base de datos, aplicación, componentes, entre otros)
- Los servidores de producción del S.I no deben almacenar versiones anteriores ni backups, para ello debe existir un ambiente de pruebas.
- No deben existir cuentas por defecto en los diferentes componentes del aplicativo (p.e. FTP, portal de administración, ssh.
- El sistema de Información debe usar cuentas de servicio (no locales ej networkservice), ni la misma cuenta para múltiples servicios.
- La administración del S.I aplicación debe realizarse a través de protocolos seguros (cifrados), tales como HTTPS, SSH, entre otros.
- Se debe restringir la información que se presenta en los errores de IIS y bases de datos, estos pueden presentar información útil para la ejecución de futuros ataques.
- El listado de directorio de IIS debe encontrarse deshabilitado, a menos que el negocio lo requiera. En el sistema de Información no se deben exponer archivos de configuración (.ini, .config)
- Se debe controlar el acceso a las rutas URL que permitan saltar validaciones hacia abajo y hacia arriba (ejemplo ..//)
- Antes de la salida a producción de los aplicativos, éstos deben cumplir con los análisis de vulnerabilidades que realiza la entidad con el fin de verificar o detectar vulnerabilidades y/o debilidades que impliquen riesgos de seguridad.
- El consultor debe realizar las correcciones de las vulnerabilidades reportadas por la Oficina de Tecnologías y Sistemas de Información, todas deberán ser remediadas y/o mitigadas, especialmente las altas o medias, sustentando los riesgos de aquellas que no puedan ser del todo eliminadas, para el momento de la entrega definitiva y/o durante el tiempo de garantía.
- No se debe hacer referencia a ningún usuario y contraseña en texto plano dentro del código o archivos de configuración
- El sistema de información debe tener mínimo 3 capas (Front end, Aplicación, Base de datos), los front-end no deben almacenar ningún tipo de información.
- En el sistema de Información no se debe hacer referencia a ninguna dirección IP dentro del código o archivos de configuración
- Los parámetros de autocompletar contraseñas deben deshabilitarse.
- Habilitar la opción 'X-Content-Type-Options: nosniff' en el encabezado
- Habilitar en el encabezado http la opción "X-XSS-Protection: 1; mode=block"
- Habilitar en el encabezado http las opciones “Cache-Control: no-cache,no-store” and “Pragma: no-cache”
- Con el fin de proteger ante ataques tipo 'ClickJacking', habilitar en el encabezado las opciones “X-Frame-Options: ALLOW-FROM https://www.dnp.gov.co”, “X-Frame-Options: ALLOW-FROM https://www.cnp.gov.co”, “X-Frame-Options: ALLOW-FROM https://www.sgr.gov.co”, “X-Frame-Options: ALLOW-FROM

https://www.portalterritorial.gov.co", "X-Frame-Options: ALLOW-FROM https://www.sisben.gov.co", "X-Frame-Options: ALLOW-FROM https://www.sucop.gov.co".

- En el sistema de Información las imágenes, js y demás componentes no deben utilizar CDNS (redes de despliegue de contenido) salvo que sean internos para evitar ataques de defacement.
- En el sistema de Información el usuario de acceso anónimo de IIS/Apache no deben tener ningún privilegio superior a lectura y ejecución.

*3.2.4.13 Prevención de ataques A6 – Exposición de datos sensibles **(OWASP)***

- Utilizar protocolos seguros (SFTP, HTTPS) para la transmisión de información sensible (Ej. usuario, contraseña).
- Las contraseñas de usuario deben ser protegidas por medio de técnicas criptográficas de una vía (SHA256 o superior) desde la aplicación.

*3.2.4.14 Prevención de ataques A7 – Ausencia de control de acceso a funciones (autorización) **(OWASP)***

- El acceso al portal de administración debe encontrarse restringido solamente al rol del administrador autenticado.
- El acceso al portal de administración debe realizarse únicamente desde el interior de la entidad. Se debe deshabilitar la administración de los sitios desde internet.

*3.2.4.15 Prevención de ataques A8 – Falsificación de peticiones en sitios Cruzados (XSRF) **(OWASP)***

- Los usuarios no autenticados deben tener restricción en la ejecución de tareas sin supervisión, tales como ejecución de scripts o programas (p.e. captcha).

*3.2.4.16 Prevención de ataques A9 – Utilización de componentes con vulnerabilidades conocidas **(OWASP)***

- La aplicación en su conjunto debe hacer parte de una gestión periódica de vulnerabilidades.

*3.2.4.17 Prevención de ataques A10 – Redirección y reenvío no válido **(OWASP)***

- Las funciones de redirección a diferentes sitios solo deben permitir la ejecución a través de enlaces permitidos

3.2.5 Requerimientos de escalabilidad

- La arquitectura propuesta debe separar las capas de presentación, negocio y bases de datos permitiendo que sean desplegadas físicamente en diferentes servidores.

3.2.6 Requerimientos de entorno

- La solución propuesta debe ser desplegada en la infraestructura de TI asignada a la DDDR (a no ser que por requerimientos de arquitectura se determine lo contrario), la cual está compuesta por:
    - Tres (3) servidores Windows Server 2012 R2 para ambiente de producción, uno para desplegar la capa de presentación sobre IIS, uno para desplegar servicios web sobre IIS y un servidor de base de datos con SQL Server 2016.
    - 3 servidores Windows Server 2012 R2 para ambiente de pruebas, uno para desplegar la capa de presentación sobre IIS, uno para desplegar servicios web sobre IIS y un servidor de base de datos con SQL Server 2016.
    - El entorno de desarrollo debe ejecutarse en sistemas operativos Windows, y debe estar restringido al uso de licencias libres o las licencias adquiridas por el DNP, se debe validar las mismas con la OTSI.

- La solución debe construirse bajo las siguientes tecnologías: backend con Microsoft .NET, frontend con Angular 7+ o React.
- Existe la posibilidad de utilizar la plataforma de aprendizaje del DNP, basada en Moodle.

3.2.7 Requerimientos de interoperabilidad

- La arquitectura propuesta debe exponer una capa de lógica de negocios como servicios Web SOAP o API REST. Esta capa debe poseer seguridad en la autenticación y autorización. Cualquier decisión que se tome en el uso de otra tecnología en este sentido deberá ser validada en un comité técnico una vez inicie el contrato.
- Los servicios Web de lógica de negocio deben estar asegurados con el uso de credenciales, para las operaciones que lo requieran en la capa de presentación.
- Los usuarios del sistema deben usar un servicio web con el que cuenta la DDDR para la autenticación.
- La solución debe permitir el envío de correos electrónicos usando office 365.
- La solución debe permitir rastrear el número de visitas, numero de descargas de documentos, vistas y eventos clic sobre los módulos y/o controles relevantes (determinados en una especificación más detallada posteriormente), así como la localización geográfica de dichos eventos. Lo anterior, usando Google Analytics.

3.2.8 Requerimientos organizacionales

- Conocer y cumplir, cuando apliquen, los lineamientos técnicos para los dominios de Información, Sistemas de Información y Servicios Tecnológicos del marco de referencia de arquitectura de MinTIC y Gobierno Digital.
- Conocer y cumplir los lineamientos y buenas prácticas para desarrollo de software de la Oficina de Tecnologías y Sistemas de Información (OTSI).
- Conocer y cumplir los lineamientos y buenas prácticas de Seguridad para aplicativos WEB del DNP.
- Privilegiar el uso de metodologías ágiles de desarrollo para hacer entregas frecuentes y rápidas.
- Adaptar la metodología de desarrollo de software para que guarde conformidad con la metodología de referencia del DNP.
- Proveer mecanismos que faciliten el ajuste de la identidad corporativa del DNP (logos, colores, tamaños de letra, etc.).
- Disponer de un equipo de trabajo idóneo y suficiente para atender los compromisos y asegurar la calidad de las entregas.
- Mantener actualizado el código fuente y demás documentación técnica requerida, en el repositorio que para tal fin disponga el DNP en el desarrollo de Sistemas de Información.
- Cuando aplique, el proveedor deberá hacer la cesión correspondiente de derechos patrimoniales al DNP
- Proveer ambientes de desarrollo y pruebas para el Sistema de Información a desarrollar, esto significa suministrar el recurso humano, la infraestructura, el licenciamiento de software y las herramientas necesarias para proveer y mantener operativos estos ambientes.
- Contar con una infraestructura de computación y conectividad que permita atender los compromisos contractuales cuando se requiera y no sea posible el desplazamiento a la Entidad.
- Brindar mantenimiento correctivo durante la vigencia de la garantía, la cual no deberá ser menor a 4 meses.
- Establecer Acuerdos de Nivel de Servicio (ANS) entre las partes. A continuación, se proponen algunos:

NOMBRE	DESCRIPCIÓN	FORMULA DE CALCULO	VALOR DE ACEPTACION	RESPONSABLE
Nivel de cumplimiento de entregables	Aplica para cada entregable definido en el	(Número total de entregables realizados a tiempo / Número total de entregables previstos) * 100	Igual o superior al 85%.	Proveedor

NOMBRE	DESCRIPCIÓN	FORMULA DE CALCULO	VALOR DE ACEPTACION	RESPONSABLE
	plan del proyecto y revisado en cada informe de seguimiento.			
Número de revisiones sobre los entregables	Aplica para cada entregable definido en el plan del proyecto y entregado para revisión y aprobación	Número de revisiones realizadas sobre cada entregable.	Se acepta un máximo de tres (3) revisiones por entregable antes de obtener la aprobación.	Cliente
Tiempo para revisar entregables de documentación y reportar resultados	Aplica para cada entregable definido en el plan del proyecto y entregado para revisión y observaciones	Horas hábiles para revisar y reportar, las horas hábiles son 8 por día.	Se Acepta un máximo de 32 horas para el manual técnico y el manual de usuario y 8 horas para especificación de requerimientos.	Cliente
Nivel de defectos en pruebas	Se evalúa para cada componente de software entregado para revisión y pruebas de usuario.	Nivel de defectos críticos en pruebas = (Cantidad de Requerimientos con defectos críticos / Cantidad de Requerimientos implementados en la solución) * 100	Se aceptan hasta el 5% de los Requerimientos con defectos críticos.	Proveedor
		Nivel de defectos mayores en pruebas = (Cantidad de Requerimientos con defectos mayores / Cantidad de Requerimientos implementados en la solución) * 100.	Se aceptan hasta el 10% de los Requerimientos con defectos mayores	Proveedor
		Nivel de defectos menores en pruebas = (Cantidad de Requerimientos con defectos menores / Cantidad de Requerimientos implementados en la solución) * 100	Se aceptan hasta el 20% de los Requerimientos con defectos menores	Proveedor
		Nivel de defectos cosméticos en pruebas = (Cantidad de Requerimientos con defectos cosméticos / Cantidad de Requerimientos implementados en la solución) * 100	Se aceptan hasta el 25 % de los Requerimientos con defectos cosméticos	Proveedor

NOMBRE	DESCRIPCIÓN	FORMULA DE CALCULO	VALOR DE ACEPTACION	RESPONSABLE
Reapertura de defectos en estabilización e implantación	Se evalúa para cada solución terminando la Construcción o la Actualización y Mantenimiento, como resultado de las pruebas de integración del proyecto, con la entrega oficial de la solución a pruebas de usuario. Se vuelve a evaluar al finalizar el periodo de estabilización iniciando desde cero.	Reapertura de defectos = Número de errores reportados como solucionados y vueltos a encontrar en la aplicación de pruebas o en la ejecución del software.	Para defectos críticos y mayores No se acepta la reapertura de defectos. El valor debe ser cero (0). Para defectos menores y cosméticos se acepta como máximo la reapertura de tres defectos por solución.	Proveedor
Nivel de defectos en el periodo de estabilización	Se evalúa para cada solución al finalizar el periodo de estabilización.	Defectos del periodo de estabilización = Número de defectos reportados en los primeros 30 días de operación de la solución.	No se aceptan defectos críticos. El valor debe ser cero (0). Para el caso de errores mayores, el valor debe ser menor a tres (3) Para el caso de defectos menores o cosméticos, el valor debe ser menor a cinco (5)	Proveedor
Tiempo del proyecto dedicado a la corrección de defectos en el periodo de pruebas	Se evalúa para cada solución al finalizar el periodo de pruebas.	Tiempo de correcciones = (Tiempo de corrección de defectos en horas / Tiempo total de desarrollo en horas en el periodo de pruebas) * 100.	Se acepta un porcentaje máximo del 20%.	Proveedor
Tiempo promedio dedicado a la corrección de defectos en el periodo de estabilización	La evaluación se realiza sobre cada uno de los defectos encontrados durante los siguientes 60 días después de la entrada en producción de cada una de las soluciones. El tiempo de resolución de defectos se contabiliza desde la radicación del defecto, hasta la puesta en producción de la corrección	Tiempo promedio de correcciones = (Tiempo de resolución de defectos en días / Número de defectos resueltos.	Se acepta un valor promedio máximo de 5 días.	Proveedor